The Zsigmondy Theorem

PISOLVE

7/31/11

Abstract

In this paper we will be discussing the uses and applications of **Zsigmondy's Theorem**. As some of you may consider the theorem as "large/ brutal" , it can actually be proved by elementary methods [1] - at the same time, it is applicable in so many Number Theoretic problems(All problems in this article are sourced in AoPS). We see no reasons not to use it.

Intro Problem

Let $p > 3$ be a prime. Show that every positive divisor of $\frac{2^p+1}{3}$ is in the form $2kp + 1$.

Solution: We show that all prime divisors are in this form, then the result readily follows.Let $q|\frac{2^p+1}{3}$. Then:

$$q|2^{2p} - 1$$

$$o_2(q)|2p$$

If $o_2(q) \neq 2p$, we have 3 cases:

$$o_2(q) = 1$$

Then $q|1$, clearly impossible.

$$o_2(q) = 2$$

Then $q|3$, meaning $q = 3$. Thus, $9|2^p + 1$. This means that $p = 6j + 3$ for nonnegative integer j, so $3|p$, also impossible.

$$o_2(q) = p$$

Then $q|2^p - 1$ and also $q|2^p + 1$, meaning $q|2$, impossible since $\frac{2^p+1}{3}$ is odd. Thus, $o_2(q) = 2p$. Note that since $(2, q) = 1$ we also have:

$$q|2^{q-1} - 1$$

Thus:

$$q|2^{(q-1,2p)} - 1$$

This means $(q - 1, 2p) = 2p$ or $q = 2pk + 1$ as desired.

Remark: This was a nice problem with order of the element; generally, the sequences $a^n - 1, a^n + 1$ can be dealt with this way. But what about the general $a^n \pm b^n$? That is the question we answer today.

The Theorem

The beautiful theorem that we will be discussing for the whole article is **Zsigmondy's Theorem**

Zsigmondy Theorem:

Form 1:
If $a > b \geq 1$, $(a, b) = 1$, then $a^n - b^n$ has at least one **primitive prime factor** with the following two exceptions:
1. $2^6 - 1^6$
2. $n = 2$, and $a + b$ is a power of 2

Form 2:
If $a > b \geq 1$ then $a^n + b^n$ has at least one primitive prime factor with the exception $2^3 + 1^3 = 9$
Due to the lengthiness of the proof for this theorem, we leave it out for now. For those who are interested, see [4].

Corollary 1

Given that same prime $p|a^n + b^n$ with $p \not| a^k + b^k$ for $1 \leq k < n$, then also $p \not| a^j + b^j$ for $n < j \leq 2n$.
Proof: First, let $j = n + x, 1 \leq x \leq n - 1$. We show that $p \not| ab$. If it does, then WLOG $p|a$. This means $p|a^n \implies p|b^n \implies p|b$, a contradiction since $(a, b) = 1$.
Now note that $p|(a^n + b^n)(a^x + b^x) = a^j + b^j + a^x b^x (a^{n-x} + b^{n-x})$. Since $p \not| ab, p \not| a^{n-x} + b^{n-x}$, then also $p \not| a^j + b^j$ as desired. If $j = 2n$, then $p|(a^n + b^n)^2 = a^j + b^j + 2a^n b^n$. This imples either $p \not| a^j + b^j$ or $p = 2$. Howevver, $p = 2$ is impossible since $n > 1$. So, our corollary is proven.

Corollary 2

Given that same prime $p|a^n + b^n$ with $p \not| a^k + b^k$ for $1 \leq k < n$, then also $p \not| a^j - b^j$ for $1 \leq j < \frac{n}{2}$.
Proof: Note that:

$$p|(a^n + b^n)(a^{n-2j} + b^{2-2j}) = a^{2n-2j} + b^{2n-2j} + a^{n-2j} b^{n-2j} (a^{2j+b^{2j}})^2$$

Also:

$$p \not| (a^{n-j} + b^{n-j})^2 = a^{2n-2j} + b^{2n-2j} + 2a^{n-j} b^{n-j}$$

Subtracting the second from the first gives:

$$p \not| a^{2n-2j} b^{2n-2j} (a^j - b^j)^2$$

so $p \not| a^j - b^j$ as desired.

Applications

Example 1:

Prove that the sequence $a_n = 3^n - 2^n$ contains no three numbers in geometric progression. *(Romania TST 1994)*

Solution: Assume the contrary. Then for some indicies $x < y < z$ we have:

$$(3^y - 2^y)^2 = (3^x - 2^x)(3^z - 2^z)$$

By Zsigmondy's Theorem, there exists some prime $q|3^z - 2^z$ such that $q \not| 3^y - 2^y$, which is a contradiction. Thus no such indices exist and we are done.
Remark: This problem shows some of the true power of Zsigmondy's Theorem, immediately solving problems which would otherwise involve analysis and such.

Example 2:

Find all triples of positive integers (a, b, p) such that $2^a + p^b = 19^a$ *(Italy TST 2003)*

Solution: Rearranging gives, $19^a - 2^a = p^b$, which again resembles of **Zsigmondy**! It is a direct implication that $p = 17$ by factorizing the LHS. Now note that if $a > 3$, then the LHS exists a prime, k, such that $k \neq 17$, contradiction. Thus, it suffices to work on the cases when $a = 2, a = 1$. Which gives us the only solution $(1, 1, 17)$
Remark: Very simple and direct application. Not much to analyze, but it suffices to notice the exponent a - that directly led us to **Zsigmondy**.

Example 3:

Find all nonnegative integers m, n such that $3^m - 5^n$ is perfect square.

Solution: Taking $\pmod 4$ implies that m is a multiple of 2. Hence, from $3^{2k} - 5^n = a^2$ we have

$$(3^k - a)(3^k + a) = 5^n$$

which gives, $3^k - a = 5^x, 3^k + a = 5^y$ where $y > x$. Summing up gives $2 * 3^k = 5^x + 5^y$. If suffices some case work. When $x = 0$, $y = 0$, but they are very similar.

If $x = 0$, then we have $1 + 5^y = 2 * 3^k$ By **Zsigmondy** , if $y \geq 3$ then we have a prime $q \not| 5 + 1$, thus, we must have $y = 0$, $y = 1$, $y = 2$. By simple computation we get the solutions, $(0, 0), (2, 1)$
Remark: There also exists a *similar problem:*

Find all $x, y, z \in \mathbb{N}^3$ such that:

$$5^x - 3^y = z^2$$

(BMO 2009 Problem 1)

Example 4:

Let $2 < p < q$ be two odd prime numbers. Prove that $2^{pq} - 1$ has at least three distinct prime divisors. *(Polish Mathematical Olympiad)*

Solution: By Zsigmondy there exists a prime r with $r|2^{pq} - 1$ and $r \not| 2^b - 1$, with $b < pq$. Also, note that $2^p - 1|2^{pq} - 1, 2^q - 1|2^{pq} - 1$. It suffices to show that there are at least 2 distinct prime factors dividing $2^p - 1$ and/or $2^q - 1$. Obviously some prime $s|2^p - 1$ must hold. But also, some prime $t|2^q - 1$ exists from Zsigmondy such that $t \not| 2^p - 1$. So, r, s, t are distinct primes which divide $2^{pq} - 1$, W^5.

Example 5

Find all positive integers x, y such that $p^x - y^p = 1$ where p is a prime. *(Czech Slovakia 1996)*

Solution Rearrange to get, $p^x = 1 + y^p$. By Zsigmondy's Theorem, when $y \geq 2, p \geq 3$, there exists at least 2 prime factors dividing the RHS since $y+1|y^p+1$. When $p = 2$, this gives $2^x = y^2+1$, a contradiction mod 4 for $x > 1$. Thus the only solution is $x = 1, p = 2, y = 1$ in this case. The other exception is the exception of Zsigmondy's Theorem, namely $x = 2, p = 3, y = 2$. These are the only solutions, so we are done.

Summary

This theorem is extremely useful when applied to the right problem, and usually makes for a swift, beautiful solution! Normally when you apply this theorem, all you're left with are just a few cases. Though, we have to emphasize that **there is always more than one approach for a problem.**

Exercises:

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

2. Determine all triples of positive integers (a, m, n) such that $a^m + 1$ divides $(a + 1)^n$ *(ISL 2000 N4)*

3. Find all positives integers a ,b, and $c \geq 2$ such that : $a^b + 1 = (a + 1)^c$

4. Let $b, m, n \in \mathbb{N}$ with $b > 1$ and $m \neq n$. Suppose that $b^m - 1$ and $b^n - 1$ have the same set of prime divisors. Show that $b + 1$ must be a power of 2. *(ISL 1997)*

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. *(Problems From the Book)*

6. If natural numbers x, y, p, n, k with $n > 1$ odd and p an odd prime satisfy $x^n + y^n = p^k$, prove that n is a power of p. *(Hungary-Israel Binational 2006)*

7. Find positive integer solutions to $p^a - 1 = 2^n(p - 1)$ where p is a prime number.

8. Determine all positive integer m, n, l, k with $l > 1$such that :

$$(1 + m^n)^l = 1 + m^k$$

9. Find all naturals numbers x and y,such that $3^x 7^y + 1$ is a perfect odd power.

10. Find all of quintuple of positive integers (a, n, p, q, r) such that:

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$$

(Japanese Math Olympiad 2011)
11. Find all quadruples of positive integers (x, r, p, n)such that p is a prime number ,$n, r > 1$ and $x^r - 1 = p^n$. *(MOSP 2001)*
12. Let $p \geq 5$ be a prime. Find the maximum value of positive integer k such that

$$p^k | (p - 2)^{2(p-1)} - (p - 4)^{p-1}$$

(LTE article)
13. Find all positive integers a such that $\frac{5^a+1}{3^a}$ is an integer. *(LTE article)*
14. Find all prime p, q such that $\frac{(5^p-2^p)(5^q-2^q)}{pq}$ is an integer. *(LTE article)*
15. Fins positive integer solutions to:

$$(a + 1)(a^2 + a + 1) \cdots (a^k + a^{k-1} + ... + a + 1) = a^p + a^{p-1} + ... + a + 1$$

(Pisolve) 16. Show that $\phi(a^n + b^n) \equiv omodn$ for relatively prime positive integers a, b.
17. Find positive integer solutions to $11^a = 8^b + 9^c$. *(Pisolve)*

References

http://www.artofproblemsolving.com/Forum/search.php *(Most exercises sourced from the posts in here)*

http://www.artofproblemsolving.com/Forum/viewtopic.php?f=721t=401494p=2235791hilit=LTEp2235791
(LTE article - a few exercises from here were used)

http://mathworld.wolfram.com/ZsigmondyTheorem.html

http://www.math.dartmouth.edu/ thompson/Zsigmondy's%20Theorem.pdf

Further Reading

For another corollary: http://www.fq.math.ca/Scanned/39-5/boase.pdf
http://www.ams.org/journals/proc/1997-125-07/S0002-9939-97-03981-6/S0002-9939-97-03981-6.pdf