Zsigmondy's Theorem

Bart Michels

February 4, 2014*

Zsigmondy's theorem is a by few known theorem that often proves useful in various number theory problems. In this article we give an elementary proof of Zsigmondy's theorem.

Zsigmondy's theorem. *Let* $a, b \in \mathbb{N}$ *such that* $\gcd(a, b) = 1$ *and* $n \in \mathbb{N}$, $n > 1$. *There exists a prime divisor of* $a^n - b^n$ *that does not divide* $a^k - b^k$ *for all* $k \in \{1, 2, \ldots, n-1\}$, *except in the following cases:*

- $2^6 - 1^6$,
- $n = 2$ *and* $a + b$ *is a power of* 2.

Such a prime divisor is called a *primitive prime divisor of* $a^n - b^n$. Note that 2 can never be a primitive prime divisor.

The theorem was discovered by Zsigmondy in 1892 and independently rediscovered by Birkhoff and Vandiver in 1904. The special case where $b = 1$ was discovered earlier by Bang in 1886.
The proof we present is mainly a reformulation of Birkhoff and Vandivers proof, which was published in 1904, see [1]. [1, Theorem 1] is nowadays, among Olympiad enthousiasts, known as a case of the Lifting The Exponent Lemma. Here we present this Lemma as Lemma 5, for a proof we refer to [4]. We give a shorter proof of [1, Theorem 5], using some properties of cyclotomic polynomials. The most important properties are restated here, a more detailed version with proofs is to be found in [2]. Case 3 in the third part of the proof given here is a generalisation of its source of inspiration, namely [3, Key Lemma].

1 Prerequisites

Before proving the main theorem we present some elementary properties of cyclotomic polynomials. The proofs can be found in [2].
Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial.

Theorem 1. *Let* p *be a prime number. If the polyomial* $x^n - 1$ *has a double root modulo* p, *that is, there exists an integer* a *and a polynomial* $f(x) \in \mathbb{Z}[x]$ *for which*

$$x^n - 1 \equiv (x - a)^2 f(x) \pmod{p},$$

then $p \mid n$.

*Modified december 1st, 2014

Theorem 2. *If n is a positive integer, then*

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

and

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}. \tag{2}$$

Here a negative exponent in the right hand side of (2) has to be interpreted as a division of polynomials.

Theorem 3. *Let p be a prime number and n, k be positive integers. Then*

$$\Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}) & \text{if } p \mid n \\ \dfrac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})} & \text{if } p \nmid n. \end{cases}$$

In particular we have that $\Phi_{p^k n}(a) \mid \Phi_n(a^{p^k})$ for all $a \in \mathbb{Z}$.

Theorem 4. *Let n be a positive integer and a be any integer. Then every prime divisor p of $\Phi_n(a)$ either satisfies $p \equiv 1 \pmod{n}$ or $p \mid n$.*

There are three more Lemmas that will be useful.

Lemma 5. *Let x and y be integers, let n be a positive integer, and let p be an odd prime such that $p \mid x - y$ and none of x and y is divisible by p. Then*

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Here $v_p(a)$ denotes the highest integer exponent k such that $p^k \mid a$. We also write $p^k \parallel a$. We will refer to this as the *Lifting The Exponent Lemma.*

Lemma 6. *Let p be prime, $n = p^\alpha q \in \mathbb{Z}$ such that $p \nmid q$. The integer zeroes of Φ_n modulo p have order q modulo p.*

Proof.
From $p \mid \Phi_n(a)$ we certainly have $p \mid a^n - 1 \equiv a^q - 1$, so $k = \text{ord}_p(a)$ exists and $k \mid q$. Because (theorem 3) $\Phi_n(a) \mid \Phi_q(a^{p^\alpha}) \equiv \Phi_q(a) \pmod{p}$ we have that $p \mid \Phi_q(a)$.
If $k < q$ there would be a divisor $d \mid k$ for which $p \mid \Phi_d(a)$ (a consequence of (1)). As $d \mid q$ and $d < q$ this means the polynomial $x^q - 1 = \prod_{r|q} \Phi_r(x)$ has a double root, a, modulo p due to a factor $\Phi_d(x)\Phi_q(x)$. From theorem 1 we would obtain that $p \mid q$, which is impossible. Therefore $k = q$. $\square$

Lemma 7. *If n is a positive integer and $x > 1$ is a real number, then*

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

where the first inequality becomes an equality only if $n = 2$.

Proof.
From the triangle inequality for complex numbers we have $x-1 \leqslant |x-\zeta| \leqslant x+1$ for any complex number ζ with $|\zeta|=1$. The first inequality is strict unless $\zeta=1$, and the second is strict unless $\zeta=-1$. Applying this we obtain

$$(x-1)^{\varphi(n)} \leqslant \prod_{\substack{\zeta^n=1 \\ \operatorname{ord}(\zeta)=n}} |x-\zeta| < (x+1)^{\varphi(n)},$$

with equality only if $\varphi(n)=1$, that is, $n=2$. Note that the second inequality is always strict, because $|x-1|<|x+1|$. The product in the middle is, by definition $|\Phi_n(x)|$. If $x>1$ then from (2) we have $\Phi_n(x)>0$, hence $|\Phi_n(x)|=\Phi_n(x)$. □

We are ready to prove Zsigmondy's theorem.

2 Proof of Zsigmondy's theorem

Fix two coprime positive integers a and b with $a>b$.
It is sufficient to prove that a^n-b^n has a prime divisor that does not divide a^k-b^k for all positive divisors $k \mid n$. Indeed, if $p \mid a^n-b^n$, c is an inverse of b modulo p and k is the smallest integer such that $p \mid a^k-b^k$, then $k=\operatorname{ord}_p(ac)$ has to be a divisor of n, as $(ac)^n \equiv 1 \pmod p$.

1. Connection to cyclotomic polynomials
We define $z_n=a^n-b^n$ and

$$\Psi_n=\prod_{d\mid n} {z_{\frac{n}{d}}}^{\mu(d)}. \tag{3}$$

Because $z_n=b^n\left(\left(\frac{a}{b}\right)^n-1\right)$, from (1) and (2) we have that

$$\Psi_n=b^{\varphi(n)}\Phi_n\left(\frac{a}{b}\right) \tag{4}$$

and

$$z_n=\prod_{d\mid n}\Psi_d. \tag{5}$$

If $z_n=p_1^{a_1}\cdots p_r^{a_r}$ where $p_{s_1},\ldots,p_{s_t}$ are the primitive prime divisors of z_n, we set

$$P_n=p_{s_1}^{a_{s_1}}\cdots p_{s_t}^{a_{s_t}}.$$

From (4) we have $\Psi_n\in\mathbb{Z}$ and from (3) it follows that $P_n \mid \Psi_n$, because the only z_k for which $\gcd(P_n,z_k)>1$ is z_n, by definition of P_n. Let $\Psi_n=\lambda_nP_n$. We will prove that $P_n>1$ in the cases Zsigmondy's theorem does not exclude.

2. An upper bound on $\boldsymbol{\lambda_n}$
From (5) it follows that $\Psi_n \mid \frac{z_n}{z_d}$ for every positive divisor $d\mid n$ with $d<n$.
Note that $\gcd(\lambda_n,P_n)=1$, because $\lambda_nP_n=\Psi_n \mid z_n$ and by definition P_n contains all primitive divisors of z_n, so λ_n can not be a multiple of a prime which divides P_n.
Let p be a prime divisor of Ψ_n such that $p\mid\lambda_n$, so p is not primitive. We will prove that $p\mid n$. Let $d<n$ such that $p\mid z_d$.

If $p = 2$, then from theorem 4 we have $2 \mid n$, at least if $n > 1$. Suppose p is odd. If $p \nmid n$ then by the Lifting The Exponent Lemma, $v_p(z_n) = v_p(z_d)$ so $p \nmid \frac{z_n}{z_d}$, a contradiction to $\Psi_n \mid \frac{z_n}{z_d}$. Hence $\mathrm{rad}(\lambda_n) \mid n$.
Suppose $\lambda_n > 1$. If p is a prime divisor of λ_n with $p^\alpha \parallel n$ and $n = p^\alpha q$, then from theorem 3 we have

$$p \mid \Psi_n \mid \Psi_q(a^{p^\alpha}, b^{p^\alpha}) \equiv \Psi_q \pmod{p},$$

where more generally we denote

$$\Psi_n(x,y) = y^{\varphi(n)}\Phi_n\left(\frac{x}{y}\right).$$

This means if p is a prime divisor of λ_n, then $p \mid \Psi_q$. From theorem 4 we obtain that $p \equiv 1 \pmod{q}$, because $p \nmid q$ by our assumption. So $p > q = \frac{n}{p^\alpha}$.
If r is another prime divisor of n, then $r \mid q$, so $r \leqslant q < p$. This means p is uniquely determined as the largest prime divisor of n.
Therefore, set $\lambda_n = p^\beta$. We will prove that $\beta = 1$ if $n > 2$, and treat the case $n = 2$ seperately.

If $n = 2$, $a^2 - b^2$ obviously has a primitive prime divisor (any odd prime dividing $a + b$) unless $a + b$ is a power of 2, an exception mentioned in the theorem.

If $p = 2$ we have that n is a power of 2. Then $\Psi_n = a^{\frac{n}{2}} + b^{\frac{n}{2}}$, a and b odd. Modulo 4 this is congruent to 2, which implies $\beta = 1$.
Suppose $p > 2$. Let $d \mid n$ such that $p \mid z_d$. Let c be an inverse of b modulo p, then $p \mid \Psi_n$ and thus $p \mid \Phi(ac)$, so by lemma 6, $\mathrm{ord}_p(ac) = q$. So certainly we should have $q \mid d$.
Now from (3) we have $\beta = v_p(\Psi_n) = v_p(z_n) - v_p(z_{\frac{n}{p}})$, because the only factors that do not vanish due to the exponent $\mu(d)$ and contain a factor p are z_n and $z_{\frac{n}{p}}$. By the Lifting The Exponent Lemma, $\beta = 1$.

3. A lower bound on P_n

In this part of the proof we exploit the result of Lemma 7. We consider three cases.

Case 1: $\lambda_n = 1$
If $\lambda_n = 1$, then $P_n = \Psi_n \geqslant (a-b)^{\varphi(n)} \geqslant 1$. The inequality is strict unless $n = 2$ and $a - b = 1$, but then Zsigmondy's theorem is trivially true. □

Case 2: $\lambda_n = p$ and $a - b > 1$
In this case $P_n = \frac{1}{p}\Psi_n \geqslant \frac{1}{p}(a-b)^{\varphi(n)} \geqslant \frac{2^{p-1}}{p} \geqslant 1$. Again the inequality is strict unless $a - b = 2$ and $n = 2$, which has already been treated. □

Case 3: $\lambda_n = p$ and $a - b = 1$
Suppose the inequality $P_n \geqslant 1$ is not strict, so $\Psi_n = p$. This will eventually give us the only counterexample that's left, being $n = 6$, $a = 2$.
From $p \mid z_n$ it follows that p is odd. Let $n = p^\alpha q$.
If $\alpha > 1$, then $p = \Psi_n = \Psi_{pq}(a^{p^{\alpha-1}}, b^{p^{\alpha-1}})$, but

$$\Psi_{pq}(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}) \geqslant (a^{p^{\alpha-1}} - b^{p^{\alpha-1}})^{\varphi(pq)} \geqslant a^p - b^p = \sum_{k=0}^{p-1}\binom{p}{k}b^k > p,$$

because $p > 2$, contradiction. Hence $n = pq$. Now we have

$$p = \Psi_n = \frac{\Psi_q(a^p, b^p)}{\Psi_q} \geqslant \frac{(a^p - b^p)^{\varphi(q)}}{(a+b)^{\varphi(q)}} \geqslant \frac{a^p - b^p}{a+b} \geqslant \frac{(2^p-1)b}{2b+1} \geqslant \frac{2^p - 1}{3}.$$

This is impossible when $p > 3$, so $p = 3$. Since $q < p$ the only cases to consider are $n = 3$ and $n = 6$.
If $n = 3$ the theorem is obviously true because $a^3 - b^3 = (a-b)(a^2+ab+b^2)$ and $a - b = 1$. The case $n = 6$ remains, and indeed Zsigmondy fails here. From $3 = \Psi_6 = a^2 - ab + b^2$ we easily deduce that $a = 2$ and $b = a - 1 = 1$. □

3 Applications

In this section we present some elementary applications of Zsigmondy's theorem. We start with a similar theorem for sums of nth powers.

Zsigmondy's theorem for sums. *Let $a, b \in \mathbb{N}$ such that $\gcd(a, b) = 1$ and $n \in \mathbb{N}$, $n > 1$. There exists a prime divisor of $a^n + b^n$ that does not divide $a^k + b^k$ for all $k \in \{1, 2, \ldots, n-1\}$, except for the case $2^3 + 1^3$.*
Proof.
This is an immediate consequence of Zsigmondy's theorem. For any positive integer $n > 1$ for which $2n$ does not give an exception on Zsigmondy's theorem, $a^{2n} - b^{2n}$ has a primitive prime divisor p, dividing $a^n - b^n$ or $a^n + b^n$.
Because p is primitive, p does not divide $a^n - b^n$. Thus $p \mid a^n + b^n$ and $p \nmid a^{2k} - b^{2k}$ for all $k < n$. This implies that $p \nmid a^k + b^k$ for all $k < n$. □

Note that the exception $2^6 - 1^6$ is reflected in $2^3 + 1^3$. The case $n = 2$ and $a + b$ a power of 2 disappears because we only consider $n > 1$ here.

We give a few examples where Zsigmondy's theorem can be used.

Example 1. *Find all positive integers $a, n > 1$ and k for which $3^k - 1 = a^n$.*

Solution.
Because -1 is not a quadratic residue modulo 3, we have that n is odd. From $a+1 \mid a^n+1$ we have that $3 \mid a + 1$. If $a \neq 2$ or $n \neq 3$, $a^n + 1$ has a prime divisor different from 3, which means $a^n + 1$ cannot be a power of 3.
The only remaining case is $a = 2$ and $n = 3$, giving the only solution $(a, n, k) = (2, 3, 2)$.

Example 2. *(IMO Shortlist 2002) Let $p_1, p_2, \ldots, p_n$ be distinct primes greater than 3. Show that $2^{p_1 p_2 \cdots p_n} + 1$ has at least 4^n divisors.*

Solution.
Let $a = p_1 p_2 \cdots p_n$ and $b = 2^a + 1$. It is sufficient to prove that b has at least $2n$ prime divisors. This is indeed true, because Zsigmondy's theorem for sums says that as $3 \nmid a$, $2^d + 1$ introduces a new prime for every divisor $d \mid a$. As a has 2^n divisors, b has at least 2^n prime divisors, which is much bigger than the required $2n$.

In fact, we have the following general result:

Theorem 8. *Let a, b, n be positive integers such that $3 \nmid n$ and $\gcd(a, b) = 1$. Then $\tau(a^n + b^n) \geqslant 2^{\tau(n)}$. If n is odd and $a - b > 1$, then $\tau(a^n - b^n) \geqslant 2^{\tau(n)}$.*

Here τ counts the number of positive divisors. The proof is analoguous to the solution of example 2. The conditions for the inequalites can be weakened by studying in which cases $a^d \pm b^d$ does not contain a primitive prime divisor, for some $d \mid n$.

References

[1] G.D. Birkhoff, H.S. Vandiver, *On the Integral Divisors of* $a^n - b^n$, 1904, http://www.jstor.org/stable/info/2007263

[2] Y. Ge, *Elementary Properties of Cyclotomic Polynomials*, http://www.yimin-ge.com/doc/cyclotomic_polynomials.pdf

[3] L. Thompson, *Zsigmondy's Theorem*, 2009, www.artofproblemsolving.com/Forum/download/file.php?id=25872

[4] A.H. Parvardi, *Lifting The Exponent Lemma*, 2011, http://www.artofproblemsolving.com/Resources/Papers/LTE.pdf