NTL5 – p-adic Valuation

Definition 10.1 (p-adic Valuation/ Largest Exponent)

Let p be a prime and n be an integer. Then the p-adic valuation of n is defined to be the largest integer t such that $p^t \mid n$.

If we let $2 = p_1 < p_2 < p_3 < \cdots$ be all the primes, then we can write any integer n as

$$n = \prod_{i \geq 0} p_i^{v_{p_i}(n)} = p_1^{v_{p_1}(n)} p_2^{v_{p_2}(n)} \ldots$$

Note.

- *By convention, $v_p(0) = +\infty$*
- *v_p can be positive, 0 or even negative. E.g., $v_7\left(\frac{49}{10}\right) = 2, v_5\left(\frac{20}{15}\right) = 0, v_2\left(\frac{3}{4}\right) = -2$*

Theorem 10.1 (Arithmetic Properties in p-adic Valuation)

Let x, y be integers, $n \in \mathbb{N}$, and p be a prime.

1. (Divisibility) $x \mid y \Leftrightarrow v_p(x) \leq v_p(y)$ *for all primes* p.
2. *(Product)* $v_p(xy) = v_p(x) + v_p(y)$.
3. *(Exponentiation)* $v_p(x^n) = nv_p(x)$.
4. *(Quotient)* $v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y)$
5. *(Sum)* $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, *equality holds if* $v_p(x) \neq v_p(y)$.
   i.e., if $v_p(x) > v_p(y)$ *then* $v_p(x + y) = v_p(y)$
6. *If* $p^n < x < p^{n+1}$, *then* $v_p(x) = n = \lfloor \log_p x \rfloor$.

Example 1. (2007 IMO Shortlist N2) Let $b, n > 1$ be integers. For all $k > 1$, there exists an integer a_k so that $k \mid (b - a_k^n)$. Prove that $b = m^n$ for some integer m.

Theorem 10.2 (GCD and LCM)

Let x, y be integers, for every prime p, we have

$$v_p(\gcd(x, y)) = \min\{v_p(x), v_p(y)\}$$
$$v_p(\text{lcm}[x, y]) = \max\{v_p[x], v_p[y]\}$$

Theorem 10.3 (Legendre's Formula)

For all positive integers n and positive primes p, we have

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Example 2. Show that for any positive integer n,

$$\binom{2n}{n} \mid lcm[1,2,\dots,2n].$$

Definition 10.2 (Base Systems)

Let a and p be positive integers. In base p system, a can be written as

$$a = \sum_{i=0}^{k} (c_i \cdot p^i)$$

Where $p-1 \geq c_k \geq 1$ and $p-1 \geq c_i \geq 0$ for $0 \leq i \leq k-1$

Note.

Sum of digits of a in base p system,

$$s(a) = \sum_{i=0}^{k} (c_i)$$

Theorem 10.4 (Legendre's Formula)

For all positive integers n and positive primes p, we have

$$v_p(n!) = \frac{n - s_p(n)}{p-1}$$

Where, $s_p(n)$ denotes the sum of the digits of n in base p.

Example 3. Prove Legendre's Formula (Theorem 10.3).

Example 4. (Canada) Find all positive integers n such that $2^{n-1} \mid n!$.