

p-adische Zahlen

**Vorlesung im Wintersemester 2026/2027
an der Philipps-Universität Marburg**

Panagiotis Konstantis

16. Oktober 2026

Inhaltsverzeichnis

1	Motivation	1
1.1	Hensels Analogie	1
1.2	Ganzzahlige Lösungen von Gleichungen	4

1 Motivation

Die *p*-adischen Zahlen wurden von KURT HENSEL¹ eingeführt. Hensels Motivation war, die Eigenschaften des Polynomringes $\mathbb{C}[X]$ in einer Unbekannten X und des zugehörigen Körpers der rationalen Funktionen $\mathbb{C}(X)$ auf die ganzen Zahlen $\mathbb{Z}$ und den zugehörigen Quotientenkörper $\mathbb{Q}$ zu übertragen. Wir wollen in diesem Kapitel genau das etwas näher beleuchten. Dabei werden wir nicht mathematisch rigoros vorgehen, aber stattdessen die Idee hinter den *p*-adischen Zahlen hervorheben.

1.1 Hensels Analogie

Betrachtet man ein Polynom $P \in \mathbb{C}[X]$ und eine komplexe Zahl $\alpha \in \mathbb{C}$, so ist es möglich, etwa mittels einer *Taylor-Entwicklung*, das Polynom in der Form

$$P(X) = a_0 + a_1(X - \alpha) + a_2(X - \alpha)^2 + \dots + a_n(X - \alpha)^n$$

zu schreiben für gewisse $a_i \in \mathbb{C}$. Dabei sind die Polynome der Form $X - \alpha$ *irreduzibel* in $\mathbb{C}[X]$ und können daher die Rolle einer *Primzahl* im Ring der Polynome einnehmen (und genau das ist auch die richtige Sichtweise). Aus dieser Darstellung lässt sich das Verhalten des Polynoms in allen Punkten nahe α verstehen.

Wir möchten also diese Entwicklung auf natürliche Zahlen übertragen. Ist etwa p eine Primzahl, so wollen wir eine natürliche Zahl in eine Form

$$a_0 + a_1p + a_2p^2 + a_3p^3 + \dots + a_np^n$$

schreiben. Eine solche Darstellung ist uns auch bereits bestens bekannt, denn wir schreiben natürliche Zahlen in der Basis 10 (keine Primzahl!), etwa ist

$$321 = 1 \cdot 10^0 + 2 \cdot 10^1 + 3 \cdot 10^2.$$

Wir können aber auch 321 in der Basis $p = 7$ schreiben, etwa

$$321 = 5 + 3 \cdot 7 + 6 \cdot 7^2$$

und in Analogie zur Basis 10 hätten wir hier die Zifferndarstellung 635 in der Basis $p = 7$ der Zahl 321.

Bei der Taylorentwicklung des Polynoms $P(X)$ oben lässt sich durch die Kenntnis der Koeffizienten a_i herauslesen, zu welcher Ordnung sich das Polynom durch $(X - \alpha)$ teilen lässt. Ähnlich dazu lässt sich an der Zifferndarstellung einer Zahl in einer Basis p herauslesen, welches die größte Potenz von p ist, welche die Zahl noch teilt. Für die Zahl 72 in der Basis $p = 3$ gilt

$$72 = 0 + 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3$$

¹Deutscher Mathematiker, 1861 – 1941. Professur für Mathematik an der Philipps-Universität Marburg von 1901 – 1931

und damit ist 2200 die Zifferndarstellung bezüglich $p = 3$ und wir sehen, dass 3^2 die höchste Dreierpotenz ist, welche 72 teilt.

Betrachten wir nun rationale Funktionen, wie etwa

$$f(X) = \frac{1}{1-X}.$$

Formal lässt sich f in eine geometrische Reihe entwickeln (Taylor-Entwicklung um $X = 0$)

$$f(X) = 1 + X + X^2 + X^3 + \dots$$

und wir sehen, dass

$$f(X) \equiv 1 \pmod{X}$$

$$f(X) \equiv 1 + X \pmod{X^2}$$

$$f(X) \equiv 1 + X + X^2 \pmod{X^3}$$

$\vdots$

gilt. Führen wir die Analogie fort, so hätten wir gerne für eine Primzahl p eine ähnliche Entwicklung, d.h.

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \dots$$

doch klarerweise konvergiert diese Reihe nicht in $\mathbb{R}$. Die Idee von p -adischen Zahlen ist es nun, einen geeigneten Konvergenzbegriff einzuführen, sodass

$$\frac{1}{1-p} \equiv 1 \pmod{p}$$

$$\frac{1}{1-p} \equiv 1 + p \pmod{p^2}$$

$$\frac{1}{1-p} \equiv 1 + p + p^2 \pmod{p^3}$$

$\vdots$

gegen $\frac{1}{1-p}$ konvergiert. Wir sehen an dem Beispiel, dass der Konvergenzbegriff beinhalten muss, dass Teilbarkeit durch eine große Primzahlpotenz als „klein“ gelten soll (ähnlich wie bei der geometrischen Reihe, bei der x^n für $|x| < 1$ für wachsendes n vom Betrag her kleiner wird).

Nehmen wir z.B. $p = 5$, so erhalten wir nach obiger Analogie

$$-\frac{1}{2} = 2 \cdot \frac{1}{1-5} = 2 + 2 \cdot 5 + 2 \cdot 5^2 + \dots$$

was die Darstellung $\dots 222$ ergibt und damit erhalten wir auch

$$\frac{1}{2} = 1 - \frac{1}{2} = \dots 2223.$$

Man beachte, dass wenn wir die Darstellung $\dots 2223$ mit 2 multiplizieren, so erhalten wir $2 \cdot 3 = 6$, was 11 in der Basis $p = 5$ ist, also schreiben wir $\dots 1$ und nehmen die andere 1 mit, für die nächste

Stelle haben wir $2 \cdot 2 = 4$ und mit dem Übertrag $4 + 1 = 5$, was 10 in $p = 5$ ist, also schreiben wir ...01 und nehmen die 1 wieder als Übertrag mit. Führen wir das so durch, so erhalten wir die Darstellung

$$\dots 0001,$$

was gleich 1 ist. Nun lassen sich nicht nur ganze Zahlen p -adisch entwickeln, sondern auch Brüche $x = a/b$ für $a \in \mathbb{N}$, $b \in \mathbb{Z}$ und a, b teilerfremd. Wir sagen, dass so ein Bruch durch p teilbar ist, wenn p den Nenner b nicht teilt, aber a durch p teilbar ist². Wir wollen also eine Entwicklung der Form

$$x \equiv a_0 + a_1 p + a_2 p^2 + \dots + a_k p^k \pmod{p^{k+1}}$$

für alle $k \in \mathbb{N}$ mit $a_k \in \{0, \dots, p-1\}$. Gemäß unserer Hensel-Analogie ist die p -adische Entwicklung durch folgende rekursive Berechnung möglich:

1. Wir beginnen damit, die Kongruenz $a - a_0 b \equiv 0 \pmod{p}$ zu lösen und erhalten a_0 . Wir setzen $r_0 = \frac{a - a_0 b}{p}$. Beachte, dass $r_0 \in \mathbb{Z}$ ist, da a_0 so gewählt wurde, dass die Differenz durch p teilbar ist.
2. Für $k \geq 0$ lösen wir die Gleichung $r_k - a_{k+1} b \equiv 0 \pmod{p}$ und setzen $r_{k+1} = \frac{r_k - a_{k+1} b}{p}$.

So erhalten wir die Koeffizienten $a_0, \dots, a_k, \dots$ und damit die p -adische Darstellung von x als $(\dots a_k \dots a_0)_p$. Übungsaufgabe: Zeige, dass dieser Algorithmus genau die p -adische Darstellung ergibt.

Hier ein Beispiel: Wir betrachten $x = \frac{24}{17}$ und wollen nun diesen Bruch 3-adisch entwickeln, also $p = 3$ betrachten.

k	a_k	r_k
0	0	8
1	1	-3
2	0	-1
3	1	-6
4	0	-2
5	2	-12
6	0	-4
7	1	-7
8	1	-8
9	2	-14

und damit ist

$$\frac{24}{17} = \dots 2110201010_3.$$

Wir wollen noch eine letzte Analogie ziehen. Für manche rationale Funktionen über $\mathbb{C}$ ist eine Taylor-Entwicklung nicht immer möglich, aber dafür eine *Laurent-Entwicklung*. Sind $P, Q \in \mathbb{C}[X]$ und $f := P/Q$ mit $Q \neq 0$, so gilt

$$f(X) = \sum_{k=-\infty}^{\infty} a_k (X - \alpha)^k.$$

²Beachte, dass wenn $p \nmid b$, so auch $p^k \nmid b$ für alle $k > 1$ und damit ist b invertierbar in $\mathbb{Z}_{p^k}$

Z. B. existiert folgende Laurent-Entwicklung:

$$f(X) = \frac{1}{X(1+X^2)} = \frac{1}{X} - X + X^3 - X^5 + \dots$$

Analog erwarten wir dann auch für gewisse Brüche eine p -adische Entwicklung

$$x = a_{-k}p^{-k} + a_{-k+1}p^{-k+1} + \dots + a_{-1}p^{-1} + a_0 + a_1p + a_2p^2 + \dots$$

Wir erinnern nochmal daran, dass wir in diesem Kapitel auf mathematische Formalität verzichten und eher durch heuristische Überlegungen Zugang zum Gebiet der p -adischen Zahlen erhalten wollen. Die Laurent-Entwicklung mit negativem k erhalten wir dann, wenn der Nenner durch p teilbar ist. Sei wieder $x = \frac{a}{b}$ ein gekürzter und angenommen es ist $m \in \mathbb{N}$ so gewählt, dass $p^m b' = b$ und $p \nmid b'$. Dann können wir wie oben den Bruch $\frac{a}{b'}$ p -adisch entwickeln, etwa

$$\frac{a}{b'} = a_0 + a_1p + a_2p^2 + \dots$$

und multiplizieren dann alles mit p^{-m} und erhalten

$$\frac{a}{b} = a_0p^{-m} + a_1p^{-m+1} + a_2p^{-m+2} + \dots + a_m + a_{m+1}p + a_{m+2}p^2 + \dots$$

Betrachten wir etwa $x = \frac{8}{51} = 3^{-1} \frac{8}{17}$. Geht man den Algorithmus für $\frac{24}{17}$ durch, so kann man daraus ablesen, dass

$$\frac{8}{17} = \dots 211020101_3$$

ist (man entferne die letzte Null, warum?) und damit erhalten wir

$$\frac{8}{51} = \dots 21102010.1_3$$

also alles entlang des Punktes nach rechts verschieben.

1.2 Ganzzahlige Lösungen von Gleichungen

Angenommen man möchte eine Gleichung der Form $x^2 = y$ mit $y \in \mathbb{Z}$ in den ganzen oder rationalen Zahlen lösen. Eine notwendige Bedingung ist dann

$$x^2 \equiv y \pmod{p^n}$$

für alle $n \in \mathbb{N}$, wobei, wie immer, p eine Primzahl ist. Dabei können wir uns auf die Fälle $x, y \in \mathbb{Z}$ beschränken, denn ist $\frac{a}{b}$ eine rationale Lösung mit $\text{ggT}(a, b) = 1$ und $\text{ggT}(b, p) = 1$, so ist

$$\left(\frac{a}{b}\right)^2 \equiv y \pmod{p^n} \quad \text{äquivalent zu} \quad a^2 \equiv b^2 y \pmod{p^n}.$$

Das ist genau die Idee von Euklids Beweis der Irrationalität von $\sqrt{2}$. Setzen wir $p = 2$, so müsste

$$a^2 \equiv 2b^2 \pmod{2} \quad \text{und} \quad a^2 \equiv 2b^2 \pmod{4}$$

sein. Aus der ersten Gleichung folgt $a \equiv 0 \pmod{2}$ und aus der zweiten $b \equiv 0 \pmod{2}$, was ein Widerspruch zu $\text{ggT}(a, b) = 1$ ist. Analog zeigt man, dass $x^2 = p$ für jede Primzahl p keine rationale Lösung hat.

Die Lösbarkeit einer solchen Gleichung ist eng mit den p -adischen Zahlen verbunden. Angenommen es gäbe $x_n \in \{0, \dots, p^n - 1\}$ mit

$$x_n^2 \equiv y \pmod{p^n} \quad \text{und} \quad x_{n+1} \equiv x_n \pmod{p^n}$$

für alle $n \in \mathbb{N}$ mit $n \geq 1$, so lässt sich aus der Folge (x_n) eine p -adische Zahl wie folgt bauen: Es existieren $a_n \in \{0, \dots, p-1\}$ mit

$$x_{n+1} = x_n + a_n p^n$$

und setze $a_0 := x_1$. Also

$$x_{n+1} = \sum_{k=0}^n a_k p^k$$

und die (noch) formale Reihe

$$x := a_0 + a_1 p + a_2 p^2 + \dots = \sum_{k=0}^{\infty} a_k p^k$$

definiert nach unserem obigen Verständnis eine p -adische Zahl. Diese Zahl löst nun alle unsere quadratischen Kongruenzgleichungen gleichzeitig, denn es gilt

$$x \equiv x_n \pmod{p^n} \quad \text{also} \quad x^2 \equiv x_n^2 \equiv y \pmod{p^n}$$

für alle $n \in \mathbb{N}$. Folglich können wir sagen: Existiert für die Gleichung $x^2 = y$ keine p -adische Lösung, so besitzt sie auch keine ganzzahlige oder rationale Lösung. Dieses Vorgehen lässt sich natürlich auf beliebige ganzzahlige Gleichungen anwenden.

Man beachte, dass die Existenz einer p -adischen Lösung einer solchen Gleichung nicht impliziert, dass sie eine ganzzahlige oder rationale Lösung besitzt, wie folgendes berühmte Beispiel zeigt: Der *Große Satz von Fermat* besagt, dass die Gleichung

$$x^n + y^n = z^n$$

keine ganzzahlige Lösung mit $xyz \neq 0$ und $n > 2$ besitzt³. Dass diese Gleichung stets eine p -adische Lösung besitzt, ist relativ einfach zu sehen, falls $p \nmid n$: Nimm $x = 1$, $y = p$ und löse

$$z^n = 1 + p^n$$

p -adisch (Übungsaufgabe). Für $p|n$ gibt es auch eine Möglichkeit eine p -adische Lösung zu konstruieren, nur benötigen wir hierfür etwas mehr Theorie.

14.10.2026
1. Vorlesung

³Dieser Satz wurde in der bahnbrechenden Arbeit *Modular elliptic curves and Fermat's Last Theorem* von Andrew Wiles bewiesen.