Some useful p-adic formulas

Lemma. *Write $n_0 + n_1 p + n_2 p^2 + \dots$ for the p-adic expansion of an integer $n \geqslant 1$. Then we have the following statements about p-adic valuations and residues:*

(1) *The valuation of $n!$ is*

$$v(n!) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - (n_0 + n_1 + n_2 + \dots)}{p-1}.$$

(2) *If $v = v(n!)$ then the leading term in the p-adic expansion of $n!$ is*

$$(-1)^v n_0!\, n_1!\, n_2! \dots p^v.$$

(3) *The valuation of the binomial coefficient $\binom{n}{k}$ is the sum of the carry overs in the addition of k and $n-k$.*

(4) *If $\binom{n}{k}$ is prime to p then its mod p residue is $\binom{n_0}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2}\dots$*

(5) *The valuation of the binomial coefficient $\binom{p^n}{k}$ is $n - v(k)$, for $k \geqslant 1$.*

Proof: (1) Say that $n = n_0 + n_1 p + \dots + n_r p^r$. There are $\lfloor n/p^k \rfloor$ integers $m \leqslant n$ divisible by p^k and $\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor$ integers $m \leqslant n$ of valuation k. It follows that

$$v(n!) = \sum_{k \geqslant 1} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Using the fact that $\lfloor n/p^k \rfloor = \sum_{i \geqslant k} n_i p^{i-k}$, we derive the formula

$$v(n!) = \frac{n - (n_0 + n_1 + \dots + n_r)}{p-1}.$$

(2) See also [Ha], chapter 17, § 3. For a finite set M of positive integers, let $M!$ be the product of the elements of M and write the p-adic leading term of $M!$ in the form $\mu(M) p^{v(M!)}$. Thus, we want to prove that $\mu(\{1, \dots, n\}) = (-1)^{v(n!)} n_0! \dots n_r!$. For this, it is enough to produce a partition $\{1, \dots, n\} = A_0 \sqcup \dots \sqcup A_r$ such that

$$\mu(A_i) = (-1)^{n_i \frac{p^i - 1}{p-1}} n_i!.$$

Call A_i the set of integers $m \in \{1, \dots, n\}$ such that $m_{i+1} = n_{i+1}, \dots, m_r = n_r$ and either $v(m) = i$ or $m_i < n_i$. This is a partition because n is in $A_{v(n)}$ and no other, while if $m < n$, there is a maximal i such that $m_i < n_i$ and then m is in A_i and no other. The integers $m \in A_i$ with valuation i are determined by their i-th digit which satisfies $1 \leqslant m_i \leqslant n_i$ and they contribute to $\mu(A_i)$ by a factor $n_i!$. The integers $m \in A_i$ with valuation $k < i$ are determined by their k-th to i-th digits which satisfy $1 \leqslant m_k \leqslant p-1$, $0 \leqslant m_j \leqslant p-1$ for $k < j < i$, and $0 \leqslant m_i \leqslant n_i - 1$. Using the fact that $(p-1)! \equiv -1 \mod p$, an immediate computation shows that these m contribute to $\mu(A_i)$ by a factor $(-1)^{n_i p^{i-k-1}}$. Finally the value for $\mu(A_i)$ is as announced.

(3) Let $k = k_0 + k_1 p + \cdots + k_r p^r$ and $l = n - k = l_0 + l_1 p + \cdots + l_r p^r$. Run the p-adic addition algorithm to add up k and l:

$$\begin{aligned}
&k_0 + l_0 = n_0 + \delta_0 p && \text{with } \delta_0 \in \{0,1\},\\
&k_1 + l_1 + \delta_0 = n_1 + \delta_1 p && \text{with } \delta_1 \in \{0,1\},\\
&\quad\vdots && \quad\vdots\\
&k_r + l_r + \delta_{r-1} = n_r + \delta_r p && \text{with } \delta_r \in \{0,1\},\\
&n_{r+1} = \delta_r
\end{aligned}$$

where $\delta_0, \ldots, \delta_r$ are the carry overs. Then the formula in (1) implies that $(p-1)$ times the valuation of $\binom{n}{k} = \frac{n!}{k!\,l!}$ is equal to

$$n - (n_0 + \cdots + n_{r+1}) - k + (k_0 + \cdots + k_r) - l + (l_0 + \cdots + l_r) = (p-1)(\delta_0 + \cdots + \delta_r).$$

(4) By what we have just proved, $\binom{n}{k}$ is prime to p if and only if there are no nonzero carry overs. If this holds, then $n_i = k_i + l_i$ for all i. Then the leading term in the p-adic expansion of the binomial coefficient, which in the present case is also the p-adic residue, is

$$\frac{n_0! \ldots n_r!}{k_0! \ldots k_r!\, l_0! \ldots l_r!} = \binom{n_0}{k_0} \cdots \binom{n_r}{k_r}.$$

(5) If $k = p^n$, the result is clear. If $1 \leqslant k \leqslant p^n$, we have $v(p^n - k) = v(k)$. So taking valuations in the equality

$$k! \binom{p^n}{k} = p^n (p^n - 1) \ldots (p^n - (k-1))$$

gives $v(k!) + v\left(\binom{p^n}{k}\right) = n + v((k-1)!)$, whence the result. □

References

[Ha] H. Hasse, *Number theory*, Classics in Mathematics, Springer-Verlag (2002).