P-adic Lifting the Exponent Lemma

Merosity

1 P-adic Lifting the Exponent Lemma

Here we'll derive a general version of the LTE in the p-adic setting. To really get to the crux of the issue, we formulate it for $|z| < r_p$ and $|n| \leq 1$, here $r_p = p^{\frac{-1}{p-1}}$.

$$(1+z)^n - 1 = \sum_{k \geq 1} \binom{n}{k} z^k$$

Now we just need to show that the $k = 1$ term dominates in the ultrametric inequality. Writing in terms of the falling factorial,

$$\left| \binom{n}{k} z^k \right| = \left| \frac{n^{\underline{k}}}{k!} z^k \right| \leq \left| n \frac{z^k}{k!} \right|$$

To move forward we have to recognize Legendre's formula, where v is the p-adic valuation and s is the sum of digits in base p.

$$v(k!) = \frac{k - s(k)}{p-1}$$

For $k \geq 1$ we have $s(k) \geq 1$ and so we have,

$$|k!| = r_p^{k - s_p(k)} \geq r_p^{k-1}$$

$$\left| n \frac{z^k}{k!} \right| = \left(\frac{|z|}{r_p} \right)^{k-1} |nz| < |nz|$$

This means we have firmly established that the $k = 1$ term is strictly larger than all further terms p-adically.

$$|(1+z)^n - 1| = |nz|$$

When $|n| > 1$ we can do a similar analysis, which puts a different condition on z.

$$\left| \binom{n}{k} z^k \right| = \left| \frac{n^{\underline{k}}}{k!} z^k \right| = \left| \frac{(nz)^k}{k!} \right|$$

This means we need $|z| < \frac{r_p}{|n|}$ since it converges like the exponential series, and so the exact same result holds. So we can safely extend the theorem to be:

For $|z| < \frac{r_p}{\max(1,|n|)}$, $|(1+z)^n - 1| = |nz|$.

1.1 Standard Cases

We can now reacquire the standard version of the lifting the exponent lemma by simply letting $1 + z = \frac{x}{y}$ with $|x| = |y| = 1$, so long as $\left(\frac{x}{y}\right)^n = \frac{x^n}{y^n}$ makes sense.

$$\left| \left(\frac{x}{y}\right)^n - 1 \right| = |n| \left| \frac{x}{y} - 1 \right|$$

$$|x^n - y^n| = |n||x - y|$$

Notice now however we have a much stronger theorem than we did previously, since n can be any p-adic integer.

Now what about the case when $p = 2$? In this case we have points that lie outside the ball where it's injective, $r_2 = \frac{1}{2}$ and if we're only focusing on powers of a prime, we have to do a special argument. In general for any finite extension of $\mathbb{Q}_p$ we will have to do an argument of this nature for the special case, as it is entirely cirucmstantial how many terms can compete depending on how close to $|z| = 1$ we are where the series diverges.

In the 2-adic case $|x - y| \leq \frac{1}{2}$ implies $|x + y| \leq \frac{1}{2}$ and so together we have $|x^2 - y^2| < r$. Now we can apply the regular version of the lemma when n is even, writing $n = 2m$

$$|x^n - y^n| = |x^{2m} - y^{2m}| = |m||x^2 - y^2| = |n| \left| \frac{x^2 - y^2}{2} \right|$$

This still leaves the case when $|z| = 1/2$ and $|n| = 1$. This is easy from the series perspective since the first two terms $|nz + n\frac{n-1}{2}z^2| = |nz|$ and so overpower the further terms (I believe).