Strassmann's theorem

Strassmann's theorem really highlights the differences between real and p-adic analysis. It also has applications in scenarios you really wouldn't expect such a result to come in useful. Its proof is fairly simple, but needs the following lemma.

Lemma. *Let k be a field which is complete with respect to the non-archimedean valuation $|\cdot|$. Let $b_{ij} \in k$ for $i, j = 0, 1, 2, \ldots$. Suppose that for every $\varepsilon > 0$ there is a $J(\varepsilon)$ such that $|b_{ij}| < \varepsilon$ whenever $\max(i, j) \geqslant J(\varepsilon)$. Then the series*

$$\sum_i \left(\sum_j b_{ij} \right) \qquad \textit{and} \qquad \sum_j \left(\sum_i b_{ij} \right)$$

both converge, and are equal.

Proof. Remember that in the non-archimedean case a series converges if and only if the terms being summed tend to zero. We have that $b_{ij} \to 0$ so

$$\sum_j b_{ij} \qquad \text{and} \qquad \sum_i b_{ij}$$

both converge. And using the ultrametric inequality we have

$$\left| \sum_j b_{ij} \right| \leqslant \max_j |b_{ij}| \xrightarrow{i \to \infty} 0,$$

so that the first double sum converges, and similarly for the second one.

We now note that for finite sums the rearrangement of i and j does not matter, in particular we have

$$\sum_{i=0}^{J(\varepsilon)} \left(\sum_{j=0}^{J(\varepsilon)} b_{ij} \right) = \sum_{j=0}^{J(\varepsilon)} \left(\sum_{i=0}^{J(\varepsilon)} b_{ij} \right).$$

Again using the ultrametric inequality we have

$$\begin{aligned} \left| \sum_{i=0}^{J(\varepsilon)} \left(\sum_{j=0}^{J(\varepsilon)} b_{ij} \right) - \sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} b_{ij} \right) \right| &= \left| \sum_{\max(i,j) > J(\varepsilon)} \sum_i \sum_j b_{ij} \right| \\ &\leqslant \max_{\substack{i,j, \text{ s.t.} \\ \max(i,j) > J(\varepsilon)}} |b_{ij}| \\ &< \varepsilon. \end{aligned}$$

And similarly with the i and j exchanged. Hence

$$\left|\sum_i\left(\sum_j b_{ij}\right)-\sum_j\left(\sum_i b_{ij}\right)\right| = \left|\sum_i\left(\sum_j b_{ij}\right)-\sum_{i=0}^{J(\varepsilon)}\left(\sum_{j=0}^{J(\varepsilon)} b_{ij}\right)+\sum_{j=0}^{J(\varepsilon)}\left(\sum_{i=0}^{J(\varepsilon)} b_{ij}\right)-\sum_j\left(\sum_i b_{ij}\right)\right|$$

$$\leqslant \max\left\{\left|\sum_{i=0}^{J(\varepsilon)}\left(\sum_{j=0}^{J(\varepsilon)} b_{ij}\right)-\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right|,\right.$$

$$\left.\left|\sum_{j=0}^{J(\varepsilon)}\left(\sum_{i=0}^{J(\varepsilon)} b_{ij}\right)-\sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right|\right\}$$

$$< \varepsilon.$$

Hence the two series are equal. □

So not only is it much easier to tell if a single series converges p-adically, it's also much easier to deal with double sums. Which is nice. Now we have the above result we can prove Strassmann's theorem.

Strassmann's theorem. *Let the field k be complete with respect to the non-archimedean valuation $|\cdot|$, and let*

$$f(X)=\sum_{n=0}^{\infty} f_n X^n.$$

Suppose that $f_n \to 0$ but that not all the f_n are zero. Then there are at most a finite number of $b \in \mathcal{O}_k$ such that $f(b)=0$. More precisely, there are at most N such b where N is defined by

- $|f_N| = \max|f_n|$,
- $|f_n| < |f_N|$ *for all* $n > N$.

That is, N is the index of the last maximal coefficient.

So in particular we're concerned with the case $k=\mathbb{Q}_p$, $\mathcal{O}_k=\mathbb{Z}_p$, $|\cdot| = |\cdot|_p$. Compare the above situation with the power series for sine and cosine, say, which satisfy all the hypotheses over $\mathbb{R}$ but which have infinitely many zeroes. This can't happen in $\mathbb{Q}_p$. The proof of Strassmann's theorem is by induction on N.

Proof. Suppose $N=0$. If the theorem is true there will be no zeros of f in the ring of integers, so assume that there is a $b \in \mathcal{O}_k$ with $f(b)=0$. So we have

$$f_0 = -\sum_{n\geqslant 1} f_n b^n.$$

But using the ultrametric inequality and the fact that $|f_n| < |f_0|$ for all $n > 0$ we have

$$\left|\sum_{n\geqslant 1} f_n b^n\right| \leqslant \max_{n\geqslant 1} |f_n b^n| \leqslant \max_{n\geqslant 1} |f_n| < |f_0|$$

which is a contradiction. So no such b exists.

Now consider the situation for some $N > 0$. Suppose $f(b) = 0$ for some $b \in \mathcal{O}_k$, and let $c \in \mathcal{O}_k$. Then

$$\begin{aligned} f(c) = f(c) - f(b) &= \sum_{n\geqslant 1} f_n \left(c^n - b^n\right) \\ &= (c-b) \sum_{n\geqslant 1} \sum_{j=1}^{n-1} f_n c^j b^{n-1-j}. \end{aligned}$$

By the lemma we may rearrange this double sum as

$$\begin{aligned} f(c) &= (c-b) \sum_{j=1}^{\infty} \sum_{n>j} f_n b^{n-1-j} c^j \\ &= (c-b) \sum_{j=1}^{\infty} c^j \sum_{r\geqslant 0} f_{j+1+r} b^r. \end{aligned}$$

Let

$$g(X) = \sum_{j\geqslant 1} g_j X^j$$

where

$$g_j = \sum_{r\geqslant 0} f_{j+1+r} b^r,$$

then

$$f(c) = (c-b)g(c).$$

Now, for all j we have

$$\begin{aligned} |g_j| &= \left|\sum_{r\geqslant 0} f_{j+1+r} b^r\right| \\ &\leqslant \max_{r\geqslant 0} |f_{j+1+r} b^r| \\ &\leqslant \max_{r\geqslant 0} |f_{j+1+r}| \\ &\leqslant |f_N|. \end{aligned}$$

We also have

$$\begin{aligned} |g_{N-1}| &= \left| \sum_{r \geqslant 0} f_{N+r} b^r \right| \\ &= \left| f_N + f_{N+1} b + f_{N+2} b^2 + \ldots \right| \\ &= |f_N|. \end{aligned}$$

Finally for $j > N-1$ we have

$$\begin{aligned} |g_j| &\leqslant \max_{r \geqslant 0} |f_{j+1+r}| \\ &< |f_N|. \end{aligned}$$

So $g(X)$ satisfies the hypotheses of the theorem but with $N-1$ instead of N, so by the inductive hypothesis $g(X)$ has at most $N-1$ zeros $c \in \mathcal{O}_k$. But $f(c) = 0$ implies that either $c = b$ or $g(c) = 0$, so that $f(X)$ has at most N zeros, as required. □

Strassmann's theorem has several surprising corollaries, including the following two results.

Corollary. *Suppose that $f(X)$ and $g(X)$ both converge in $\mathcal{O}_k$ and that $f(b) = g(b)$ for infinitely many $b \in \mathcal{O}_k$. Then $f(X)$ and $g(X)$ have the same coefficients.*

Proof. We have $f(b) - g(b) = 0$ for infinitely many $b \in \mathcal{O}_k$, so the power series of $f - g$ must have all zero coefficients, so f and g have the same coefficients. □

Corollary. *Suppose that k has characteristic 0. Let $f(X)$ be a power series that converges in $\mathcal{O}_k$, and suppose further that $f(X+d) = f(X)$ for some $d \in \mathcal{O}_k$. Then $f(X)$ is constant.*

Proof. The function $f(X) - f(0)$ has infinitely many zeros in $\mathcal{O}_k$ at md for $m \in \mathbb{Z}$. So $f(X)$ and $f(0)$ have the same coefficients, i.e. $f(X) = f_0$. □

This second corollary tells us that a non-constant periodic function cannot be represented by a power series in the p-adic world.

Whilst Strassmann's theorem seems useful if we want to count the zeros of a given power series, it doesn't have immediately obvious applications beyond that. However it can have powerful applications to Diophantine equations, but to use it we need the following lemma which allows us to convert the expression $(1 + x)^n$ into a power series in n.

Lemma. *Let $b \in \mathbb{Q}_p$ and suppose that*

$$\begin{array}{ll} |b|_p \leqslant 2^{-2} & \text{if } p = 2; \\ |b|_p \leqslant p^{-1} & \text{otherwise.} \end{array}$$

Then there is a power series

$$\Phi_b(x) = \sum_{n=0}^{\infty} \gamma_n x^n,$$

where

$$\gamma_n \in \mathbb{Q}_p, \qquad \gamma_n \to 0$$

such that

$$(1+b)^r = \Phi_b(r)$$

for all $r \in \mathbb{Z}$.

Provided $b \neq -1$ the power series Φ_b is vulnerable to attack by Strassmann's theorem, which means we can now also count the number of zeros of expressions like $f(x) = (1+a)^x$. This will be fully exploited in the following lemma.

Lemma (Nagell)**.** *Let u_n be defined by $u_0 = 0$, $u_1 = 1$, and*

$$u_n = u_{n-1} - 2u_{n-2} \quad (n \geqslant 2).$$

Then $u_n = \pm 1$ only for $n = 1, 2, 3, 5,$ and 13.

Proof. Let $U(z)$ be the generating function of this sequence, so

$$U(z) = \sum_{n=0}^{\infty} u_n z^n.$$

We can write the recurrence relation for *all* n as

$$u_n = u_{n-1} - 2u_{n-2} + [n = 1]$$

where

$$[P(n)] = \begin{cases} 1 & \text{if } P(n) \text{ is true} \\ 0 & \text{if } P(n) \text{ is false} \end{cases}$$

for any proposition P. Multiplying the recurrence by z^n and summing over n gives

$$\sum_n u_n z^n = \sum_n u_{n-1} z^n - 2 \sum_n u_{n-2} z^n + z,$$

which can be written as

$$U(z) = zU(z) - 2z^2 U(z) + z.$$

So we have

$$U(z) = \frac{z}{1 - z + 2z^2}.$$

Writing $U(z)$ with partial fractions and then differentiating we have

$$\frac{\mathrm{d}^n}{\mathrm{d}z^n}U(z) = \frac{n!}{2(\alpha-\beta)}\left(\frac{(-1)^n\alpha}{(z-\alpha)^{n+1}} - \frac{(-1)^n\beta}{(z-\beta)^{n+1}}\right),$$

where α and β are the roots of $2z^2 - z + 1 = 0$. Since U is the generating function of u_n we have

$$u_n = \frac{1}{n!}\frac{\mathrm{d}^n}{\mathrm{d}z^n}U(z)\bigg|_{z=0} = \frac{a^n - b^n}{a-b},$$

where a, b are the roots of $x^2 - x + 2 = 0.$, i.e.

$$a = \frac{1}{2}(1 + i\sqrt{7}) \qquad b = \frac{1}{2}(1 - i\sqrt{7}).$$

However, there is no reason to work in $\mathbb{C}$. We may also work in any p-adic field $\mathbb{Q}_p$ for which the polynomial

$$f(x) = x^2 - x + 2$$

splits. Note that $f'(x) = 2x - 1$. If we work in $\mathbb{Q}_{11}$ then we find that

$$\begin{aligned} f(5) &\equiv 0 \pmod{11} \\ f'(5) &\equiv 9 \not\equiv 0 \pmod{11} \end{aligned}$$

$$\begin{aligned} f(7) &\equiv 0 \pmod{11} \\ f'(7) &\equiv 2 \not\equiv 0 \pmod{11}. \end{aligned}$$

So by Hensel's lemma we get two solutions a, b in $\mathbb{Z}_{11}$, which we can work out satisfy

$$\begin{aligned} \alpha &\equiv 16 \pmod{11^2} \\ \beta &\equiv 106 \pmod{11^2}. \end{aligned}$$

We are essentially trying to count the number of zeros of the function $u_n \pm 1$, and we now have a p-adic expression for u_n with n appearing as an exponent, so it looks as though we're ready to apply the previous lemma. But alack and alas the hypotheses of that lemma aren't satisfied yet, we still need to massage our numbers into the right form. So we first consider the numbers A and B which, using Fermat's little theorem, satisfy

$$\begin{aligned} A = \alpha^{10} &\equiv 1 \pmod{11} \\ B = \beta^{10} &\equiv 1 \pmod{11}. \end{aligned}$$

Then $A - 1$ and $B - 1$ both satisfy the hypotheses of the previous lemma, so we can expand A^n and B^n as power series in n. To simplify matters for ourselves we first write

$$n = r + 10s \qquad 0 \leqslant r \leqslant 9,$$

so that

$$u_n = u_{r+10s} = \frac{\alpha^{r+10s} - \beta^{r+10s}}{\alpha - \beta} = \frac{\alpha^r A^s - \beta^r B^s}{\alpha - \beta}.$$

And since $A \equiv B \equiv 1 \pmod{11}$ we can see from this that

$$u_{r+10s} \equiv u_r \pmod{11}.$$

Looking at the first ten values of the sequence we have:

n	0	1	2	3	4	5	6	7	8	9
u_n	0	1	1	-1	-3	-1	5	7	-3	-17

So the only r we have to consider are $r = 1, 2, 3, 5$. For these values of r we have

r	$\alpha^r \pmod{11^2}$	$\beta^r \pmod{11^2}$
1	16	106
2	14	104
3	103	13
5	111	21
10	100	78

The final row is for reference so we know what A and B are mod 121. If we now write

$$\alpha^{10} = A = 1 + a \qquad \beta^{10} = B = 1 + b,$$

so we have

$$a \equiv 99 \pmod{11^2} \qquad b \equiv 77 \pmod{11^2}$$

and then we can use the previous lemma to develop the expression

$$(\alpha - \beta)(u_{r+10s} \mp 1) = \alpha^r(1 + a)^s - \beta^r(1 + b)^s \mp (\alpha - \beta)$$

as a power series in s, say

$$(\alpha - \beta)(u_{r+10s} \mp 1) = c_0 + c_1 s + c_2 s^2 + \ldots$$

For the "$\mp$" we take the upper sign for $r = 1, 2$ and the lower one for $r = 3, 5$. Plugging in $s = 0$ and the correct sign for each r we find that $c_0 = 0$ in all four cases. Since

$$(1 + x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k$$

and both $a \equiv b \equiv 0 \pmod{11}$ we will have

$$c_j \equiv 0 \pmod{11^2}$$

for every $j \geqslant 2$. Whereas for $r = 1, 2, 5$ we can use the table above to see that

$$c_1 \equiv \alpha^r a - \beta^r b \pmod{11^2}$$
$$\not\equiv 0 \pmod{11^2}.$$

Thus, by Strassmann's theorem the above series has at most one zero when $r = 1, 2, 5$, and since we know it has a zero at $s = 0$ there can be no others.

For $r = 3$ we have $c_1 \equiv 0 \pmod{11^2}$ so we can't immediately apply Strassmann's theorem. But if estimate the c_j more carefully we see that

$$2 \cdot 11^{-2} c_2 \equiv \alpha^3 (a/11)^2 - \beta^3 (b/11)^2 \equiv 6 \pmod{11},$$

so that

$$c_2 \not\equiv 0 \pmod{11^3}.$$

But $c_j \equiv 0 \pmod{11^3}$ for every $j \geqslant 3$, so Strassmann's theorem tells us that our series can vanish for at most two values of s. But we know that it vanishes at $s = 0$ and $s = 1$, so we have all the zeros. Thus $u_n \pm 1$ vanishes only at the values $n = 1, 2, 3, 5, 13$. □

The fact we can calculate explicitly how many times the above recurrence hits ± 1 is pretty impressive, though perhaps not immediately useful. Nagell didn't investigate this recurrence just for fun though, he used it to solve a particular Diophantine equation:

Corollary. *The only solutions of*

$$x^2 + 7 = 2^m$$

in integers x and m have $m = 3, 4, 5, 7, 15$.

Proof. Clearly x must be odd, say $x = 2y - 1$ with $y \in \mathbb{Z}$. Then the equation becomes

$$y^2 - y + 2 = 2^{m-2}.$$

If we let α be a root of $z^2 - z + 2$ then the ring $\mathbb{Z}[\alpha]$ is a UFD[1]. If we let the conjugate root be β then we have $\alpha\beta = 2$, so splitting the above equation over $\mathbb{Z}[\alpha]$ and using the fact it's a UFD gives

$$(y - \alpha)(y - \beta) = \alpha^{m-2}\beta^{m-2}$$

so that

$$y - \alpha = \alpha^{m-2} \qquad y - \beta = \beta^{m-2}$$

or

$$y - \alpha = \beta^{m-2} \qquad y - \beta = \alpha^{m-2}$$

Either way we have

$$\alpha - \beta = \pm(\alpha^{m-2} - \beta^{m-2})$$

and so solutions to our original equation can only come about for values of $n = m-2$ for which

$$\frac{\alpha^n - \beta^n}{a - b} = \pm 1.$$

But by the previous lemma this can only occur when $n = 1, 2, 3, 5, 13$, and hence the result follows. □

[1]It has a Euclidean algorithm, hence is a PID, and hence is a UFD.

So the complete set of solutions to

$$x^2 + 7 = 2^m$$

is

$$(x, m) = (\pm 1, 3), (\pm 3, 4), (\pm 5, 5), (\pm 11, 7), (\pm 181, 15).$$

Hopefully this result shows the hidden power of Strassmann's theorem. The following exercises are in the vein of Nagell's lemma.

1. Define the sequence u_n by $u_0 = 1$, $u_1 = 2$, and

$$u_n = 3u_{n-1} - 5u_{n-2}.$$

Show that $u_n = 1$ only for $n = 0, 2, 6$. (Hint: Work in $\mathbb{Q}_3$.)

2. Let $u_0 = 0$, $u_1 = 1$, and

$$u_n = 3u_{n-1} - 7u_{n-2}.$$

Find the smallest $m > 0$ such that

$$u_m \equiv 0 \pmod{5^4}.$$

Exposition and exercises mostly follow Cassels' Local Fields.