ISSN 1857-0623
E-ISSN 2587-3636

CZU: 372.851
DOI: 10.36120/2587-3636.v18i4.86-90

# THE METHODOLOGY OF USING THE LIFTING EXPONENT LEMMA AND HANSEL'S LEMMA IN CONTEST PROBLEMS

**Marcel TELEUCA**[*], associate professor, PhD
Tiraspol State University, Lyceum "Orizont"
**Mihai SPINEI**, student
Lyceum "Orizont"

*Team leader, Deputy leader of the national team of Moldova at IMO (2013, 2011, 2010, 2005) and Balkan Mathematical Olympiad.

**Summary**. In this article we will analyze how we can use Lifting the exponent lemma (LTE) and Hansel's Lemma to solve Diophantine equations in mathematical contests. Firstly, we will go through the statements of the lemmas and some simple examples, and then we will show how they can be used in some recent problems.

**Keywords**: Number Theory, LTE, Hansel's Lemma, exponential Diophantine equations, polynomials, modular congruence.

# METODOLOGIA UTILIZĂRII LEMEI LTE ȘI A LEMEI LUI HANSEL ÎN PROBLEME DE CONCURS LA MATEMATICĂ

**Rezumat**. În acest articol vom analiza modul în care putem folosi lema LTE și lema lui Hansel pentru a rezolva ecuațiile diofante la concursurile matematice. În primul rând, vom parcurge enunțurile lemelor și câteva exemple simple și apoi vom arăta cum pot fi utilizate în unele probleme recente.

**Cuvinte cheie**: teoria numerelor, LTE, lema lui Hansel, ecuații diofantine exponențiale, polinoame, congruență modulară.

## Introduction

Solving the problems of competition in mathematics requires from the participants an involvement not only at the level of knowledge, but also elements of creativity. The solution of such problems is far beyond the curricular contents of the school. We propose in this article to highlight some didactic aspects on solving the contest problems in mathematics.

Initially, we will introduce some definitions:

### a) Definition of $v_p$ function

We define $v_p(n)$ to be the greatest power of a prime $p$ that divides $n$.

(Example: $v_3(3) = 1,\ v_2(16) = 4,\ v_3(63) = 2$ )

### b) Proprieties of $v_p$ function

The following will hold for any natural numbers $k, a, b$ and for any prime $p$ : $v_p(p^k) = k$

$v_p(ab) = v_p(a) + v_p(b),$

If $p \nmid k$then $v_p(k) = 0,$

$v_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$. (Legendre's Formula)

### c) Proprieties of some recurrent expressions in the article

If for a natural number $n$ and a prime $p$ we have $n \vdots p$ then $(a^n - b^n) \vdots (a^p - b^p)$

And $(a^n - b^n) \vdots (a - b)$

**Theorem Statements**

**Hansel's Lemmas**

***Lemma* 1**: Let$x$ and $y$ be (not necessarily positive) integers and let $n$ be a positive integer. Given an arbitrary prime p such that:$\gcd(n,p) = 1$,$p \mid x - y$ and neither $x$ nor $y$ is divisible by $p$. We have $v_p(x^n - y^n) = v_p(x - y)$.

***Proof:*** We will use the fact that $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-2}x + y^{n-1})$. So $v_p(x^n - y^n) = v_p(x - y) + v_p(x^{n-1} + x^{n-2}y + \cdots + y^{n-2}x + y^{n-1})$.

Also from $p \mid x - y$ we have that $x \equiv y (mod\, p)$.

Therefore $x^{n-1} + x^{n-2}y + \cdots + y^{n-2}x + y^{n-1} \equiv x^{n-1} + x^{n-1} + \cdots + x^{n-1} + x^{n-1} \equiv nx^{n-1} \not\equiv 0\ (mod\, p)$, in other words $p \nmid x^{n-1} + x^{n-2}y + \cdots + y^{n-2}x + y^{n-1}$, so $v_p(x^{n-1} + x^{n-2}y + \cdots + y^{n-2}x + y^{n-1}) = 0$.

Hence $v_p(x^n - y^n) = v_p(x - y)$■

***Lemma* 2:** Let $x$ and $y$ be (not necessarily positive) integers and let $n$ be a odd positive integer. Given an arbitrary prime p such that: $\gcd(n,p) = 1$,$p \mid x + y$ and neither $x$ nor $y$ is divisible by $p$. We have $v_p(x^n + y^n) = v_p(x + y)$.

***Proof:*** We will use the fact that $x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \cdots - y^{n-2}x + y^{n-1})$. So $v_p(x^n + y^n) = v_p(x + y) + v_p(x^{n-1} - x^{n-2}y + \cdots - y^{n-2}x + y^{n-1})$.

Also from $p \mid x + y$ we have that $x \equiv -y(mod\, p)$.

Therefore

$x^{n-1} - x^{n-2}y + \cdots - y^{n-2}x + y^{n-1} \equiv x^{n-1} - x^{n-2}(-x) + \cdots - x(-x)^{n-2} + x^{n-1} \equiv x^{n-1} + x^{n-1} + \cdots + x^{n-1} + x^{n-1} \equiv nx^{n-1} \not\equiv 0\ (mod\, p)$, in other words $p \nmid x^{n-1} - x^{n-2}y + \cdots - y^{n-2}x + y^{n-1}$, so $v_p(x^{n-1} - x^{n-2}y + \cdots - y^{n-2}x + y^{n-1}) = 0$.

Hence $v_p(x^n + y^n) = v_p(x + y)$■

**Lifting the exponent lemma (LTE)**

***The First Lemma*:** Let $x$ and $y$ be (not necessarily positive) integers and let $n$ be a positive integer and $p$ be an odd prime such that $p \mid x - y$ and none of $x$ and $y$ are divisible by $p$. We have $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$.

***The Second Lemma*:** Let $x$, $y$ be two integers, $n$ be an odd positive integer, and $p$ be an odd prime such that $p \mid x + y$ and none of $x$ and $y$ are divisible by $p$.

We have $v_p(x^n + y^n) = v_p(x + y) + v_p(n)$.

(***Note***: We can see that the second form of the LTE lemma can be deduced form the first by setting $y := -y$ and setting $n$ to be odd.)

***Proof Sketch:*** The proof of the LTE lemma is similar to the given proof of Hansel's Lemma. Taking care of the case where $\gcd(n,p) > 1$ can be handled by using induction on the number of prime factors of n

We can use ***Lifting The Exponent Lemma*** and ***Hansel’s Lemma*** in lots of problems involving exponential equations, especially when we have some prime numbers. The conditions required seem very particular, but with enough experience of problem solving in number theory these lemmas become one of the most important tools. This lemmas shows how to find the greatest power of a prime $p$ in exponential expressions.

The proofs of these lemmas use nothing but simple mathematical proprieties and methods.

Some proofs were left unnoted because understanding the theorems usage and its meaning is more important than remembering its detailed and somewhat long proof.

**Example Problems**

***Problem* 1. (*Art of Problem Solving*).** Let $x, y, p, n, k$ be natural numbers such that $x^n + y^n = p^k$.

Prove that if $n > 1$ is odd, and $p$ is and odd prime, the $n$ is a power of $p$.

***Solution***: Let $g = \gcd(x, y)$. Clearly $g$ is a power of , so dividing both sides by $g^n$ we get the same equation. So we may assume $\gcd(x, y) = 1$, which will give us $x + y$ is divisible by $p$.

Assume $n = p^t r$ for some natural numbers $t$ ,$r$. If we assume that $> 1$, by LTE we get $v_p(x^{p^t r} + y^{p^t r})$ = $v_p(x + y) + v_p(p^t r) = v_p(x + y) + v_p(p^t) = v_p\left(x^{p^t} + y^{p^t}\right) = k$.

So $p^k m = x^{p^t} + y^{p^t} \leq\ x^{p^t r} + y^{p^t r} = p^k \leq p^k m$. So $m = 1$ and $= 1$, hence $n$ is a power of $p$ ■

***Problem* 2. (*UNESCO contest*, 1995).** Let $a, n$ be natural numbers and $p$ an odd prime, such that $a^p \equiv 1(mod\ p^n)$. Prove that $a\ \equiv 1(\ mod\ p^{n-1})$

***Solution***: The statement is equivalent to $a^p - 1$ is divisible by $p^n$. Clearly $\gcd(a, p) = 1$and $a - 1 \vdots p$.

$$v_p(a^p - 1^p) = v_p(a - 1) + v_p(p)\ \geq n.$$

So $v_p(a - 1) \geq n - 1 \Leftrightarrow a - 1 \vdots\ p^{n-1}$■

***Problem* 3. (*Bulgaria* 1997)** Assume that $3^{\mathrm{n}} - 2^n = p^k$ for some natural numbers $n, k$ and a prime $p$. Prove that $n$ is a prime.

***Solution*:** Suppose for contradiction that $n = qr$.

We get $3^q - 2^q|(3^q)^r - (2^q)^r, so\ p|3^q - 2^q$.

Applying LTE we get $v_p(3^{qr} - 2^{qr}) = v_p(3^q - 2^q) + v_p(r)$. Hence$p \mid r$$\Rightarrow$$3^p - 2^p|3^n - 2^n$$\Rightarrow$$3^p - 2^p \equiv 0\ (mod\ p) \Rightarrow 3 - 2 \equiv 0(mod\ p)(By\ Fermat's\ Theorem)$ which is a contradiction.

***Problem* 4. ( *TST Romania* 2009)** Let $a$ ,$n\ \geq 3$ be two positive integers such that there exists a natural number $k$ satisfying

$n \mid (a - 1)^k$. Prove that $n|\ a^{n-1} + a^{n-2} + \cdots + a + 1$.

***Solution*:** $a^{n-1} + a^{n-2} + \cdots + a + 1 = \frac{a^n - 1}{a - 1}$.

Let $p$ be a prime that divides $n. v_p(a^n-1) = v_p(a-1)+v_p(n) \Rightarrow v_p\left(\frac{a^n-1}{a-1}\right) = v_p(n) \Rightarrow n \mid \frac{a^n-1}{a-1}$.

***Problem* 5. (*P4 IMO* 2019):** Find all pairs of positive integers $(n,k)$ such that:

$$k! = (2^n-1)(2^n-2)(2^n-4)\cdots(2^n-2^{n-1})$$

(***Hint***: The main idea is to try to bound the ranges of $k$ and $n$ to reduce the problem to just solving some finite cases.)

***Solution*:** Comparing the $v_2$ on both sides we get:

$$v_2(LHS) = \sum_{i=1}^{\infty} \lfloor \frac{k}{2^i} \rfloor \leq k$$

$$v_2(RHS) = 1+2+\cdots+n-1 = \frac{n(n-1)}{2}$$

Hence $k \geq \frac{n(n-1)}{2}$.

(***Note***. that $v_3(2^{2i}-1) = 1 + v_3(i)(By\ the\ LTE\ Lemma\ 1)$and $v_3(2^{2i-1}-1) = 0.$)

Comparing the $v_3$on both sides we get:

$$v_3(LHS) = v_3(k!) \geq \frac{k}{3}$$

$$v_3(RHS) = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} 1 + v_3(i) = \left\lfloor \frac{n}{2} \right\rfloor + v_3(\left\lfloor \frac{n}{2} \right\rfloor !) \leq \frac{n}{2} + \frac{n}{4}$$

$$\frac{k}{3} \leq v_3(k!) = v_3\big((2^n-1)(2^n-2)(2^n-4)\cdots(2^n-2^{n-1})\big) \leq \frac{n}{2} + \frac{n}{4}$$

And finally $\frac{n(n-1)}{2} \leq k \leq \frac{9n}{4}$, meaning$n \leq 4$. Now we can check that the only solutions are $(k,n) = (1,1),(3,2)$. ■

***Problem* 6. (*Shortlist IMO* 2014)** Find all triplets of natural numbers $(n,m,p)$ such that both $x+y^{p-1}\ and\ x^{p-1}+y$ are powers of $p$, where $p$ is a prime.

***Solution***: If $=2$, then any pair $(x, 2^k - x)$ is a solution. If $p \geq 3$ we have that:

If $p$ divides one of $x$or $y$, then it clearly divides the other. Assume that $v_p(x) = a$ and $v_p(y) = b$ and $a, b > 0$. WLOG assume that $b \leq a$. $v_p(x^{p-1}+y) = b$, but clearly $x^{p-1}+y > p^b$, which is a contradiction.

If $p$ does not divide any of $x$ and $y$, then we have $x^{p-1}-1 \vdots p\ and\ y^{p-1}-1 \vdots p$.

Clearly $x \neq y$, WLOG assume x > y.

Let $p^b = x+y^{p-1}\ and\ p^a = x^{p-1}+y, with\ a > b$. We have that:

$p^b = x + y^{p-1} | x^{p-1}+y \Rightarrow p^b | y^{p-2}(x^{p-1}+y) - x - y^{p-1} = x(x^{p-2}y^{p-2}-1) \Rightarrow$
$p^b | x^{p-2}y^{p-2}-1$. But $x \equiv -y^{p-1}(mod\ p^b) \Rightarrow (xy)^{p-2}-1 \equiv -y^{p(p-2)}-1\ (mod\ p^b)$
$\Rightarrow$
$p^b | y^{(p-2)p}+1$. Since $y^{p-2}+1 \equiv 0\ (mod\ p) \Rightarrow v_p(y^{p(p-2)}+1) = v_p(y^{p-2}+1)+1 \Rightarrow$
$x+y^{p-1} = p^b | p(y^{p-2}+1) \Rightarrow p(y^{p-2}+1) \geq p^b = x+y^{p-1} > y+y^{p-1}$
$= y(y^{p-2}+1)$

$\Rightarrow p > y \;\Rightarrow y = p - 1.$
$x + y^{p-1} | p(y^{p-2} + 1) = (y+1)(y^{p-2}+1) = y^{p-1} + (y^{p-2} + y + 1) < 2y^{p-1} + 2x \Rightarrow x + y^{p-1} = p(y^{p-2}+1) \Rightarrow p^{b-1} = (p-1)^{p-2} + 1.$

For $p = 3$ we get $y = 2\, and\, x = 5$. If $p > 3$, we have that $(p-1)^{p-2} + 1 > p$ and $(p-1)^{p-2} + 1 \equiv p(p-2) - 1 + 1 \equiv -2p(mod\, p^2) \Rightarrow (p-1)^{p-2} + 1$ can not be a power of p.

So finally we have the solutions: $(x, y, p) = (x, 2^k - x, 2), (2,5,3), (5,2,3)$.

***Problem* 7. (*Iran* 2008)** Let $a$ be a natural number such that $4(a^n + 1)$ is a perfect cube for any natural number $n$. Prove that $a = 1$.

***Solution*:** Set $n = 2k$ for some natural number $k$. Take some prime divisor of $a^2 + 1, p$.
$3 \,|\, v_p(4(a^n+1)) = v_p(a^2+1) + v_p(k)$, but clearly we can change the value of $k$, such that 3 does not divide $v_p(4(a^n+1))$.

***Problem* 8. (*China TST* 2009)** Let $a$ and $b$ be two natural numbers greater than 1, and $b$ is odd, and $n$ is a natural number such that $b^n | a^n - 1$. Prove that $a^b > \frac{3^n}{n}$.

***Solution*:** Let $p$ be the smallest prime divisor of $b$ $(\, p \geq 3, since\ b\ is\ odd)$.
Then $p^n | b^n | a^n - 1 \;\Rightarrow n \leq v_p(b^n) \leq v_p(a^n - 1)$.
We also have that $v_p(a^n - 1) \leq v_p((a^{p-1})^n - 1) = v_p(a^n - 1) + v_p(n) = v_p(n(a^n - 1)) \Rightarrow n \leq v_p(a^n - 1) \leq v_p(n(a^n-1)) \Rightarrow p^n \leq n(a^n - 1) \Rightarrow a^b > a^{p-1} - 1 \geq \frac{p^n}{n} \geq \frac{3^n}{n}$.

## Conclusions

Even though number theory is not covered as a topic in school, students that are preparing for national and international contests need to have advanced knowledge in some topics as LTE and Hansel's Theorem. This article is a guideline to the study of these theorems on a variety of contest problems.

## References

1. Amir Hossein Parvardi Lifting The Exponent Lemma, 2011. http://services.artofproblemsolving.com/download.php?id=YXR0YWNobWVudHMvYy82LzdjNTI1OGIyMmNjYmZkZGY4MDhhY2ViZTc3MGE1NDRmMzFhMTEzLnBkZg==&rn=TGlmdGluZyBUaGUgRXhwb25lbnQgTGVtbWEgLSBBbWlyIEhvc3NlaW4gUGFydmFyZGkgLSBWZXJzaW9uIDMucGRm
2. Problem Sources: https://artofproblemsolving.com/community
3. Billal M., Parvardi A.H. Topics in Number Theory: An Olympiad Oriented Approach, v. 1.2, 2018.
4. Teleucă M., Pop V., Croitoru D. Probleme de teoria elementară a numerelor pentru concursurile şcolare. Ed. Mega, 2016.