P-adic Valuation

Raymond Feng

NRU

These are problems where you want to look at the highest power of a prime that divides a number. This is the ν_p function.

§ 1   Introduction

Formally, we define the p-adic valuation of n, or $\nu_p(n)$ as follows:

Definition 1 (p-adic valuation) For a positive integer n, $\nu_p(n)$ is the largest integer that satisfies $p^{\nu_p(n)} \mid n$.

Now we introduce some useful facts about the ν_p function.

Fact 1 (Properties of ν_p) The following properties of ν_p follow readily from the definition. It is important to know these well in order to understand why this function is useful.

- ✦ If $a \mid b$, then $\nu_p(a) \leq \nu_p(b)$ for all primes p.

- ✦ $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

- ✦ $\nu_p(\gcd(a, b)) = \min(\nu_p(a), \nu_p(b))$.

- ✦ $\nu_p(\mathrm{lcm}(a, b)) = \max(\nu_p(a), \nu_p(b))$.

- ✦ $\nu_p(a + b) \geq \min(\nu_p(a), \nu_p(b))$. Equality *always holds* if $\nu_p(a) \neq \nu_p(b)$, but *does not necessarily hold* when $\nu_p(a) = \nu_p(b)$. For example $\nu_2(2 + 6) \neq \min(\nu_2(2), \nu_2(6))$.

Proof: The first four facts follow immediately from the definition of ν_p and unique prime factorizations. The interesting result is the last fact: it follows from $\gcd(a, b) \mid a + b$ in combination with the first fact. The equality cases can be easily verified. ■

So why do we care so much about the ν_p function? It all lies in the following (possibly obvious) lemma:

Lemma 1 If m, n are integers such that $\nu_p(m) = \nu_p(n)$ for all primes p, then $m = n$.

Proof: This is just a restatement of natural numbers having unique prime factorization! ■

Using the above properties we are already able to solve the following problem:

![MAST logo]

Example 1 Prove that for positive integers a and b we have

$$\gcd(a + b, \operatorname{lcm}(a, b)) = \gcd(a, b).$$

Solution: It suffices to verify that ν_p of both sides are equal for all p. Fix a certain value of p, and WLOG suppose $\nu_p(a) \geq \nu_p(b)$. Then the desired equation is

$$\min(\nu_p(a + b), \max(\nu_p(a), \nu_p(b))) = \min(\nu_p(a), \nu_p(b)).$$

If $\nu_p(a) = \nu_p(b)$ the equation reduces to $\nu_p(a) = \nu_p(a)$, which is true. If $\nu_p(a) > \nu_p(b)$ then the equation reduces to $\nu_p(b) = \nu_p(b)$, which is also true. Therefore, for any p we have shown that the ν_p of both sides are equal, i.e. the two sides are actually the same natural number.

We can even extend the notion of ν_p to the rational numbers, by applying $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ to rational inputs. For example $\nu_5\left(\frac{2}{3}\right) = 0$ while $\nu_7\left(\frac{6}{49}\right) = -2$. As you might expect, we can distinguish integers from generic rational numbers using ν_p.

Fact 2 If $q \in \mathbb{Q}$, then $q \in \mathbb{Z}$ if and only if for all primes p, $\nu_p(q) \geq 0$.

Furthermore, the fifth property from earlier also hold for all rationals a, b. The proof is only slightly different from the proof from earlier and so will be omitted (hint: use the second property to first clear denominators, and then bring them back). Using this extended definition of ν_p we can tackle the following classic.

Example 2 (Classic) Prove that for all $n > 1$, $\sum_{i=1}^{n} \frac{1}{i}$ is not an integer.

Walkthrough:

1. Take ν_2 of the sum.

2. There is a unique minimum among

$$\nu_2\left(\frac{1}{1}\right), \nu_2\left(\frac{1}{2}\right), \ldots, \nu_2\left(\frac{1}{n}\right).$$

3. Repeatedly apply the fifth property of ν_p.

4. Conclude that $\nu_2\left(\sum_{i=1}^{n} \frac{1}{i}\right) < 0$.

Example 3 (Wolstenholme's Theorem) For primes $p > 3$ show that

$$\nu_p\left(\sum_{i=1}^{p-1} \frac{1}{i}\right) \geq 2.$$

Walkthrough:

1. Proving things mod p^2 is hard, so do some wishful thinking: is there an easy way to rearrange the sum and factor out a factor p?

2. Once the above step is done, it suffices to show what's left is 0 mod p. This should be straightforward after noting inverses are a bijection on $\{1, 2, \ldots, p-1\}$.

3. Where did we need $p > 3$?

MAST

§2 Common targets of ν_p

It is often useful to know the p-adic valuation of various numbers or expressions, so we give an overview of common techniques involving them.

§2.1 Factorials

The following theorem is the heart of finding ν_p of both factorials and binomial coefficients.

Theorem 1 (Legendre) For a positive integer n and prime p, we have

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Proof 1: Switching the order of summation:

$$\nu_p(n!) = \sum_{i=1}^{n} \nu_p(i) = \sum_{i=1}^{n} \sum_{k=1}^{\nu_p(i)} 1 = \sum_{k=1}^{\infty} \left[\sum_{\substack{i \in \{1,2,\dots,n\} \\ p^k \mid i}} 1 \right] = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

$\blacksquare$

Proof 2: Note that $\left\lfloor \frac{n}{p} \right\rfloor$ counts the number of multiples of p between 1 and n. For each multiple of p^2, we must add 1 more to the sum (since they contribute at least 2 factors of p, and only 1 has been counted so far), so add on $\left\lfloor \frac{n}{p^2} \right\rfloor$. Similarly, for each multiple of p^3, we must add 1 more to the sum, so add on $\left\lfloor \frac{n}{p^3} \right\rfloor$. Continuing this reasoning shows that

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

as desired. $\blacksquare$

Remark: Do you understand how the first algebraic proof encapsulates the reasoning explained in English in the second proof?

Using Legendre's theorem, we can prove the following corollary, which is just as useful (and will be used to prove Kummer's theorem in the next section).

Corollary 1 We also have
$$\nu_p(n!) = \frac{n - s_p(n)}{p - 1},$$
where $s_p(n)$ is the sum of the digits of n in base p.

Walkthrough:

MAST

1. Write $n = \sum_{i=0}^{k} a_i p^i = (\overline{a_k a_{k-1} \ldots a_0})_p$ for integers $0 \le a_i < p$; then what are

$$\left\lfloor \frac{n}{p} \right\rfloor, \left\lfloor \frac{n}{p^2} \right\rfloor, \left\lfloor \frac{n}{p^3} \right\rfloor, \ldots$$

   in terms of the a_i?

2. Use Legendre's theorem to calculate $\nu_p(n!)$, and do some algebra to finish.

Example 4 (USSR Math Olympiad) Show that $\binom{1000}{500}$ is not divisible by 7.

Solution: Note by Legendre, we have $\nu_7(1000!) = 142 + 20 + 2 = 164$ while $\nu_2(500!) = 71 + 10 + 1 = 82$, so

$$\nu_7\left(\binom{1000}{500}\right) = \nu_7\left(\frac{1000!}{(500!)^2}\right) = \nu_7(1000!) - 2\nu_7(500!) = 0 \implies 7 \nmid \binom{1000}{500},$$

as desired.

§2.2   Binomial Coefficients

Using the corollary from above, we can actually determine the ν_p of any binomial coefficient (which isn't too surprising, given that binomial coefficients can be written in terms of factorials, which we found nu_p for earlier).

Theorem 2 (Kummer) If c is the number of carries that must be made when adding n to $m - n$ in base p, then

$$\nu_p\left(\binom{m}{n}\right) = c.$$

Walkthrough:

1. Show that the number of carries when adding n to $m - n$ in base p is precisely

$$\frac{s_p(n) + s_p(m - n) - s_p(m)}{p - 1}.$$

2. Recall the earlier corollary, and conclude.

   We solve the earlier USSR Math Olympiad problem in a different way now:

Example 5 (USSR Math Olympiad) Show that $\binom{1000}{500}$ is not divisible by 7.

Solution: Note that $500_{10} = 1313_7$, and no carries occur when adding 1313_7 to itself. By Kummer's theorem, this implies that

$$\nu_p\left(\binom{1000}{500}\right) = 0 \implies 7 \nmid \binom{1000}{500},$$

as desired.

MAST

§ 2.3 Lifting the Exponent

This section will cover the extremely useful lemma, Lifting the Exponent (LTE), which allows us to evaluate ν_p on the difference of powers. It has seen an increase in usage in the past few years of AIME.

> **Theorem 3 (LTE)** Let p be an *odd prime* and a, b integers such that *all of the following hold*:
> $$p \nmid a, \quad p \nmid b, \quad p \mid a - b.$$
> Then for any positive integer n, we have
> $$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n).$$

Walkthrough:

1. Prove the statement for $\nu_p(n) = 0$. You will need to use
$$x^n - y^n = (x - y)\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right).$$

2. Use induction to prove the statement for $n = p^m$ for some positive integer m. You will need to use
$$x^p - y^p = (x - y)\left(x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1}\right).$$

3. Let $m = \nu_p(n)$ and suppose $n = p^m \cdot k$ where $p \nmid k$ by definition. How can we rewrite $a^n - b^n$ so that the new exponent is a power of p?

4. Finish by applying the first two steps.

5. Where does the proof go wrong if $p = 2$?

6. Can you derive an alternate form for LTE for when $p = 2$?

> **Fact 3** The following cases resolve LTE for $p = 2$.
>
> ✦ For odd integers a, b such that $4 \mid a - b$ and any positive integer n, we have
> $$\nu_2(a^n - b^n) = \nu_2(a - b) + \nu_2(n).$$
>
> ✦ For odd integers a, b such that $4 \nmid a - b$ and any *even* positive integer n, we have
> $$\nu_2(a^n - b^n) = \nu_2(a - b) + \nu_2(a + b) + \nu_2(n) - 1.$$
>
> ✦ For odd integers a, b such that $4 \nmid a - b$ and any *odd* positive integer n, we have
> $$\nu_2(a^n - b^n) = 1.$$

These cases are quite cumbersome to commit to memory; it is therefore *highly recommended* that you understand the proof of LTE for odd primes well and just repeat a similar induction argument to rederive it when needed. Another equivalent reformulation that may be easier to remember/use is the following:

> **Fact 4** For odd integers a, b and any positive integer n, we have
> $$\nu_2(a^n - b^n) = 1 \quad \text{or} \quad \nu_2(a^n - b^n) = \nu_2(a - b) + \nu_2(a + b) + \nu_2(n) - 1.$$

MAST

Corollary 2 Let p be an *odd prime* and a, b integers such that *all of the following hold*:

$$p \nmid a, \quad p \nmid b, \quad p \mid a + b.$$

Then for any positive *odd* integer n, we have

$$\nu_p(a^n + b^n) = \nu_p(a + b) + \nu_p(n).$$

Let's tackle the following problem using LTE! Hopefully the example will emphasize just how important each condition is.

Example 6 Evaluate $\nu_5\left(10^{100} - 5^{100}\right)$.

Walkthrough:

1. We can't apply LTE directly since $5 \mid 10, 5$. Factor out some obvious factors of 5 to fix this issue.

2. You should be left with $2^{100} - 1$. We can't apply LTE directly since $5 \nmid 2 - 1$. Fix this issue by writing $100 = m \cdot \frac{100}{m}$ for some m and noting $2^{100} - 1 = (2^m)^{\frac{100}{m}} - 1$.

3. Finish the problem.

MAST

§3 Problems

Minimum is [50 ✏]. Problems with the ⬦ symbol are required.

> "I try to show the schemers how pathetic their attempts to control things really are."
>
> Joker

[1 ✏] **Problem 1** Determine $\nu_3(2021!)$.

[1 ✏] **Problem 2** Find the smallest integer n such that $43 \nmid \binom{2021}{n}$.

[2 ⬦] **Problem 3 (Classic)** If $2^{n-1} \mid n!$, prove that n is a power of 2.

[2 ✏] **Problem 4** (Classic) Prove that for all $n > 1$, $\sum_{i=1}^{n} \frac{1}{2i-1}$ is not an integer.

[3 ✏] **Problem 5** (AIME I 2018/11) Find the least positive integer n such that when 3^n is written in base 143, its two right-most digits in base 143 are 01.

[3 ✏] **Problem 6** (Proposed by Columbia to IMO 1989) Show that there are infinitely many positive integers n for which $n - \nu_2(n!) = 1989$.

[4 ⬦] **Problem 7 (AIME I 2020/12)** Let n be the least positive integer for which $149^n - 2^n$ is divisible by $3^3 \cdot 5^5 \cdot 7^7$. Find the number of positive divisors of n.

[4 ✏] **Problem 8** (brilliant.org) Show that 2 is a primitive root mod 3^k for all positive integers k.

[4 ✏] **Problem 9** (Classic) For positive integers n, determine all possible values of

$$\gcd\left(\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}\right).$$

[6 ⬦] **Problem 10 (BAMO 2018/4)** Let a, b, c be positive integers. Show that if $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ is an integer, then $\sqrt[3]{abc}$ is an integer as well.

[6 ✏] **Problem 11** (RMM TST 2010/1/5) Let a and n be two positive integers such that the prime factors of a are all greater than n. Prove that

$$n! \mid (a - 1)(a^2 - 1) \cdots (a^{n-1} - 1).$$

[6 ✏] **Problem 12** (USAMO 1985/1) Determine whether or not there are any positive integral solutions of the simultaneous equations

$$x_1^2 + x_2^2 + \cdots + x_{1985}^2 = y^3,$$
$$x_1^3 + x_2^3 + \cdots + x_{1985}^3 = z^2$$

with distinct integers $x_1, x_2, \ldots, x_{1985}$.

[9 ⬦] **Problem 13 (USEMO 2020/1)** Which positive integers can be written in the form

$$\frac{\operatorname{lcm}(x, y) + \operatorname{lcm}(y, z)}{\operatorname{lcm}(x, z)}$$

MAST

for positive integers x, y, z?

[9 ⬦] **Problem 14 (China 2015/4)** Determine all integers k such that there exists infinitely many positive integers n not satisfying

$$n + k \mid \binom{2n}{n}.$$

[9 ✎] **Problem 15** (Kosovo 2020/12.4) Let a_0 be a fixed positive integer. We define an infinite sequence of positive integers $\{a_n\}_{n\geq 1}$ in an inductive way as follows: if we are given the terms $a_0, a_1, ...a_{n-1}$, then a_n is the smallest positive integer such that $\sqrt[n]{a_0 \cdot a_1 \cdot ... \cdot a_n}$ is a positive integer. Show that the sequence $\{a_n\}_{n\geq 1}$ is eventually constant.

[9 ✎] **Problem 16** (Dospinescu) Prove that

$$\nu_p \left(2 \cdot \sum_{k=1}^{p-1} \frac{1}{k} + p \cdot \sum_{k=1}^{p-1} \frac{1}{k^2} \right) \geq 4.$$

[9 ✎] **Problem 17** (Alternate Version of Wolstenholme's Theorem) For positive integers a, b and a prime $p > 3$ prove that

$$\nu_p \left(\binom{ap}{bp} - \binom{a}{b} \right) \geq 3.$$

[13 ✎] **Problem 18** (ISL 2013 N4) Determine whether there exists an infinite sequence of nonzero digits $a_1, a_2, a_3, \cdots$ and a positive integer N such that for every integer $k > N$, the number $\overline{a_k a_{k-1} \cdots a_1}$ is a perfect square.

[13 ✎] **Problem 19** (IMO 2015/2) Find all postive integers (a, b, c) such that

$$ab - c, \quad bc - a, \quad ca - b$$

are all powers of 2.

MAST