Weak Zsigmondy's Theorem

Batyrkhan Sakenov

January 2022

Abstract

Using the Zsigmondy's theorem is not allowed on a large share of competitions of diverse levels, from the regional ones to the worldwide, such as IMO. The reason of this tendency lies in a highly complex proof of the theorem, which transcends the scope of the high school math. However, there is a simplified version of the given theorem, which is still useful and handy. In this article, we are going to present it together with a proof. At the very end, there is a list of problems, which the given version aids to solve.

Let $P(m)$ be the set of prime divisors of m. The Weak Zsigmondy's theorem proves that for $k < n, P(a^k - b^k) \neq P(a^n - b^n)$ for positive integers a and b (with some exceptions), without proving the existence of a primitive prime divisor of $a^n - b^n$. Instead, we prove this solely by inequalities, modular arithmetic, and divisibility.

Introduction

Some facts and notations that will be used further throughout the paper:

- (a, b) is the greatest common divisor of a and b.
- $\text{ord}_a(n)$ is the order of n modulo a. In other words, it is the least positive integer k such that $n^k \equiv 1 \pmod{a}$.
- Let a, b, n, m be positive integers. If $(n, m) = d$, then
$$(a^n - b^n, a^m - b^m) = a^d - b^d \tag{1}$$
- For any non-negative x, the following inequality holds
$$3^x \geq x + 1 \tag{2}$$
(Actually $e^x \geq x + 1$.)
- If x, y are positive real numbers and $x > y$, then
$$x^n - y^n \geq (x - y)^n \ \forall n \in \mathbb{N} \tag{3}$$
- **Lifting the Exponent (*LTE*)**[3]: Let p be a prime number and let $\nu_p(n)$ be the exponent of p in the prime factorization of n. If $a, b \in \mathbb{Z}$ and $a \equiv b \not\equiv 0 \pmod{p}$, then
  1. $\nu_p(a^n - b^n) = \nu_p(n) + \nu_p(a - b)$, if $p > 2$;
  2. $\nu_2(a^n - b^n) = \nu_2(n) + \nu_2(a - b)$, if $p = 2$ and $4 \mid a - b$;
  3. $\nu_2(a^n - b^n) = \nu_2(n) + \nu_2(a - b) + \nu_2(a + b) - 1$, if $p = 2, n$ is even.

Received: October 13, 2021 Accepted: January 29, 2022 Published: April 4, 2022

The theorem and its weaker version

Zsigmondy's theorem.[4]

For any pair of co-prime positive integers $a > b \geq 1$ and any positive integer $n > 1$ there exists a prime number p, such that $p \mid a^n - b^n$, but $p \nmid a^k - b^k$ for any positive integer $k < n$. Exceptions:

- $n = 2, a + b = 2^m,\ m \geq 2$;
- $n = 6, a = 2, b = 1$.

Weak Zsigmondy's theorem.

For any pair of co-prime positive integers $a > b \geq 1$ and any pair of positive integers $n > k \geq 1$ there exists a prime number p such that $p \mid a^n - b^n$, but $p \nmid a^k - b^k$. Exceptions:

- $n = 2, a + b = 2^m,\ m \geq 2$.

The proof is split into two sections – Main lemma and the completion of the proof.

Proof of the weak version

Main lemma

For any pair of co-prime positive integers $a > b \geq 1$ and any $n > 1$ there exists prime p such that $p \mid a^n - b^n$, but $p \nmid a - b$. Exceptions:

- $n = 2, a + b = 2^m, m \geq 2$

Proof. Clearly, the case $n = 2, a + b = 2^m, m \geq 2$ is an exception. Now we suppose that the statement of Main lemma is not true. Suppose that $a - b$ and $a^n - b^n$ have the same sets of prime divisors. In other words, in canonical forms $a - b = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$, and $a^n - b^n = 2^{\beta} p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t}$. Notice that $\alpha_i \leq \beta_i$ for any $1 \leq i \leq t$ as $a - b \mid a^n - b^n$. We consider two cases:

1. n is odd
2. n is even

Case 1.1. n is odd.

Notice that $2 \nmid a - b \implies 2 \nmid a^n - b^n$. On the other hand, if $2 \mid a - b$, from the expansion

$$(a^n - b^n) = (a - b)(a^{n-1} + \dots + b^{n-1}),$$

we get that

$$\nu_2(a^n - b^n) = \nu_2(a - b),$$

as $a^{n-1} + \dots + b^{n-1}$ is an odd number. So, in both cases $\nu_2(a^n - b^n) = \nu_2(a - b) = \alpha = \beta$. Also from LTE:

$$\nu_{p_i}(a^n - b^n) = \nu_{p_i}(a - b) + \nu_{p_i}(n) \iff \nu_{p_i}(n) = \beta_i - \alpha_i\ \forall 1 \leq i \leq t.$$

Hence,

$$n \geq p_1^{\beta_1-\alpha_1} p_2^{\beta_2-\alpha_2} \dots p_t^{\beta_t-\alpha_t} = \prod_{i=1}^{t} p_i^{\beta_i-\alpha_i} = d. \tag{4}$$

At this point the value of n seems very large, so we use inequalities. We know that $n \geq 3$, so from (2)

$$a^n - b^n \geq a^3 - b^3 > (a-b)^3.$$

Therefore, there exists $1 \leq l \leq t$ such that $\beta_l > 3\alpha_l \geq \alpha_l$. Now, we prove that $\alpha_i p_i^{\beta_i-\alpha_i} \geq \beta_i$.

$$\alpha_i p_i^{\beta_i-\alpha_i} \geq \beta_i \iff \alpha_i \left(p_i^{\beta_i-\alpha_i} - 1\right) \geq \beta_i - \alpha_i.$$

But this is true, because from (2) and $\alpha_i \geq 1$ we get:

$$\alpha_i \left(p_i^{\beta_i-\alpha_i} - 1\right) \geq p_i^{\beta_i-\alpha_i} - 1 \geq 3^{\beta_i-\alpha_i} - 1 \geq \beta_i - \alpha_i \ \forall i : 1 \leq i \leq t.$$

However, from $\beta_l > \alpha_l$ we deduce that $3^{\beta_l-\alpha_l} - 1 > \beta_l - \alpha_l$, meaning that we got a strict inequality. That is why $\alpha_i p_i^{\beta_i-\alpha_i} \geq \beta_i$ for any $1 \leq i \leq t$, and $\alpha_l p_l^{\beta_l-\alpha_l} > \beta_l$. These facts combined with (4) and (3) give us

$$\begin{aligned} 2^\beta p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t} &= a^n - b^n \geq (a-b)^n \geq (a-b)^d = \\ &= 2^{\alpha d} \prod_{i=1}^{t} p_i^{\alpha_i d} \geq 2^\alpha \prod_{i=1}^{t} p_i^{\alpha_i p_i^{\beta i-\alpha_i}} > 2^\beta p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t}, \end{aligned}$$

a contradiction.

This is the backbone of the proof as the rest of it consists of a simple case work and the direct application of the Case 1.1.

Case 1.2. n is even.

Let $n = 2^s n_1$, and $(n_1, 2) = 1$. There are two possible cases:

Case 1.2.1. $n_1 > 1$.

Then $a^{n_1} - b^{n_1} \mid a^n - b^n$. From Case 1.1

$$\exists\, p : p \mid a^{n_1} - b^{n_1} \mid a^n - b^n,\ p \nmid a - b,$$

leading to a contradiction.

Case 1.2.2. $n_1 = 1, s \geq 2$.

If $a - b \neq 2^k$ for some positive integer k, then as $(a-b, a+b) = (2b, a-b) = (2, a+b) \leq 2$ there exists a prime $p \mid a+b \mid a^{2^s} - b^{2^s},\ p \nmid (a-b)$. A contradiction.

Therefore, it remains to consider $a - b = 2^k$ for some positive integer k. Since $s \geq 2$,

$$a^{2^s} - b^{2^s} \equiv 0 \pmod{a^4 - b^4}.$$

Also we know that $(a-b, a+b) = (a+b, a^2+b^2) = (a^2+b^2, a-b) = 2$.

Clearly, $a^2+b^2 > a+b > 2$, so $a+b$ and a^2+b^2 cannot be both some powers of 2. Thus, there exists prime p,

$$p \mid (a+b)(a^2+b^2) \mid a^{2^s} - b^{2^s},\ p \nmid a-b.$$

Which is a contradiction.

We got contradictions in both cases (n is even and n is odd) – that's why the statement of Main lemma is true. □

Completion of the proof

Now we finish the proof of the Weak Zsigmondy's theorem. As before, we have an exception when $n = 2, a+b = 2^m$. We consider the other cases. There are three major cases:

1. $(n,k) = k > 1$;
2. $(n,k) = 1$;
3. $(n,k) = d, 1 < d < k$.

Case 2.1. $(n,k) = k > 1$.

Let $a_1 \coloneqq a^k, b_1 \coloneqq b^k, n \coloneqq kn_1$. From Main lemma

$$\exists\ p : p \mid a_1^{n_1} - b_1^{n_1} = a^n - b^n,\ p \nmid a_1 - b_1 = a^k - b^k,$$

which is a contradiction except for the case when $n_1 = 2, a^k + b^k = 2^m, m \geq 2$. Now we prove that this case is impossible.

Since a and b are relatively prime, $a \equiv b \equiv 1 \pmod 2$. By looking at $a^k + b^k$ modulo 4, we get that k is odd. This means that $a + b \equiv 0 \pmod 4$, which is why according to LTE

$$m = \nu_2\left(a^k + b^k\right) = \nu_2(a+b) + \nu_2(k) = \nu_2(a+b).$$

But that is impossible, because $a^k + b^k > a + b$ and $a^k + b^k \equiv 0 \pmod{a+b}$.

Case 2.2. $(n,k) = 1$.

According to Main lemma we can find a prime p such that

$$p \mid a^n - b^n,\ p \nmid a - b.$$

Then $p \nmid a^k - b^k$, because $\left(a^n - b^n, a^k - b^k\right) = a - b$, which is not divisible by p.

Case 2.3: $(n,k) = d, 1 < d < k$.

Let $a_1 = a^d, b_1 = b^d, n_1 = \frac{n}{d}, k_1 = \frac{k}{d}$. From Main lemma, Case 2.1, and Case 2.2

$$\exists\ p : p \mid a_1^{n_1} - b_1^{n_1} = a^n - b^n,\ p \nmid a_1 - b_1 \implies p \nmid a_1^{k_1} - b_1^{k_1} = a^k - b^k.$$

All three cases lead to contradictions. This concludes the proof of the Weak Zsigmondy's theorem. □

Example problems

Despite the fact that the weak version is not as strong as the original Zsigmondy's theorem, it is still of great use for solving several problems of olympiad math level. Below are several examples.

Example 1.

(IMO shortlist 1997) Let q, m, n be positive integers such that $q > 1$ and $m \neq n$. Prove that if $q^m - 1$ and $q^n - 1$ have the same prime divisors, then $q + 1$ is a power of 2.

Proof. This is a special special case of the Weak Zsigmondy's Theorem, where $a = q, b = 1$. We know that this might be possible only when $q + 1 = 2^r$ for $r \geq 2$. □

Example 2.

Prove that there are no triples (a, b, c) of positive integers such that for any $n \geq 1$:

$$a^n - b^n \mid c^n$$

Proof. Suppose that $c = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Then all prime divisors of $a^n - b^n$ belong to the set $\{p_1, \dots, p_k\}$. But the Weak Zsigmondy's theorem contradicts that. □

Example 3.

For prime numbers p and q there exist positive integers m and n such that:

(a) $1 + q + \dots + q^n$ is a power of p,

(b) $1 + p + \dots + p^m$ is a power of q.

Prove that either p or q equals to 2.

Proof. Suppose that $q > 2$ and $p > 2$, then from (a) and (b) we get that $n+1$ and $m+1$ must be odd. Let $q^{n+1} - 1 = (q-1)p^\alpha$ and $p^{m+1} - 1 = (p-1)q^\beta$.

Claim 1. $n + 1$ and $m + 1$ are prime numbers.

Assume that there is a positive integer d such that $d \mid n + 1$, then

$$q - 1 \mid q^d - 1 \mid q^{n+1} - 1 \implies q^d - 1 = (q-1)p^\gamma$$

for some positive integer γ.

But, according to the Weak Zsigmondy's theorem, $q^{n+1} - 1$ has a prime divisor that doesn't divide $q^d - 1$, hence we got a contradiction, and $n + 1$ must be prime. Analogously, $m + 1$ is prime. □

Claim 2. $\alpha \equiv 0 \pmod{n+1}$ and $\beta \equiv 0 \pmod{m+1}$.

Let $k = \text{ord}_p(q)$. Since $n+1 \equiv 0 \pmod{k}$, either $k = 1$ or $k = n+1$. If $k = 1$, then $q - 1 \equiv 0 \pmod{p}$, but LTE gives

$$\nu_p\left(q^{n+1} - 1\right) = \nu_p(q-1) + \nu_p(n+1) = \nu_p(q-1) + \alpha > \nu_p(q-1).$$

Hence $p \mid n+1 \implies n+1 = p,\ \alpha = 1 \implies q^3 - 1 \leq q^p - 1 = (q-1)p \leq (q-1)^2$, which is not true. That's why $k \neq 1$, so $k = n+1$ and notice that $q^\beta \equiv 1 \pmod{p}$, hence $n+1 = k \mid \beta$. Likewise, it can be proven that $m+1 \mid \alpha$. □

The divisibility implies that $\beta \geq n+1$ and $\alpha \geq m+1$, but then

$$\left(q^{n+1} - 1\right)\left(p^{m+1} - 1\right) = (q-1)(p-1)p^\alpha q^\beta \geq (q-1)(p-1)p^{n+1}q^{m+1},$$

which is impossible. So either p or q equals to 2.
(Example: $p = 2, q = 7, n = 1, m = 2$.) □

Practice problems

Main problem. For any pair of co-prime nonzero integers $a > b$ (note: a and be might negative) and any pair of positive integers $n > k \geq 1$ there exists prime number p, such that $p \mid a^n + b^n$, but $p \nmid a^k + b^k$. Exceptions:

- $n = 3, a = 2, b = 1$.

(Note: Solution needs some not too difficult modifications.)

Problem 1. (IMO 2000 shortlist) Find all triplets of positive integers (a, m, n) such that $a^m + 1 \mid (a+1)^n$.

Problem 2. ([5]) Let A be a finite set of prime numbers and let a be an integer greater than 1. Prove that there are only finitely many positive integers n such that all prime factors of $a^n - 1$ are in A.

Problem 3. Prove that the sequence $a_n = 3^n - 2^n$ contains no three numbers in geometric progression.

Problem 4. (Balkan MO 2009) Solve the equation $3^x - 5^y = z^2$ in positive integers.

Problem 5. Find all solutions of the equation $x^{2009} + y^{2009} = 7^z$ for x, y, z positive integers.

Problem 6. (IMO shortlist 2000) Does there exist a positive integer n such that n has exactly 2000 prime divisors and n divides $2^n + 1$?

Problem 7. (IZhO 2017) For each positive integer k denote $C(k)$ to be sum of its distinct prime divisors. For example $C(1) = 0, C(2) = 2, C(45) = 8$. Find all positive integers n for which $C(2^n + 1) = C(n)$.

References

[1] **The Zsigmondy's Theorem**, PISOLVE,
https://artofproblemsolving.com/community/c6h422330

[2] **Zsigmondy's Theorem**, Bart Michels,
http://pommetatin.be/files/zsigmondy_en.pdf

[3] **Lifting the Exponent**, Parvardi A.H.,
https://artofproblemsolving.com/community/c6h401494p2235791

[4] **Zsigmondy's Theorem**, Andy Loo,
Mathematical Excalibur February 2012 issue
https://www.math.ust.hk/excalibur/v16_n4.pdf

[5] **Problems From The Book**, Chapter 14, page 330, Titu Andreescu