p-adic Valuation

Number Theory Handout
18 Dec 2022

Let p be a prime number. Given a nonzero integer n, we define the p-adic valuation $v_p(n)$ of n to be the largest integer k such that $p^k \mid n$.

More generally, given a nonzero rational number $\frac{m}{n}$ where $\gcd(m, n) = 1$, we define its p-adic valuation $v_p\left(\frac{m}{n}\right)$ as $v_p(m) - v_p(n)$. However, we will assume the domain of v_p is $\mathbb{N}$ unless stated otherwise.

A few trivial facts:

- $v_p(mn) = v_p(m) + v_p(n)$. (They operate like logarithms)
- $v_p(n) = 0$ if and only if $p \nmid n$.
- $v_p(n) = k$ if and only if $p^k \mid n$ and $p^{k+1} \nmid n$. We write this also as $p^k || n$.
- $v_p(a + b) \geq \min(v_p(a), v_p(b))$. (When is the equality strict?)
- $(a + bp)^k \equiv a^k + ka^{k-1}bp \pmod{p^2}$.

1 Warm Up

1. Denote $s_p(n)$ as the sum of digits of n in base p.

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - s_p(n)}{p - 1}$$

2. Prove that p does not divide $\binom{p^k m}{p^k}$ where $p \nmid m$.

3. Let a and b be integers such that $a \mid b^2, b^3 \mid a^4, a^5 \mid b^6, b^7 \mid a^8, \cdots$. Prove that $a = b$.

4. Prove that for all positive integers a, b, c,

$$\frac{\operatorname{lcm}(a, b, c)^2}{\operatorname{lcm}(a, b) \cdot \operatorname{lcm}(b, c) \cdot \operatorname{lcm}(c, a)} = \frac{\gcd(a, b, c)^2}{\gcd(a, b) \cdot \gcd(b, c) \cdot \gcd(c, a)}$$

2 *Lifting the Exponent* Lemma

We will analyse what $v_p(x^n - y^n)$ is in terms of $x - y$ and n. Turns out that for suitable conditions for x, y, the relation is simple. However, we need to separate into two regimes:

2.1 $p \neq 2$

Theorem 1. Assume $x \equiv y \not\equiv 0 \pmod{p}$. Then for any positive integer n,

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

Proof. We use induction, but first let's settle a large number of cases: If $p \nmid n$, then

$$\frac{x^n - y^n}{x - y} = \sum_{k=0}^{n-1} x^{n-1-k} y^k \equiv \sum_{k=0}^{n-1} x^{n-1-k} x^k \equiv n x^{n-1} \not\equiv 0 \pmod{p}$$

thus $v_p(x^n - y^n) = v_p(x - y)$. Next, we prove that $v_p(x^p - y^p) = v_p(x - y) + 1$. To do this, we prove that $v_p((x^p - y^p)/(x - y)) = 1$. By taking mod p^2 and letting $y = x + pN$,

$$\begin{aligned}
\frac{x^p - y^p}{x - y} &= \sum_{k=0}^{p-1} x^{p-1-k}(x + Np)^k \\
&\equiv \sum_{k=0}^{p-1} x^{p-1-k}(x^k + kx^{k-1}Np) \\
&\equiv \sum_{k=0}^{p-1} (x^{p-1} + Npkx^{p-2}) \\
&\equiv px^{p-1} + Np \cdot \frac{p(p-1)}{2} \cdot x^{p-2} \\
&\equiv px^{p-1} \pmod{p^2}
\end{aligned}$$

and hence this is divisible by p but not p^2 (Where did we use $p \neq 2$?). Finish the proof. □

Theorem 2. Assume $x \equiv -y \not\equiv 0 \pmod{p}$. Then for any **odd** positive integer n,

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

Proof. Analogous to Theorem 1.

2.2 $p = 2$

Theorem 3. Assume $x \equiv y \not\equiv 0 \pmod 2$. Then for any **odd** positive integer n,

$$v_2(x^n \pm y^n) = v_2(x \pm y).$$

Proof. Analogous to the first part of Theorem 1.

Theorem 4. Assume $x \equiv y \not\equiv 0 \pmod 2$. Then for any **even** positive integer n,

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

Proof. It suffices to prove for $n = 2^m$ (Why?):

$$\begin{aligned} v_2\left(x^{2^m} - y^{2^m}\right) &= v_2\left((x - y)\prod_{k=0}^{m-1}\left(x^{2^k} + y^{2^k}\right)\right) \\ &= v_2(x - y) + v_2(x + y) + \sum_{k=1}^{m-1} v_2\left(x^{2^k} + y^{2^k}\right) \\ &= v_2(x - y) + v_2(x + y) + \sum_{k=1}^{m-1} 1 \quad \text{(Why?)} \\ &= v_2(x - y) + v_2(x + y) + m - 1. \end{aligned}$$

□

2.3 Exercises

1. Let $k > 0$ be fixed. Find all $n \in \mathbb{N}$ such that $3^k \mid 2^n - 1$.

2. Prove that if p is an odd prime, $a^p \equiv 1 \pmod{p^n} \Rightarrow a \equiv 1 \pmod{p^{n-1}}$.

3. Find all $x \in \mathbb{N}$ such that $4(x^n + 1)$ is a perfect cube for all $n > 0$.

4. Let $k > 1$ be fixed. Show there are infinitely many n such that

$$n \mid 1^n + 2^n + \cdots + k^n.$$

5. Find all triples (a, b, p) of positive integers with p prime and

$$a^p = b! + p.$$