Differentiating by prime numbers

Jack Jeffries *

It is likely a fair assumption that you, the reader, are not only familiar with but even quite adept at differentiating by x. What about differentiating by 13? That certainly didn't come up in my calculus class! From a calculus perspective, this is ridiculous: are we supposed to take a limit as 13 changes?

[Joy85] André Joyal, *δ-anneaux et vecteurs de Witt*, C. R. Math. Rep. Acad. Sci. Canada **7** (1985), no. 3, 177–182. MR789309

[Bui96] ______, *Geometry of p-jets*, Duke Math. J. **82** (1996), no. 2, 349–367. MR1387233

Alexandru Buium

arXiv:2311.13551 [math.HO]

Speaker: Maxim Bezuglov

Let p be a prime number. By Fermat's little theorem, for any integer n, we have

$$n \equiv n^p \mod p,$$

so we can divide the difference $n - n^p$ by p. The starting point of our journey is that not only *can* we divide by p here, but we *should*. The p-derivation on $\mathbb{Z}$ is the result of this process. Namely:

Definition 1 *For a prime number p, the p-*derivation *on $\mathbb{Z}$ is defined as the function $\delta_p : \mathbb{Z} \to \mathbb{Z}$ given by the formula*

$$\delta_p(n) = \frac{n - n^p}{p}.$$

n	$\delta_2(n)$	$\delta_3(n)$	$\delta_5(n)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
-4	-10	20	204
-3	-6	8	48
-2	-3	2	6
-1	-1	0	0
0	0	0	0
1	0	0	0
2	-1	-2	-6
3	-3	-8	-48
4	-6	-20	-204
5	-10	-40	-624
6	-15	-70	-1554
$\vdots$	$\vdots$	$\vdots$	$\vdots$

A quick look at this table suggests a few observations, easily verified from the definition:

- Numbers are no longer "constants" in the sense of having derivative zero, but at least 0 and 1 are.
- These functions are neither additive nor multiplicative, e.g.:

$$\delta_p(1) + \delta_p(1) \neq \delta_p(2),$$

$$\delta_p(1)\delta_p(2) \neq \delta_p(2).$$

- δ_p is an odd function, at least for $p \neq 2$.
- The outputs of δ_2 are just the negatives of the triangular numbers.

Comparison 1 (Order-decreasing property)

- *If $f \in \mathbb{R}[x]$ is a polynomial and $x = r$ is a root of f of multiplicity $a > 0$, then $x = r$ is a root of the polynomial $\frac{d}{dx}(f(x))$ of multiplicity $a - 1$.*
- *If n is an integer and p is a prime factor of n of multiplicity $a > 0$, then p is a prime factor of the integer $\delta_p(n)$ of multiplicity $a - 1$.*

Comparison 2 (Sum and product rules)

- *For polynomials $f(x), g(x)$, one can compute each of $\frac{d}{dx}(f+g)$ and $\frac{d}{dx}(fg)$ as a fixed polynomial expression in the inputs $f, g, \frac{d}{dx}(f), \frac{d}{dx}(g)$, namely $\frac{d}{dx}(f+g) = \frac{d}{dx}(f) + \frac{d}{dx}(g)$ and $\frac{d}{dx}(fg) = f\frac{d}{dx}(g) + g\frac{d}{dx}(f)$.*
- *For integers m, n, one can compute each of $\delta_p(m+n)$ and $\delta_p(mn)$ as a fixed polynomial expression in the inputs $m, n, \delta_p(m), \delta_p(n)$, namely $(+)$ and $(\times)$.*

Theorem 1 (Buium [Bui97]**)** *Any function $\delta : \mathbb{Z} \to \mathbb{Z}$ that satisfies*

- *a sum rule $\delta(m+n) = S(m, n, \delta(m), \delta(n))$ for some polynomial S with integer coefficients*
- *a product rule $\delta(mn) = P(m, n, \delta(m), \delta(n))$ for some polynomial P with integer coefficients*

is of the form

$$\delta(n) = \pm \frac{n - n^{p^e}}{p} + f(n)$$

for some prime integer p, positive integer e, and polynomial f with integer coefficients.

Definition 2 *Let R be a commutative ring with 1 and p a prime integer. A p-*derivation *on R is a function $\delta : R \to R$ such that $\delta(0) = \delta(1) = 0$ and δ satisfies the sum rule $(+)$ and the product rule $(\times)$ above; i.e., for all $r, s \in R$,*

$$\delta_p(r+s) = \delta_p(r) + \delta_p(s) - \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} r^i s^{p-i} \qquad (+)$$

and

$$\delta_p(rs) = r^p \delta_p(s) + r^p \delta_p(s) + p\delta_p(r)\delta_p(s). \qquad (\times)$$

$$\delta(f(x_1, \ldots, x_n)) = \frac{f(x_1^p, \ldots, x_n^p) - f(x_1, \ldots, x_n)^p}{p},$$

and this function is a p-derivation. Just so we can refer to this function later, let's call this the *standard* p-derivation on $\mathbb{Z}[x_1, \ldots, x_n]$ and denote it by $\delta_{\mathrm{st},p}$

A Zariski-Nagata theorem for symbolic powers

Theorem 4 (Zariski-Nagata Theorem) *Let $X \subseteq \mathbb{C}^n$ be the solution set of the system of polynomial equations*

$$f_1 = \cdots = f_m = 0.$$

Suppose that $f_1, \ldots, f_m$ generate a prime ideal $\mathfrak{q}$. Then $\mathfrak{q}^{(r)}$ is exactly the set of polynomials $f \in \mathbb{C}[x_1, \ldots, x_n]$ such that

$$\left.\frac{\partial^{a_1+\cdots+a_n} f}{\partial x_1^{a_1} \cdots \partial x_n^{a_n}}\right|_X \equiv 0 \text{ for all } a_1 + \cdots + a_n < r.$$

Theorem 5 (De Stefani-Grifo-Jeffries) *Consider the ring $\mathbb{Z}[x_1, \ldots, x_n]$ and let $\mathfrak{q} = (f_1, \ldots, f_m)$ be a prime ideal. Suppose that $\mathfrak{q}$ contains the prime integer p. Then $\mathfrak{q}^{(r)}$ is exactly the set of polynomials $f \in \mathbb{Z}[x_1, \ldots, x_n]$ such that*

$$\delta_{\mathrm{st},p}^{a_0}\left(\frac{\partial^{a_1+\cdots+a_n} f}{\partial x_1^{a_1} \cdots \partial x_n^{a_n}}\right) \in \mathfrak{q} \text{ for all } a_0+a_1+\cdots+a_n < r.$$

Thank you for your attention!