Exponent GCD Lemma

Masum Billal

Abstract

It is not that this particular lemma hasn't been known so far. But it hasn't been established as a lemma yet, whereas I find it pretty useful to solve many problems in olympiads. Therefore, I would like to infer this as *The Exponent Gcd Lemma*. The problems this lemma can prove, can be proved in other ways too. But this way I have found solutions much more easier and elegant, more importantly, avoiding some sledge hammers. This lemma sounds like *Lifting The Exponent(LTE)* lemma a bit. But they actually have not much in common. But as a matter of fact, LTE can be proven by this lemma. And also, a very important special case of *Zsigmondy's Theorem* can be proven using this lemma. The most impressive property of this lemma is it's simplicity.

1 Main Lemma

Before we introduce our lemma, we shall denote x is co-prime to y by $x \perp y$. That is,

$$x \perp y \Rightarrow \gcd(x, y) = 1$$

For brevity assume,

$$f(x, y, n) = \frac{x^n - y^n}{x - y},$$

where $\nu_p(n) = \alpha$ means α is the greatest positive integer so that, $p^\alpha | n$. Alternatively, we can denote by $p^\alpha || n$.

Lemma 1.1 (Exponent GCD Lemma)**.** *If $x \perp y$,*

$$g = \gcd(x - y, f(x, y, n)) | n$$

Proof Of Lemma. Re-call the identity,

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$$

This yields

$$f(x, y, n) = x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}$$

We know that,

$$P(x) = (x - a) \cdot Q(x) + r$$

then $r = P(a)$. So, in this case,

$$f(x, y, n) = (x - y) \cdot Q(x, y, n) + r$$

Hence, $r = f(y, y, n)$. Here,

$$f(y, y, n) = y^{n-1} + y^{n-2} \cdot y + \ldots + y^{n-1} = ny^{n-1}$$

From Euclidean algorithm, we can infer

$$\gcd(x - y, f(x, y, n)) = \gcd(x - y, f(y, y, n)) = \gcd(x - y, ny^{n-1})$$

Earlier we assumed $x \perp y$, and so $x - y \perp y^{n-1}$ because

$$\gcd(x-y, y) = \gcd(x, y) = 1$$

Thus,

$$g = \gcd(x - y, f(x, y, n)) = \gcd(x - y, n)$$

This gives us $g|n$.

$\square$

Corollary 1. *This can be true for all odd n too:*

$$\gcd\left(x+y, \frac{x^n + y^n}{x+y}\right) |n$$

Corollary 2. *For a prime p,*

$$\gcd(x - y, f(x, y, p)) = 1 \mathit{or}\ p$$

2 Applications

Problem 1 (Hungary, 2000)**.** *Find all positive primes p for which there exist positive integers n, x, y such that*

$$x^3 + y^3 = p^n$$

Solution. For $p = 2, x = y = 1$ suffices. Assume $p > 2$, hence odd.

If $\gcd(x, y) = d$ then, we have $d|p^n$. So, d is a power of p. But in that case, we can divide the whole equation by d and still it remains an equation of the same form. Let's therefore, consider $\gcd(x, y) = 1$.

$$(x + y)(x^2 - xy + y^2) = p^n$$

According to the lemma,

$$g = \gcd(x + y, f(x, y, 3)| \gcd(x + y, 3)$$

This means $g|3$. If $g = 3$, then we have $3|p$ or $p = 3$. On the other hand, $g = 1$ shall mean that $x + y = 1$ or $x^2 - xy + y^2 = 1$. Neither of them is true. Because $x, y > 0, x + y > 1$ and $(x - y)^2 + xy > 1$.

Problem 2 (APMO 2012 - Problem 3)**.** *Find all pairs of (n, p) so that $\dfrac{n^p + 1}{p^n + 1}$ is a positive integer where n is a positive integer and p is a prime number.*

Solution. We can re-state the relation as

$$p^n + 1|n^p + 1$$

Firstly, we exclude the case $p = 2$. In this case,

$$2^n + 1|n^2 + 1$$

Obviously, we need

$$n^2 + 1 \geq 2^n + 1 \Rightarrow n^2 \geq 2^n$$

But, using induction we can easily say that for $n > 4$, $2^n > n^2$ giving a contradiction. Checking $n = 1, 2, 3, 4$ we easily get the solutions:

$$(n, p) = (2, 2), (4, 2)$$

We are left with p odd. So, $p^n + 1$ is even, and hence $n^p + 1$ as well. This forces n to be odd. Say, q is an arbitrary prime factor of $p + 1$. If $q = 2$, then $q|n + 1$ and since

$$n^p + 1 = (n + 1)(n^{p-1} - .... + 1)$$

and p odd, there are p terms in the right factor, therefore odd. So, we infer that $2^k|n + 1$ where k is the maximum power of 2 in $p + 1$.

We will use the following lemmas without proof for being well-known.

Lemma 2.1. *If $a|b$ and $a|c$, then $a|\gcd(b, c)$.*

Lemma 2.2. *If*

$$a^x \equiv b^x \pmod n$$

and,

$$a^y \equiv b^y \pmod n$$

then

$$a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod n$$

Lemma 2.3.

$$\lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = e$$

where e is the Euler constant.

Now, we prove the following lemmas.

Lemma 2.4. *If x is the smallest positive integer such that*

$$a^x \equiv 1 \pmod n$$

then if,

$$a^m \equiv 1 \pmod n$$

m is divisible by x.

Proof. Let, $m = xk + r$ with $r < x$. Then, since $a^x \equiv 1$,

$$a^m \equiv (a^x)^k \cdot a^r \equiv 1$$

This implies,

$$a^r \equiv 1 \pmod n$$

But this is a contradiction for the minimum $x > r$. So, we must have $r = 0$ that is, $x|m$. □

Lemma 2.5. *If p is an odd prime, then $p^n \leq n^p$ for $p \leq n$.*

Proof. This is true for $n = 1$. Say, this is also true for some smaller values of n. Now, we prove this for $n+1$.

Since $p \leq n$,

$$(pn+p)^p \leq (pn+n)^p$$

and therefore,

$$(n+1)^p = n^p(1+\frac{1}{n})^p \leq p^n(1+\frac{1}{p})^p \leq p^n \cdot e < p^{n+1}$$

$\square$

Back to the problem. Assume that q is odd.

$$q|p^n+1|n^p+1$$

Write them using congruence. And we have,

$$n^p \equiv -1 \pmod{q}$$

$$\Rightarrow n^{2p} \equiv 1 \pmod{q}$$

Suppose, $e = ord_q(n)$ i.e. e is the smallest positive integer such that

$$n^e \equiv 1 \pmod{q}$$

Then, $e|2p$ and $e|q-1$ from lemma 2.4.

Also, from Fermat's theorem,

$$n^{q-1} \equiv 1 \pmod{q}$$

Therefore,

$$n^{\gcd(2p,q-1)} \equiv 1 \pmod{q}$$

From p odd and $q|p+1$, $p>q$ and so p and $q-1$ are co-prime. Thus,

$$\gcd(2p,q-1) = \gcd(2,q-1) = 2$$

From lemma 2.1, $e|\gcd(2p,q-1)$ and so we must have $e=2$. Again, since p odd, if $p = 2r+1$,

$$n^{2r+1} \equiv n \pmod{q}$$

Hence, $q|n+1$. If $q|\frac{n^p+1}{n+1}$, then by the lemma 1.1 we get

$$q|\gcd\left(n+1, \frac{n^p+1}{n+1}\right)|p$$

which would imply $q=1$ or p. Both of the cases are impossible. So, if s is the maximum power of q so that $q^s|p+1$, then we have $q^s|n+1$ too for every prime factor q of $p+1$. This leads us to the conclusion $p+1|n+1$ or $p \leq n$ which gives $p^n \geq n^p$ by lemma 2.5. But from the given relation,

$$p^n+1 \leq n^p+1 \Rightarrow p^n \leq n^p$$

Combining these two, $p=n$ is the only possibility to happen.

Thus, the solutions are

$$(n,p) = (4,2), (p,p)$$

Problem 3 (Masum Billal). *For rational a, b and all prime p, $a^p - b^p$ is an integer. Prove that, a and b must be integer.*

Solution. Since a, b are rational, we can assume that $a = \frac{m}{d}, b = \frac{n}{d}$ with $m \perp d, n \perp d$. Otherwise, if $m \not\perp d$ we can divide by the common factor. Moreover, we can assume $m \perp n$. Indeed, if not, say r is a prime factor of d. Then we must have $r \not| \gcd(m, n)$. Otherwise the condition $m \perp d$ would be broken. Therefore, without loss of generality, $m \perp n$. Let q be a prime factor of d. Thus,

$$q^p | m^p - n^p$$

for all p, and e be the smallest positive integer such that

$$m^e \equiv n^e \pmod q$$

Like lemma 2.4, we can say that $e|p$ for all prime p. But this impossible except for $e = 1$. Hence, $q|m - n$. Now, take a prime $p \neq q$, and from Exponent GCD lemma we have

$$\begin{aligned} &\gcd\left(m - n, f(m, n, p)\right)|p \\ \Longrightarrow &q \not| f(m, n, p) \end{aligned}$$

This gives us, $q^p|m - n$ for all prime $p \neq q$ which leaves a contradiction inferring that d can't have a prime factor i.e. d must be 1. And then, a and b both are integers.

Problem 4 (A Special Case Of Zsigmondy's Theorem[1]). *Prove that $x^{p^k} - y^{p^k}$ has a prime factor q such that $q|x^{p^k} - y^{p^k}$ but $q \not| x^{p^i} - y^{p^i}$ for $0 \leq i < k$.*

Problem 5 (Lifting The Exponent Lemma). *If p is an odd prime, and x, y integers so that $x \perp y$ and $p|x - y$ with*

$$\nu_p(x - y) = \alpha, \nu_p(n) = \beta$$

then,

$$\nu_p(x^n - y^n) = \alpha + \beta$$

Problem 6 (Masum Billal). *If $p > x^2 - x + 1$ is a prime and $x > 2$ a positive integer. Prove that*

$$f(x) = (1 + x)^p - (1 + x^p)$$

has at least 4 distinct prime factors.

Masum Billal
CSE, University Of Dhaka

[1]It is the most important case of Zsigmondy's theorem we use in problems. If someone considers the original theorem to be a sledge hammer, in that this lemma should work fine.