BINOMIAL COEFFICIENTS AND p-ADIC LIMITS

KEITH CONRAD

Look at the power series for $\sqrt{1+x}$, $\sqrt[3]{1+x}$, and $\sqrt[6]{1+x}$ at $x=0$:

$$\begin{aligned}
\sqrt{1+x} &= 1+\frac{1}{2}x-\frac{1}{8}x^2+\frac{1}{16}x^3-\frac{5}{128}x^4+\frac{7}{256}x^5-\frac{21}{1024}x^6+\cdots, \\
\sqrt[3]{1+x} &= 1+\frac{1}{3}x-\frac{1}{9}x^2+\frac{5}{81}x^3-\frac{10}{243}x^4+\frac{22}{729}x^5-\frac{154}{6561}x^6+\cdots, \\
\sqrt[6]{1+x} &= 1+\frac{1}{6}x-\frac{5}{72}x^2+\frac{55}{1296}x^3-\frac{935}{31104}x^4+\frac{4301}{186624}x^5-\frac{124729}{6718464}x^6+\cdots.
\end{aligned}$$

It appears that the Taylor coefficients are all rational. Now look at their denominators. In $\sqrt{1+x}$ each coefficient has denominator that is a power of 2, in $\sqrt[3]{1+x}$ each coefficient has denominator that is a power of 3 ($243=3^5$ and $729=3^6$), and in $\sqrt[6]{1+x}$ each coefficient is a power of 2 times a power of 3 ($1296=2^43^4$, $31104=2^73^5$, $186624=2^83^6$, and $6718464=2^{10}3^8$). We will show the power series of $\sqrt[n]{1+x}$ at $x=0$ has rational Taylor coefficients and the prime factors of the denominators of the coefficients divide n.

It is not hard to get a formula for the coefficients in $\sqrt[n]{1+x}=(1+x)^{1/n}$: the coefficient of x^k is

$$\frac{d^k}{dx^k}(1+x)^{1/n}=\frac{1}{n}\left(\frac{1}{n}-1\right)\left(\frac{1}{n}-2\right)\cdots\left(\frac{1}{n}-(k-1)\right)(1+x)^{1/n-k}$$

so the coefficient of x^k is

$$\left.\frac{(\sqrt[n]{1+x})^{(k)}}{k!}\right|_{x=0}=\frac{(1/n)(1/n-1)\cdots(1/n-(k-1))}{k!}=\binom{1/n}{k}.$$

These numbers for $k\geq 0$ are all rational. They are binomial coefficients evaluated at $1/n$.

For $r\in\mathbf{Q}$ the power series for $(1+x)^r$ at $x=0$ has coefficients that are binomial coefficients evaluated at r:

$$(1+x)^r=\sum_{k\geq 0}\frac{r(r-1)(r-2)\cdots(r-(k-1))}{k!}x^k=\sum_{k\geq 0}\binom{r}{k}x^k.$$

What primes occur in the denominators of $\binom{r}{k}$? Writing $r=a/b$ in reduced form,

$$\binom{a/b}{k}=\frac{(a/b)(a/b-1)(a/b-2)\cdots(a/b-(k-1))}{k!}=\frac{a(a-b)(a-2b)\cdots(a-kb)}{b^kk!}$$

and it is obvious that the only possible primes in the denominator are prime factors of b or a prime factor of $k!$. It is true, but not at all clear, that only prime factors of b matter: a prime factor of $k!$ that is not a factor of b gets completely canceled out when the ratio in $\binom{r}{k}$ is simplified. We will explain this purely algebraic phenomenon by using p-adic limits!

Theorem 1. *For rational r, a prime dividing the denominator of $\binom{r}{k}$ must divide the denominator of r. In particular, a prime dividing the denominator of $\binom{1/n}{k}$ must divide n.*

Proof. To prove the theorem we will prove the contrapositive: each prime p that does *not* divide the denominator of r also does not divide the denominator of $\binom{r}{k}$. Expressed in terms of p-adic absolute values, this says: if $|r|_p \leq 1$ then $|\binom{r}{k}|_p \leq 1$ for $k \geq 0$. To prove this, observe that the expression

$$\binom{x}{k} = \frac{x(x-1)(x-2)\cdots(x-(k-1))}{k!}$$

is a polynomial in x with rational coefficients, so it is a *continuous function* $\mathbf{Q} \to \mathbf{Q}$ when $\mathbf{Q}$ has the p-adic topology just as it is a continuous function $\mathbf{Q} \to \mathbf{Q}$ when $\mathbf{Q}$ has its usual real topology. (For every field F and absolute value $|\cdot|$ on F, polynomials with coefficients in F are continuous functions $F \to F$ with respect to $|\cdot|$.) When $|r|_p \leq 1$, r is a p-adic limit of nonnegative integers: writing $r = a/b$ with $p \nmid b$, for each $i \geq 1$ we can solve $bm_i \equiv a \bmod p^i$ for an integer m_i, so $|r - m_i|_p = |a/b - m_i|_p = |(a - bm_i)/b|_p = |a - bm_i|_p \leq 1/p^i$. Thus $r = \lim_{i\to\infty} m_i$ where the limit is using the p-adic absolute value. By p-adic continuity of the polynomial function $\binom{x}{k}$,

$$\binom{r}{k} = \lim_{i\to\infty} \binom{m_i}{k}.$$

Each $\binom{m_i}{k}$ is in $\mathbf{Z}$ since binomial coefficients with nonnegative integers upstairs are integers ($\binom{m_i}{k} = 0$ if $0 \leq m_i < k$ and $\binom{m_i}{k} \in \mathbf{Z}^+$ if $m_i \geq k$, by combinatorics). Thus $|\binom{m_i}{k}|_p \leq 1$ for each i, so taking a p-adic limit of $\binom{m_i}{k}$ tells us $|\binom{r}{k}|_p \leq 1$. □

Example 2. When the binomial coefficient $\binom{33/20}{7}$ is expanded out and simplified, the denominator can only have prime factors 2 and 5. Explicitly,

$$\binom{33/20}{7} = -\frac{352590381}{102400000000} = -\frac{352590381}{2^{18}5^8}.$$

The theorem we proved admits a converse.

Theorem 3. *Each prime p that divides the denominator of r also divides the denominator of every $\binom{r}{k}$ for $k \geq 1$.*

Proof. Let's reformulate the theorem in terms of p-adic absolute values: if $|r|_p > 1$ then $|\binom{r}{k}|_p > 1$ for all $k \geq 1$. (This is not true for $k = 0$.) The top of $\binom{r}{k}$ is $r(r-1)\cdots(r-(k-1))$, and for each positive integer j we have $|r - j|_p = |r|_p$ since $|r|_p > 1 \geq |j|_p$ so

$$\begin{aligned}
\left|\binom{r}{k}\right|_p &= \left|\frac{r(r-1)(r-2)\cdots(r-(k-1))}{k!}\right| \\
&= \frac{|r|_p|r-1|_p|r-2|_p\cdots|r-(k-1)|_p}{|k!|_p} \\
&= \frac{|r|_p^k}{|k!|_p} \\
&= |r|_p^k\, p^{\mathrm{ord}_p(k!)} \\
&\geq |r|_p^k \\
&> 1.
\end{aligned}$$

□

Example 4. Every Taylor coefficient of $\sqrt[6]{1+x}$ besides the constant term must have its reduced form denominator divisible by 2 and by 3; it can never be a power of just one of those primes.