Lifting the exponent

Carl Joshua Quines
July 20, 2019

Valuation

Define $\nu_p(n)$ for positive integers $n$ as

$$\nu_p(n) = k \iff p^k \mid n, p^{k+1} \nmid n.$$ 

This is known as the $p$-adic valuation of $n$. Note that this is $\nu_p$ with the Greek letter $\nu$ (spelled nu, pronounced “new”).

Some properties that you should convince yourself are true:

- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
- Similarly $\nu_p \left( \frac{a}{b} \right) = \nu_p(a) - \nu_p(b)$. We can use this to extend the definition of $\nu_p$ to be a function from $\mathbb{Q} \setminus 0 \to \mathbb{Z}$.

What should $\nu_p(0)$ be? To satisfy the product rule, we can pick $\nu_p(0) = \infty$.

- $\nu_p(a + b) \geq \min \{\nu_p(a), \nu_p(b)\}$, equality holds if $\nu_p(a) \neq \nu_p(b)$.
- $\nu_p(a - b) \geq e \iff a \equiv b \pmod{p^e}$ from the previous.
- $\nu_p(\gcd(a, b)) = \min \{\nu_p(a), \nu_p(b)\}$.
- $\nu_p(\text{lcm}(a, b)) = \max \{\nu_p(a), \nu_p(b)\}$.
- $a = b \iff \nu_p(a) = \nu_p(b)$ for all $p$.
- More generally, $a \mid b \iff \nu_p(a) \leq \nu_p(b)$ for all $p$.

Examples

1. Prove that $\gcd(a, b, c) = \frac{abc \cdot \text{lcm}(a, b, c)}{\text{lcm}(a, b) \text{lcm}(b, c) \text{lcm}(c, a)}$.

   **Sketch:** Pick a prime $p$, idea is to show $\nu_p$ of LHS and RHS are the same. Let $x = \nu_p(a)$, $y = \nu_p(b)$, and $z = \nu_p(c)$. In the LHS you have $\min \{x, y, z\}$, on the RHS you have $x + y + z + \max \{x, y, z\} - \max \{x, y\} - \max \{y, z\} - \max \{z, x\}$. But these are equal.

2. Suppose $a \mid b^2 \mid a^3 \mid b^4 \mid a^5 \mid \cdots$. Prove that $a = b$.

   **Sketch:** This is an easy problem, but it’s a bit hard to write up. Using $\nu_p$ makes it easier. We have

   $$a^{2n-1} \mid b^{2n} \implies (2n-1)\nu_p(a) \leq 2n\nu_p(b) \implies \nu_p(a) \leq \frac{2n}{2n-1}\nu_p(b).$$

   Taking the limit as $n \to \infty$ means $\nu_p(a) \leq \nu_p(b)$; similarly we can prove $\nu_p(b) \leq \nu_p(a)$. This shows $\nu_p(a) = \nu_p(b)$.

\[1\] This is sometimes written as $v_p$ with the English letter $v$. I don’t think this is standard, as I see more sources use $\nu_p$. I don’t even know why $\nu$ is the letter chosen for this, other than its superficial similarity to the letter $v$. 

3. Let \( p \) prime, \( n \in \mathbb{N} \). Suppose \( p \mid 2^n - 1 \). Show that \( p \mid 2^{p-1} - 1 \). (We say \( p \mid n \iff p \mid n, p^2 \nmid n \).)

**Remark:** While this is typically done with the so-called lifting the exponent lemma, many people learn the statement without knowing the proof, which I think is bad, because the proof gives useful intuition. So we’re going to motivate the proof using this problem and the next problem.

**Sketch:** Let \( m \) be the order of 2 modulo \( p \). That is, the smallest positive integer \( m \) such that \( p \mid 2^m - 1 \). Because \( m \) is the order, we have \( m \mid n \), so \( 2^m - 1 \mid 2^n - 1 \), therefore, we get \( p \mid 2^m - 1 \).

Now we use the main idea, and that’s dividing \( 2^{p-1} - 1 \) by \( 2^m - 1 \). With some algebra,

\[
\frac{2^{p-1} - 1}{2^m - 1} = 1 + 2^m + 2^{2m} + \cdots + 2^{p-1-m}.
\]

Modulo \( p \), this is \( \frac{p-1}{m} \) (because \( p \mid 2^m - 1 \)). So this is not equal to 0, so \( p^2 \nmid 2^{p-1} - 1 \). But by FLT, \( p \mid 2^{p-1} - 1 \), the conclusion follows.

4. Let \( n \in \mathbb{N}^0 \). Find \( \nu_3 (2^{3^n} + 1) \).

**Sketch:** This is induction. Find the answer when \( n = 0 \). Then observe that

\[
\frac{2^{3^n+1} + 1}{2^{3^n} + 1} = 2^{3^n} - 2^{3^n} + 1 \equiv 1 - (-1) + 1 \equiv 3 \pmod{9},
\]

then it’s divisible by 3 but not 9, so going \( n \to n + 1 \) increases \( \nu_3 \) by 1.

**Lifting the exponent**

We can now state and prove the lifting the exponent lemma. It states that if \( p \) is an odd prime, \( p \nmid a, p \nmid b \), and \( p \mid a - b \), then

\[
\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n)
\]

for all positive integers \( n \). The condition \( p \mid a - b \) is very important, yet easy to forget. Always remember to check this condition. In particular, you must have \( \nu_p(a - b) > 0 \).

The proof is by induction on \( n \). The main idea here is the inductive step. The idea is that we want to take out the powers of \( p \) from \( n \). For example, if we take \( n = p^\alpha \), we can rewrite this as

\[
\nu_p\left((a^{p^{\alpha-1}})^p - (b^{p^{\alpha-1}})^p\right) = \nu_p\left(a^{p^{\alpha-1}} - b^{p^{\alpha-1}}\right) + 1.
\]

But to prove this, we only have to show that it’s true for \( n = p \). Similarly, if we have \( n = p^\alpha \beta \), where \( \gcd(p, \beta) = 1 \), we can write

\[
\nu_p\left((a^{p^{\alpha}})^\beta - (b^{p^{\alpha}})^\beta\right) = \nu_p\left(a^{p^{\alpha}} - b^{p^{\alpha}}\right),
\]

which means we only have to show the case when \( \nu_p(n) = 0 \). This is already our inductive step! So these two cases, the one where \( \nu_p(n) = 0 \) and \( n = p \), will form the two base cases of our induction.

The case \( \nu_p(n) = 0 \) is easy. Write

\[
\nu_p(a^n - b^n) = \nu_p(a - b) \iff \nu_p\left(\frac{a^p - b^p}{a - b}\right) = 0;
\]
where we get the second equation by transposing \( \nu_p(a - b) \) and applying the quotient rule. We only need to show that
\[
p \nmid a^{p-1} + a^{p-2}b + \cdots + b^{p-1}.
\]
This follows because \( a \equiv b \pmod{p} \), so substitute this to get
\[
a^{p-1} + a^{p-1} + \cdots + a^{p-1} \equiv na^{p-1} \not\equiv 0.
\]
The other base case, \( n = p \), is harder. We need to show that
\[
\nu_p(a^p - b^p) = \nu_p(a - b) + 1 \iff \nu_p\left(\frac{a^p - b^p}{a - b}\right) = 1.
\]
There are two parts here. First, we want to show
\[
p \mid a^{p-1} + a^{p-2}b + \cdots + b^{p-1}.
\]
This follows because \( a \equiv b \pmod{p} \), so using a similar process from the other base case, we get \( pa^{p-1} \equiv 0 \). Second, we want to show that
\[
p^2 \nmid a^{p-1} + a^{p-2}b + \cdots + b^{p-1}.
\]
This second part is an algebra bash. We substitute \( b \equiv pk + a \pmod{p^2} \), then expand with the binomial theorem. It’s not that bad because all of the terms with \( p^2 \) disappear, leaving us with
\[
a^{p-1} + (a^{p-1} + a^{p-2}pk) + (a^{p-1} + 2a^{p-2}pk) + \cdots + (a^{p-1} + (p-1)a^{p-2}pk) = a^{p-1} + (a^{p-2}pk) + (a^{p-1} + 2a^{p-2}pk) + \cdots + (a^{p-1} + (p-1)a^{p-2}pk) = \frac{a^p - b^p}{a - b}.
\]
The \( a^{p-2}pk \) terms have coefficients \( 1 + 2 + \cdots + p - 1 \equiv 0 \pmod{p} \), so coupled with the extra \( p \) factor, they all sum to \( 0 \pmod{p^2} \). This leaves you with \( pa^{p-1} \not\equiv 0 \pmod{p^2} \).

An alternative formulation follows if \( n \) is odd. Then we can replace \( b \) with \(-b\) to get
\[
\nu_p(a^n + b^n) = \nu_p(a + b) + \nu_p(n).
\]
Note, again, this only applies if \( n \) is odd.

**Example:** Suppose \( a, b, n, p, k \in \mathbb{N} \) such that \( n > 1 \) is odd, \( p \) is an odd prime, and \( a^n + b^n = p^k \). Prove that \( n \) is a power of \( p \).

**Sketch:** Check all the conditions before using LTE! We have \( p \) is an odd prime. If \( p \mid a \), then \( p \mid b \), and we can divide both \( a \) and \( b \) by \( p \) until neither is divisible by \( p \), so WLOG \( p \nmid a \) and \( p \nmid b \). Also, \( n \) is odd so we can use the + case of LTE.

Now we check the hard condition. By factorization, since \( a + b \mid a^n + b^n = p^k \), it must follow that either \( a + b = 1 \) (impossible) or \( p \mid a + b \). This gives us all the conditions and now we can use LTE:
\[
k = \nu_p\left(p^k\right) = \nu_p(a^n + b^n) = \nu_p(a + b) + \nu_p(n).
\]
Now suppose \( \ell = p^r(n) \). Then
\[
\nu_p\left(a^\ell + b^\ell\right) = \nu_p(a + b) + \nu_p(n).
\]
So \( p^k \mid a^\ell + b^\ell \mid a^n + b^n = p^k \), so they must all be equal and \( n = \ell \) which is a power of \( p \).
Problems

1. (Folklore) Fix $k \in \mathbb{N}$. Find all $n$ such that $3^k \mid 2^n - 1$.

2. (Iran 2008) Fix $a \in \mathbb{N}$. Suppose $4(a^n + 1)$ is a perfect cube for all $n \in \mathbb{N}$. Prove that $a = 1$.


5. (AIME 2018) Find the smallest $n$ such that $3^n$ ends with 01 when written in base 143.

Hints

1. $2^{2n} - 1 = 4^n - 1$ and $3 \mid 4 - 1$.

2. Taking $a^2 + 1 \mod 4$, we see it’s never a power of 2.

3. $2^p + 3^p$ is not a square. Find $\nu_5 (2^p + 3^p)$.


5. $11 \mid 3^5 - 1$ so $3^n - 1 = (3^5)^{n/5} - 1$.

References

The classic reference is Amir Hossein Parvardi’s [Lifting the Exponent Lemma] handout, but I don’t think it motivates LTE well enough. The exposition here roughly follows Evan Chen’s [OTIS Excerpts].

Thanks to Konwoo Kim for sending a correction.