R M M

ROMANIAN MATHEMATICAL MAGAZINE

www.ssmrmh.ro

LIFTING THE EXPONENT LEMMA-(LTE)

Albert Iulian Romaniuc –10th grade

National College "Roman-Vodă" Roman-Romania

Definition. We define $v_p(x)$ to be the greatest power in which a prime p divides x: if $v_p(x) = m$, then $p^m | x$ and $p^{m+1} \nmid x$. We also write $p^m || x$ if and only if $v_p(x) = m$.

Properties.

1. $\mathbf{v_p(n) = m \in \mathbb{N}^* \Leftrightarrow p^m \mid n \text{ and } p^{m+1} \nmid n}$.
2. $\mathbf{v_p(n) = 0 \Leftrightarrow gcd(p, n) = 1}$.
3. $\mathbf{v_p(p) = 1, \text{for all primes } p}$.
4. $\mathbf{v_p(m + n) \geq \min\{v_p(m), v_p(n)\}}$.
5. $\mathbf{v_p(mn) = v_p(m) + v_p(n)}$.

Note. We have $v_p(0) = \infty$ for all primes p.

Lemma 1. Let x and y be 2 integers and let n be a positive integer. Given an arbitrary prime p(in particular, we can have p = 2) such that $gcd(n, p) = 1$, $p \mid x - y$ and neither x, nor y is divisible by p, we have:

$$\mathbf{v_p(x^n - y^n) = v_p(x - y)}.$$

Proof. $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})$. Let's show that $p \nmid x^{n-1} + x^{n-2}y + \cdots + y^{n-1}$. From $p \mid x - y \Longrightarrow x \equiv y \pmod p \Longrightarrow x^{n-1} + x^{n-2}y + \cdots + y^{n-1} \equiv x^{n-1} + x^{n-2} \cdot x + \cdots + x^{n-1} \equiv$ $\equiv nx^{n-1} \pmod p$. Now, because we know that $gcd(n, p) = 1$ and $p \nmid x \Longrightarrow p \nmid nx^{n-1}$.

Therefore, since $p \nmid nx^{n-1} \Longrightarrow v_p(x^n - y^n) = v_p(x - y)$, q. e. d.

Lemma 2. Let x and y be 2 integers and let n be an odd positive integer. Given an arbitrary prime p(in particular, we can have p = 2) such that $gcd(n, p) = 1$, p | x + y and neither x, nor y is divisible by p, we have:

$$\mathbf{v_p(x^n + y^n) = v_p(x + y)}.$$

Proof. Since n is an odd positive integer, we know that $y^n = -(-y)^n \overset{\text{Lemma 1}}{\Longrightarrow} v_p(x^n + y^n) =$ $= v_p(x^n - (-y)^n) = v_p\big(x - (-y)\big) \Longrightarrow v_p(x^n + y^n) = v_p(x + y)$, q. e. d.

Theorem 1 (First Form of LTE). Let x and y be (not necessary positive) integers, let n be a positive integer, and let p be an odd prime such that $p \mid x-y$, $p \nmid x$ and $p \nmid y$. We have:

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

Theorem 2 (Second Form of LTE). Let x, y be two integers, n be an odd positive integer, and p be an odd prime such that $p \mid x+y$, $p \nmid x$ and $p \nmid y$. We have:

$$\mathbf{v_p(x^n + y^n) = v_p(x+y) + v_p(n).}$$

Theorem 3 (LTE for p = 2). Let x and y be two odd integers such that $4 \mid x-y$. We have:

$$\boldsymbol{v_2(x^n - y^n) = v_2(x-y) + v_2(n).}$$

Theorem 4. Let x and y be two odd integers and let n be an even positive integer. We have:

$$\boldsymbol{v_2(x^n - y^n) = v_2(x-y) + v_2(x+y) + v_2(n) - 1.}$$

Problem 1. Find all possible values of n, where n is a positive integer, such that $\frac{3^n-1}{2^n}$ is also an integer.

Solution. If n is even $\overset{\text{Theorem 4}}{\Longrightarrow} v_2(3^n - 1^n) = v_2(3-1) + v_2(3+1) + v_2(n) - 1 = v_2(n) + 2$. Because $\frac{3^n-1}{2^n}$ is an integer $\Rightarrow v_2(3^n - 1^n) \geq n \Rightarrow v_2(n) + 2 \geq n$, but we also know that $v_2(n) \leq \log_2 n \Rightarrow 2 + \log_2 n \geq n \Leftrightarrow \log_2 4 + \log_2 n \geq n \Leftrightarrow \log_2(4n) \geq n \Leftrightarrow 4n \geq 2^n$, which is true only for $n \leq 4$ (for $n \geq 5$, it's easy to show that $2^n > 4n$ with the Principle of Mathematical Induction). Therefore, in this case we have the solutions n = 2 and n = 4.

If $n = 1 \Rightarrow \frac{3^1-1}{2^1} = 1$, which is an integer and so n = 1 is a solution. If n is odd and $n \geq 3 \Rightarrow \Rightarrow n = 2k + 1$, where k is a positive integer. For $n \geq 3$, it's clear that $v_2(2^n) \geq 3 \Rightarrow 4 \mid 2^n$, but $3^n - 1 = (4-1)^n - 1 \equiv -1 - 1 \equiv -2 \equiv 2 \pmod 4 \Rightarrow 4 \nmid 3^n - 1$ for $n \geq 3$.

In conclusion, $n \in \{1, 2, 4\}$, q.e.d.

Problem 2. Find all positive integers a such that $\frac{5^a+1}{3^a}$ is an integer.

Solution. From $\frac{5^a+1}{3^a} \Rightarrow 3^a \mid 5^a + 1$. If a is even, then: $5^a + 1 \equiv (-1)^a + 1 \equiv 2(\text{mod } 3)$, which is false. So, a must be an odd positive integer $\xrightarrow{\text{Theorem 2}} v_3(5^a + 1^a) = v_3(5^a + 1) = v_3(5 + 1) + v_3(a) \Rightarrow v_3(5^a + 1) = v_3(a) + 1$. Let $a = 3^r s$, where r ≥ 0 and s ≥ 1 are 2 integers $\Rightarrow v_3(a) = r$, but $v_3(3^a) = a$ and because $\frac{5^a+1}{3^a}$ is an integer $\Rightarrow v_3(3^a) \le v_3(5^a + 1) \Leftrightarrow 3^r s \le r + 1$. For $r \ge 1$, it's obvious that $3^r > r + 1$ (it's easy to show this with the Principle of Mathematical Induction). Therefore, r = 0 ⟹ s = 1 ⟹ a = 3.

Problem 3. Let p > 2013 be a prime. Also, let a and b be positive integers such that p | a + b, but $\mathbf{p^2 \nmid a + b}$. If $\mathbf{p^2 \mid a^{2013} + b^{2013}}$, then find the number of positive integer $\mathbf{n \le 2013}$ such that $\mathbf{p^n \mid a^{2013} + b^{2013}}$.

Solution. From p | a + b and $p^2 \nmid a + b \Rightarrow v_p(a + b) = 1$. We also must have $v_p(a^{2013} + b^{2013}) \ge 2$. If p ∤ a and p ∤ b $\xrightarrow{\text{Theorem 2}} v_p(a^{2013} + b^{2013}) = v_p(a + b) + v_p(2013) = 1$, which is obvious false.

Now, WLOG let's consider that p | a and p ∤ b $\Rightarrow p \nmid a + b$, which is false. Therefore p | a and p | b. If p | a and p | b $\Rightarrow p^{2013} \mid a^{2013}$ and $p^{2013} \mid b^{2013} \Rightarrow p^{2013} \mid a^{2013} + b^{2013} \Rightarrow p^k \mid a^{2013} + b^{2013}$ for every k positive integer, k ≤ 2013. In conclusion, the answer is: n can take all positive integers less than or equal to 2013 and so the number of positive integer n ≤ 2013 is 2013.

Problem 4. Let a and b two integers and p ≠ 3 a prime number such that p | a + b and $\mathbf{p^2 \mid a^3 + b^3}$. Show that $\mathbf{p^2 \mid a + b}$ or $\mathbf{p^3 \mid a^3 + b^3}$.

Solution. If p | a, from p | a + b ⟹ p | b ⟹ $p^3 \mid a^3$ and $p^3 \mid b^3 \Rightarrow p^3 \mid a^3 + b^3$. Analogous if p | b. Now, let's consider that p ∤ ab. Because p | a + b $\xrightarrow{\text{Theorem 2}} v_p(a^3 + b^3) = v_p(a + b) + v_p(3) = = v_p(a + b)$. From $p^2 \mid a^3 + b^3 \Rightarrow v_p(a^3 + b^3) \ge 2 \Rightarrow v_p(a + b) \ge 2 \Rightarrow p^2 \mid a + b$.

Problem 5. Find all positive integer solutions of the equation $\mathbf{x^{2009} + y^{2009} = 7^z}$.

Solution. Because $x + y \mid x^{2009} + y^{2009}$ and $x + y > 1 \Rightarrow 7 \mid x + y$. Removing the highest possible power of 7 from x, y, we get from Theorem 2 that: $v_7(x^{2009} + y^{2009}) = v_7(x + y) + v_7(2009) = = v_7(x + y) + 2 \Rightarrow x^{2009} + y^{2009} = 49k(x + y)$, where $7 \nmid k$. From $x^{2009} + y^{2009} = 7^z \Rightarrow$ the only prime factor of $x^{2009} + y^{2009}$ is 7 ⟹ k = 1. Therefore, $x^{2009} + y^{2009} = 49(x + y)$. If x = 1 or y = 1 ⟹ $y^{2009} = 48 + 49y$ or $x^{2009} = 48 + 49x$, which obvious doesn't have any solutions in $\mathbb{Z}_+$ because LHS is always greater than RHS. In conclusion, the equation $x^{2009} + y^{2009} = 7^z$ doesn't have any solutions in $\mathbb{Z}_+$.

Problem 6. Let k > 1 be an integer. Show that there exists infinitely many positive integers n such that n | $1^n + 2^n + \cdots k^n$.

Solution. Case I. k is not a power of 2. Let p be any odd prime divisor of k. Let's show that $n = p^m$ works for any positive integer m.

Consider $i^n + (p-i)^n$, where $i = 1,2,3,\dots,p-1$. From Theorem 2, we have: $v_p(i^n + (p-i)^n) = v_p(p) + v_p(n) = 1 + m$. Therefore, $p^{m+1} \mid i^n + (p-i)^n$. Summing, we have: $p^{m+1} \mid 2(1^n + 2^n + \cdots + (p-i)^n)$ and so $p^{m+1} \mid 1^n + 2^n + \cdots + (p-1)^n + p^n + (p+1)^n + \cdots + k^n$.

In conclusion, $n = p^m$ works for every positive integer m.

Case II. k is a power of 2.

Let p be any odd prime divisor of k + 1. Using a similar proof above, it's easy to show that $n = p^m$ works again for any positive integer m.

Problem 7. Let k be a positive integer. Find all positive integers n such that $3^k \mid 2^n - 1$.

Solution. If n is an odd positive integer $\Rightarrow$ n = 2a + 1, where a is a nonnegative integer. Then, $2^n - 1 = 2^{2a+1} - 1 = (3-1)^{2a+1} - 1 \equiv -1 - 1 \equiv -2 \equiv 1 \pmod 3$, but because $v_3(3^k) > 0$, this case is impossible. So, n is an even number, n = 2m, where m is a positive integer. Now, we have: $3^k \mid 4^m - 1$. From Theorem 1: $v_3(4^m - 1) = v_3(4^m - 1^m) = v_3(4-1) + v_3(m) = 1 + v_3(m) \Rightarrow v_3(m) \geq k - 1$.Therefore, the answer is $n = 2 \cdot 3^{k-1} \cdot t$, where t is a nonnegative integer.

Problem 8. Prove that for all positive integers n, there is a positive integer m that $7^n \mid 3^m + 5^m - 1$.

Solution. We will show that m = 7^{n-1} works. From Theorem 1 $\Rightarrow v_7\left(3^{7^{n-1}} + 4^{7^{n-1}}\right) = v_7(3+4) + v_7(7^{n-1}) = 1 + n - 1 = n \Rightarrow 3^{7^{n-1}} \equiv -4^{7^{n-1}} \pmod{7^n}$.

In a similar way, we get $5^m \equiv -2^m \pmod{7^n} \Leftrightarrow 5^{7^{n-1}} \equiv -2^{7^{n-1}} \pmod{7^n}$. So, we get: $3^{7^{n-1}} + 5^{7^{n-1}} \equiv -4^{7^{n-1}} - 2^{7^{n-1}} \pmod{7^n} \Leftrightarrow 3^{7^{n-1}} + 5^{7^{n-1}} - 1 \equiv -\left(4^{7^{n-1}} + 2^{7^{n-1}} + 1\right) \pmod{7^n}$. Since we want to show that $3^{7^{n-1}} + 5^{7^{n-1}} - 1 \equiv 0 \pmod{7^n}$, it's enough to show that $4^{7^{n-1}} + 2^{7^{n-1}} + 1 \equiv \equiv 0 \pmod{7^n}$. Since $7 \nmid 2^{7^{n-1}} - 1$(since $2^i \equiv 2,4,1 \pmod 7$ and $2^i \equiv 1 \pmod 7 \Leftrightarrow i \equiv 0 \pmod 3$), it is enough to show that: $(4^{7^{n-1}} + 2^{7^{n-1}} + 1)(2^{7^{n-1}} - 1) \equiv 0 \pmod 7 \Leftrightarrow 8^{7^{n-1}} - 1 \equiv 0 \pmod 7$, which is actually true from Theorem 1: $v_7\left(8^{7^{n-1}} - 1\right) = v_7(8-1) + v_7(7^{n-1}) = n$.

In conclusion, there is a positive integer m such that $7^n \mid 3^m + 5^m - 1$, m = 7^{n-1}.

References:

[1] https://artofproblemsolving.com/community/c6_high_school_olympiads

[2] https://pregatirematematicaolimpiadejuniori.files.wordpress.com/2016/07/lte.pdf

[3] https://brilliant.org/wiki/lifting-the-exponent/

[4] https://pregatirematematicaolimpiadejuniori.files.wordpress.com/2016/07/material-lte-iunie-2016.pdf