

p -adische Zahlen

Stefan Kottwitz

31. Dezember 2007

Zusammenfassung

Die bekannte Darstellung einer natürlichen Zahl in einer Basis p läßt sich erweitern zu Darstellungen beliebiger ganzer Zahlen, weiterhin für rationale Zahlen, und diese schließlich zu einem Zahlkörper, der sich von den reellen Zahlen erheblich unterscheidet. Man reduziert die Betrachtung sinnvoll auf Primzahlen p , und spricht dann von den p -adischen Zahlen.

Die p -adischen Zahlen kann man analog zu den reellen Zahlen als alternative vervollständigende Erweiterung des rationalen Zahlkörpers \mathbb{Q} konstruieren. In bekannter Weise betrachtet man \mathbb{Q} als metrischen Raum, dessen Metrik der gewohnte Absolutbetrag induziert und vervollständigt ihn etwa durch Einbettung in die Äquivalenzklassen der Cauchy-Folgen von \mathbb{Q} , man erhält \mathbb{R} .

Es läßt sich aber auch eine andere Metrik einführen, welche die Abstände zwischen rationalen Zahlen anders mißt, und diesen neuen metrischen Raum kann man zum p -adischen Zahlkörper vervollständigen. Diese neue Metrik wird durch den p -adischen Absolutbetrag bestimmt. Die p -adischen Zahlen werden hier zunächst noch nicht als Vervollständigung von \mathbb{Q} betrachtet, sie sollen motiviert und formal algebraisch eingeführt werden.

Dieser Artikel wurde auf matheplanet.de veröffentlicht.

Inhaltsverzeichnis

1	Hensels Analogie	2
2	Die p-adische Entwicklung	3
3	Die p-adischen Zahlen	5
4	\mathbb{Z}_p und der projektive Limes	6
5	Rechnen mit p-adischen Zahlen in PARI/GP	8
6	Literatur und Links	10

1 Hensels Analogie

Gegen Ende des 19. Jahrhunderts wurde die Theorie der p -adischen Zahlen im Wesentlichen durch Kurt Hensel entwickelt. Buchveröffentlichungen Hensels sind Interessierten im Internet frei verfügbar, siehe [3] und [4].

Kurt Hensel verglich den Ring \mathbb{Z} und seinen Quotientenkörper \mathbb{Q} mit dem Polynomring $\mathbb{C}[X]$ und dessen Quotientenkörper $\mathbb{C}(X)$. $f(X) \in \mathbb{C}(X)$ ist als rationale Funktion ein Quotient zweier Polynome:

$$f(X) = \frac{P(X)}{Q(X)}, \quad P(X), Q(X) \in \mathbb{C}[X], \quad Q(X) \neq 0.$$

Ähnlich ist eine rationale Zahl $r \in \mathbb{Q}$ darstellbar als Quotient zweier ganzer Zahlen:

$$r = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad b \neq 0.$$

\mathbb{Z} und $\mathbb{C}[X]$ sind beide Ringe mit eindeutiger Faktorzerlegung. Jedes Polynom läßt sich (bis auf Reihenfolge) eindeutig als Produkt linearer Polynome darstellen:

$$P(X) = c(X - \alpha_1)^{k_1}(X - \alpha_2)^{k_2} \cdots (X - \alpha_n)^{k_n},$$

$c, \alpha_i \in \mathbb{C}, k_i \in \mathbb{N}$ und jede ganze Zahl $f \in \mathbb{Z}$ kann man in eindeutiger Weise in Primfaktoren zerlegen:

$$f = \pm 1 \cdot p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \quad p_1, \dots, p_n \text{ Primzahlen.}$$

Die Primzahlen $p_i \in \mathbb{Z}$ zeigen sich als analog zu den linearen Polynomen $(X - \alpha_i) \in \mathbb{C}[X]$, welche die Primideale des Ringes $\mathbb{C}[X]$ erzeugen. Die ± 1 in der Primfaktorzerlegung ist in diesem Vergleich das Gegenstück zum konstanten Polynom c in der Polynomzerlegung, beide sind (jeweils alle) Einheiten im jeweiligen Ring \mathbb{Z} bzw. $\mathbb{C}[X]$, besitzen multiplikative Inverse.

Die Analogie geht weiter. Bekanntlich gibt es für jedes Polynom $P(X)$ und fest gewähltes komplexes α eine Summendarstellung

$$P(X) = \sum_{i=0}^n a_i (X - \alpha)^i \tag{1}$$

mit $a_i \in \mathbb{C}$. $P(X)$ läßt sich in eine Taylor-Reihe entwickeln. Dies kann man ähnlich für ganze Zahlen $f \in \mathbb{Z}$ tun. So wie wir oben $(X - \alpha)$ festlegten, wählen wir nun ein festes p . O.B.d.A. betrachten wir positive ganze Zahlen. f kann man anstatt dezimal in der Basis p schreiben:

$$f = \sum_{i=0}^n a_i p^i \tag{2}$$

mit $a_i \in \mathbb{Z}$ und $0 \leq a_i < p$. An beiden Entwicklungen kann man lokale Informationen ablesen: Die Entwicklung (1) zeigt, ob $P(X)$ eine Nullstelle in α besitzt und welche Vielfachheit sie hat. Und die Entwicklung (2) zeigt, ob f durch p teilbar ist, und mit welcher Vielfachheit.

Weiterhin können wir diese Entwicklungen auch für Quotienten von Polynomen angeben, $f(X) \in \mathbb{C}(X), \alpha \in \mathbb{C}$:

$$f(X) = \frac{P(X)}{Q(X)} = \sum_{i \geq n_0} a_i (X - \alpha)^i, \tag{3}$$

dies ist die aus der Funktionentheorie bekannte, im Allgemeinen unendliche, Laurent-Entwicklung von $f(X)$ an der Stelle α , mit endlichem Hauptteil. In (3) kann man ablesen, ob $f(X)$ in α eine Nullstelle oder einen Pol hat, und mit welcher Ordnung. Der Körper $\mathbb{C}(X)$ der rationalen Funktionen läßt sich in den Körper aller Laurent-Entwicklungen in α einbetten. Nicht jede Laurent-Entwicklung entspricht einer rationalen Funktion.

Nun wird die Analogie zwischen \mathbb{Z} und $\mathbb{C}[X]$ ausgedehnt auf die jeweiligen Quotientenkörper \mathbb{Q} und $\mathbb{C}(X)$. Gesucht ist eine Entwicklung analog zu (3) für rationale Zahlen.

Im weiteren bezeichne p jeweils eine feste Primzahl.

2 Die p -adische Entwicklung

Jede natürliche Zahl $f \in \mathbb{N}$ besitzt eine p -adische Entwicklung (2), mit Koeffizienten¹ $a_i \in \{0, 1, \dots, p-1\}$. Diese Entwicklung ist eindeutig und endlich, die Koeffizienten lassen sich durch fortgesetzte Division mit Rest bezüglich p berechnen.

Schreibweise: $f = a_0, a_1 a_2 \dots a_n (p)$

Beispiel 1:

$$108 = 3, 12 \quad (7)$$

$$216 = 1, 331 \quad (5)$$

$$448 = 0, 121 \quad (7)$$

Um negative und gebrochene Zahlen p -adisch entwickeln zu können, benötigen wir unendliche Reihen $\sum_{i=0}^{\infty} a_i p^i$ bzw. $\sum_{i=-m}^{\infty} a_i p^i$. Zunächst ohne Konvergenzbetrachtungen², wir verwenden die Reihen nur formal als Folge ihrer Partialsummen (s_n). Dies veranlaßt zunächst zur folgenden

Definition 1: Eine ganze p -adische Zahl ist eine formale unendliche Reihe $\sum_{i=0}^{\infty} a_i p^i$ mit $0 \leq a_i < p$ für alle i .

Die Menge der ganzen p -adischen Zahlen wird mit \mathbb{Z}_p bezeichnet. \mathbb{Z}_p ist übrigens überabzählbar.

Um eine rationale Zahl f , zunächst für $f \in \mathbb{Z}_{(p)}$ ³, p -adisch entwickeln zu können, benutzen wir folgenden

Satz 1: Für die Restklassen $a \bmod p^n \in \mathbb{Z}/p^n \mathbb{Z}$ existiert eine eindeutige Darstellung

$$a \equiv \sum_{i=0}^{n-1} a_i p^i \pmod{p^n} \quad (4)$$

mit $0 \leq a_i < p$ für alle i .

¹„ p -adischen Ziffern“

²Die offensichtliche Divergenz kann man durch Änderung des Konvergenzbegriffs bzw. der Metrik beheben.

³ $\mathbb{Z}_{(p)}$ ist der lokale Ring $\mathbb{Z}_{(p)} = \left\{ \frac{g}{h} : g, h \in \mathbb{Z}, p \nmid h \right\}$. Dessen Elemente werden auch als „für p ganze Zahlen“ bezeichnet.

Beweis: erfolgt mittels vollständiger Induktion. Im Fall $n = 1$ haben wir die Restklassen mod p zu betrachten, die Darstellung ist offensichtlich, mit a_0 als Repräsentanten aus $\{0, 1, \dots, p - 1\}$. Gelte nun die Behauptung für $n - 1$, also

$$a \equiv \sum_{i=0}^{n-2} a_i p^i \pmod{p^{n-1}},$$

damit eine eindeutige Darstellung

$$a = \sum_{i=0}^{n-2} a_i p^i + g p^{n-1} \tag{5}$$

mit $g \in \mathbb{Z}$. Ist $g \equiv a_{n-1} \pmod{p}$ mit $0 \leq a_{n-1} < p$, so ist a_{n-1} eindeutig bestimmt, und es ist $g = a_{n-1} + kp$ mit $k \in \mathbb{Z}$, damit wird (5) zu

$$\begin{aligned} a &= \sum_{i=0}^{n-2} a_i p^i + (a_{n-1} + kp) p^{n-1} \\ a &= \sum_{i=0}^{n-2} a_i p^i + a_{n-1} p^{n-1} + kp^n \end{aligned}$$

und die Kongruenz (4) ist gezeigt, Satz 1 nach Induktionsprinzip bewiesen. ■

Jedes für p ganze f , also $f \in \mathbb{Z}_{(p)}$, bestimmt somit eine Folge $(\bar{s}_n)_{n \in \mathbb{N}}$ von Restklassen:

$$\bar{s}_n = f \pmod{p^n} \in \mathbb{Z}/p^n \mathbb{Z},$$

für deren Glieder nach Satz 1 gilt:

$$\begin{aligned} \bar{s}_1 &= a_0 \pmod{p}, \\ \bar{s}_2 &= a_0 + a_1 p \pmod{p^2}, \\ &\dots \\ \bar{s}_n &= \sum_{i=0}^{n-1} a_i p^i \pmod{p^n} \\ &\dots \end{aligned}$$

mit eindeutig bestimmten Koeffizienten $a_i \in \{0, 1, \dots, p - 1\}$. Die zugehörige Zahlenfolge $(s_n)_{n \in \mathbb{N}}$:

$$s_n = \sum_{i=0}^{n-1} a_i p^i$$

definiert eine ganze p -adische Zahl $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$. Dies ist die p -adische Entwicklung von f .

Beispiel 2: $f = \frac{31}{4}$:

$$\begin{aligned}\frac{31}{4} &\equiv 4 \pmod{5}, & \text{denn } \frac{31}{4} - 4 &= \frac{31}{4} - \frac{16}{4} = \frac{15}{4} = \frac{3}{4} \cdot 5, \\ \frac{31}{4} &= 4 + \frac{3}{4} \cdot 5, \\ \frac{3}{4} &\equiv 2 \pmod{5}, & \frac{3}{4} &= 2 + \left(-\frac{1}{4}\right) \cdot 5, \\ -\frac{1}{4} &\equiv 1 \pmod{5}, & -\frac{1}{4} &= 1 + \left(-\frac{1}{4}\right) \cdot 5\end{aligned}$$

und es wird periodisch. Wir haben für $n \geq 3$

$$s_n = 4 + 2 \cdot 5 + 5^2 + 5^3 + \dots + 5^{n-1} + \left(-\frac{1}{4}\right) \cdot 5^n,$$

und die zugehörige p -adische Entwicklung ist

$$\frac{31}{4} = 4,21111\dots(5).$$

Beispiel 3: $\sqrt{2} \in \mathbb{Z}_7$ ist $3,12612124662\dots(7)$. Die Berechnung wird durch die Grafik in der Einführung⁴ illustriert: sukzessive werden die Kongruenzen $x^2 \equiv 2 \pmod{7^n}$ gelöst.

3 Die p -adischen Zahlen

Der anfänglichen Analogie folgend erweitert man die Menge der ganzen p -adischen Zahlen, ähnlich der Laurent-Entwicklung (3), und betrachtet formale Reihen mit „endlichem Hauptteil“:

Definition 2: Eine p -adische Zahl ist eine formale unendliche Reihe $\sum_{i=-m}^{\infty} a_i p^i$ mit $m \in \mathbb{Z}$ und $0 \leq a_i < p$ für alle i .

Die Menge p -adischer Zahlen wird mit \mathbb{Q}_p bezeichnet.

Ist f eine beliebige rationale Zahl, so kann man p aus Zähler und Nenner „herausziehen“ und schreiben:

$$f = \frac{g}{h} p^{-m}, \quad g, h \in \mathbb{Z}, \quad (gh, p) = 1,$$

folglich ist $\frac{g}{h} \in \mathbb{Z}_{(p)}$ und hat nach dem vorigen Abschnitt eine p -adische Entwicklung $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$, die rationale Zahl f erhält dann die p -adische Entwicklung

$$f = \sum_{i=0}^{\infty} a_i p^{i-m} \quad \text{bzw.} \quad f = \sum_{i=-m}^{\infty} a_{i+m} p^i \in \mathbb{Q}_p.$$

Bemerkung: \mathbb{Q} läßt sich so kanonisch in \mathbb{Q}_p injektiv einbetten, wobei \mathbb{Z} in \mathbb{Z}_p überführt wird. Identifizieren wir in dieser Weise \mathbb{Q} mit seinem Bild in \mathbb{Q}_p , so können wir für jede rationale Zahl $f \in \mathbb{Q}$ schreiben:

$$f = \sum_{i=-m}^{\infty} a_i p^i \tag{6}$$

⁴in der Version auf auf matheplanet.de

und dies ist nun das zahlentheoretische Analogon zur Laurentreihenentwicklung (3).

Die Laurent-Reihen (3) aus der Funktionentheorie liefern uns Informationen über das lokale Verhalten einer Funktion $f(X) \in \mathbb{C}(X)$ an einer Stelle $\alpha \in \mathbb{C}$, nämlich Polstellen und Nullstellen mit ihrer Vielfachheit. Die p -adische Entwicklung (6) gibt uns ebenso Informationen über das lokale Verhalten einer rationalen Zahl $f = \frac{g}{h}$ „an der Stelle p “, vorausgesetzt, der Bruch liegt bereits in gekürzter Darstellung vor:

$$\begin{aligned} -m < 0 &\Rightarrow p \mid h \text{ und } p \nmid g \\ -m = 0 &\Rightarrow p \nmid g \text{ und } p \nmid h \\ -m > 0 &\Rightarrow p \mid g \text{ und } p \nmid h \end{aligned}$$

Der erste Fall entspricht „Polstellen“ in p , der dritte Fall „Nullstellen“ in p ($\frac{g}{h} \equiv 0 \pmod{p}$) mit entsprechender Vielfachheit.

Bemerkung: In der Definition p -adischer Zahlen wird mitunter zunächst die Bedingung $a_i \in \{0, \dots, p-1\}$ für die Koeffizienten der formalen Reihe weggelassen und es werden allgemeine rationale a_i zugelassen. Das ergibt natürlich nur Sinn, wenn die $a_i \in \mathbb{Z}_{(p)}$ sind, also der Nenner der a_i in gekürzter Darstellung nicht durch p teilbar ist. Dann muß man, um mit den p -adischen Zahlen vernünftig rechnen zu können, die Gleichheit p -adischer Zahlen mittels einer Äquivalenzrelation definieren. In diesem allgemeineren Fall werden zwei p -adische Zahlen f, f' als gleich identifiziert, wenn für jedes n jeweils die Partialsummen s_n, s'_n in derselben Restklasse modulo p^n liegen. Im folgenden Abschnitt wird das formal konkretisiert.

4 \mathbb{Z}_p und der projektive Limes

Ein Griff in die Werkzeugkiste der Kategorientheorie: der projektive Limes, auch inverser Limes genannt, umfaßt Strukturen einer Kategorie, welche durch Morphismen untereinander verbunden sind. Wir erklären zunächst den allgemeinen Begriff, bevor wir ihn für unser spezielles Thema definieren.

Definition 3: $\{O_i\}_{i \in I}$ sei eine Familie von Objekten einer Kategorie C^5 , indiziert durch eine halbgeordnete Menge I .

Weiterhin sei $\Phi = \{\phi_{ij} : O_i \rightarrow O_j\}$ eine Menge von Morphismen in C mit

$$\begin{aligned} \phi_{ii}(x) &= x \quad \forall x \in O_i \\ \phi_{ik} &= \phi_{jk} \circ \phi_{ij} \quad \forall i > j > k. \end{aligned}^6$$

Das Paar $(\{O_i\}_{i \in I}, \Phi)$ heißt projektives System von Objekten aus C und Morphismen in C über I .

Auf $\{O_i\}_{i \in I}$ haben wir damit eine transitive Relation durch die Morphismen vorgegeben:

$$O_i \leq O_j \Leftrightarrow \exists \phi_i \in \Phi : O_i \rightarrow O_j.$$

⁵Gruppen, Ringe, Moduln über demselben Ring, Algebren, Vektorräume, ...

⁶ $\{\phi_{ij}\}$ ist eine transitive Menge von Morphismen.

Definition 4: Der projektive Limes O eines projektiven Systems $(\{O_i\}_{i \in I}, \Phi)$ ist die Menge aller Familien $(x_i)_{i \in I}$ mit $x_i \in O_i$ für alle $i \in I$ und der Eigenschaft

$$i > j \Rightarrow \phi_{ij}(x_i) = x_j.$$

Bemerkung: Der projektive Limes ist eine Unterstruktur des direkten Produkts aller O_i und gehört derselben Kategorie an. Es existieren die natürlichen Projektionen

$$\pi_i : O \rightarrow O_i$$

welche den projektiven Limes auf seine i -te Komponente abbilden.

Nun zu unserem speziellen Fall, dem projektiven Limes von Ringen, indiziert durch die natürlichen Zahlen. Wir betrachten das direkte Produkt von Ringen

$$\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n \in \mathbb{N}} : x_n \in \mathbb{Z}/p^n\mathbb{Z}\}, \quad (7)$$

zwischen den verschiedenen Ringen $\mathbb{Z}/p^n\mathbb{Z}$ existieren Ringhomomorphismen, nämlich die kanonischen Projektionen $\lambda_i : \mathbb{Z}/p^{i+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^i\mathbb{Z}$:

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\lambda_3} \dots \quad (8)$$

Innerhalb dieses direkten Produktes (7) gibt es eine Teilmenge, deren Elemente $(x_n)_{n \in \mathbb{N}}$ die Eigenschaft $\lambda_n(x_{n+1}) = x_n$ für alle n besitzen. Diese Teilmenge wird als projektiver Limes der Ringe $\mathbb{Z}/p^n\mathbb{Z}$ bezeichnet.

Zusammenfassung und Schreibweise:

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n \in \mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \lambda_n(x_{n+1}) = x_n \forall n \in \mathbb{N} \right\}$$

Als Teilring des direkten Produkts (7) ist der projektive Limes selbst ein Ring.

Betrachten wir nun die ganzen p -adischen Zahlen $f = \sum_{i=0}^{\infty} a_i p^i$ statt als Folgen der ganzzahligen Partialsummen

$$s_n = \sum_{i=0}^{n-1} a_i p^i \in \mathbb{Z}$$

als Folgen der Restklassen

$$\bar{s}_n = s_n \pmod{p^n} \in \mathbb{Z}/p^n\mathbb{Z}.$$

Für die Glieder dieser Folgen (s_n) gilt

$$\lambda_n(\bar{s}_{n+1}) = \bar{s}_n$$

unter der kanonischen Projektion λ_n aus (8), oder anders ausgedrückt:

$$m > n \Rightarrow \bar{s}_m \equiv \bar{s}_n \pmod{p^n}$$

Wir können \mathbb{Z}_p mit $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ identifizieren, wodurch sich \mathbb{Z}_p als Ring erweist, denn als direkte Folgerung aus Satz 1 erhalten wir

Satz 2: Die Abbildung

$$\mathbb{Z}_p \rightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

$$f = \sum_{i=0}^{\infty} a_i p^i \mapsto (\bar{s}_n)_{n \in \mathbb{N}}$$

mit

$$\bar{s}_n = \sum_{i=0}^{n-1} a_i p^i \pmod{p^n} \in \mathbb{Z}/p^n\mathbb{Z}$$

ist eine Bijektion.

Bemerkung: Addition und Multiplikation sind im Ring \mathbb{Z}_p wohldefiniert, denn der projektive Limes ist Unterring eines direkten Produktes und übernimmt dessen komponentenweise Addition und Multiplikation. Der Ring \mathbb{Z}_p ist nullteilerfrei, wir erhalten \mathbb{Q}_p als den Quotientenkörper von \mathbb{Z}_p . \mathbb{Z} ist ein Teilring von \mathbb{Z}_p , dabei hat jedes $f \in \mathbb{Z}$ eine endliche Darstellung

$$f \equiv \sum_{i=0}^{n-1} a_i p^i \pmod{p^n}$$

mit $0 \leq a_i < p$.

Beispiel 4:

$$\begin{aligned} \mathbb{Z} \ni 35 = 1, 10001 \ (2) &\in \mathbb{Z}_2 \\ &= (1, 3, 3, 3, 3, 35, 35, 35, \dots) \in \varprojlim_n \mathbb{Z}/2^n\mathbb{Z} \end{aligned}$$

Man erhält natürlich für jede Primzahl p einen Ring \mathbb{Z}_p bzw. einen Körper \mathbb{Q}_p , unendlich viele, auch wenn man allgemein von \mathbb{Q}_p an sich spricht. Legt man keine Primzahl p zugrunde, sondern allgemeiner eine beliebige natürliche, möglicherweise zusammengesetzte Zahl, dann spricht man von g -adischen Zahlen, siehe z.B. [5]. Die g -adischen Zahlen bilden genau dann einen Körper, wenn g eine Primzahlpotenz p^n ist, was letztlich gleiche Resultate wie für p liefert, so ist das Interesse an primen p begründet.

5 Rechnen mit p -adischen Zahlen in PARI/GP

Manche Computer-Algebra-Systeme (CAS) verfügen über Funktionen zum Rechnen mit p -adischen Zahlen. Als Beispiel sei **PARI/GP** erwähnt.

PARI/GP ist ein CAS, das sich insbesondere für zahlentheoretische Berechnungen eignet. Es ist unter Unix/Linux, Mac OS und Windows lauffähig. Als freie Software steht es unter der **GNU General Public License**, der Quellcode ist frei verfügbar, daher läßt es sich für viele Betriebssysteme compilieren und installieren. Es gibt auch fertige Pakete ohne die Notwendigkeit der Compilierung, z.B. für Windows, Mac OS X und Debian bzw. Ubuntu Linux. In letzterem benötigt die Installation nur eine einzige Befehlszeile in der Shell oder einige Mausklicks im Synaptic Installer.

In PARI/GP gibt man p -adische Zahlen als ganzzahlige oder rationale Ausdrücke ein, zu denen $\mathcal{O}(p^n)$ addiert wird, wobei n die p -adische Genauigkeit angibt, die Anzahl signifikanter p -adischer Ziffern.

Dokumentation findet man bei Interesse auf der oben verlinkten PARI/GP-Homepage.

Man kann die gebräuchlichen arithmetischen Operationen in \mathbb{Q}_p durchführen, im folgenden in einer Beispielsitzung demonstriert. Zunächst wird die Darstellung von Zahlen aus Beispiel 1 kontrolliert: 108 in \mathbb{Z}_7 und 216 in \mathbb{Z}_5 , danach wird das Produkt $12, 314 \cdot 1, 203$ in \mathbb{Q}_7 berechnet.

```
? 108+O(7^3)
%1 = 3 + 7 + 2*7^2 + O(7^3)
? 216+O(5^4)
%2 = 1 + 3*5 + 3*5^2 + 5^3 + O(5^4)
? m = 7^-1 + 2 + 3*7 + 7^2 + 4*7^3 + O(7^10)
%3 = 7^-1 + 2 + 3*7 + 7^2 + 4*7^3 + O(7^10)
? n = 1 + 2*7 + 3*7^3 + O(7^10)
%4 = 1 + 2*7 + 3*7^3 + O(7^10)
? m*n
%5 = 7^-1 + 4 + 4*7^2 + 6*7^3 + 4*7^4 + 5*7^5 + 5*7^6 + 7^7 + O(7^9)
```

Das Ergebnis ist also 14,0464551 (7). Diese Zahl können wir mit der lift-Funktion als rationale Zahl darstellen:

```
? lift(m*n)
%6 = 10553796/7
```

Auch transzendente Funktionen sind implementiert, z.B. der p -adische Logarithmus und die Exponentialfunktion:

```
? x = 341 + O(7^8)
%7 = 5 + 6*7 + 6*7^2 + O(7^8)
? log(x)
%8 = 5*7 + 5*7^2 + 5*7^3 + 3*7^5 + 3*7^6 + 2*7^7 + O(7^8)
? exp(%8)
%9 = 1 + 5*7 + 2*7^3 + 3*7^4 + 2*7^5 + 5*7^6 + 7^7 + O(7^8)
? (x/%9)^6
%10 = 1 + O(7^8)
```

$x/\exp(\log(x))$ ist nämlich eine $(p-1)$ -te Einheitswurzel.

Definition und Eigenschaften der p -adischen Exponential- und Logarithmusfunktion finden sich z.B. [hier auf PlanetMath](#).

Die Grafik der Einführung⁷ visualisiert die Approximation der Quadratwurzel von 2 in den 7-adischen Zahlen. Die Zahlenwerte dieser Grafik und das Ergebnis aus Beispiel 3 wurden mit PARI/GP berechnet und mit PGF/TikZ in LaTeX gesetzt. Ein Ausschnitt der Berechnung:

```
? lift(sqrt(2+O(7^4)))
%11 = 2166
? sqrt(2+O(7^12))
%12 = 3 + 7 + 2*7^2 + 6*7^3 + 7^4 + 2*7^5 + 7^6 + 2*7^7 + 4*7^8 + 6*7^9
+ 6*7^10 + 2*7^11 + O(7^12)
```

⁷in der Version auf matheplanet.de

Wer PARI/GP nicht installieren kann oder möchte, der kann z.B auf [The SAGE Notebook](#) unter [SAGE](#) mit dem PARI/GP-Interface für SAGE online rechnen.

Diese Einführung entwickelte die p -adischen Zahlen mit algebraischen Mitteln als formale Objekte. Rein über Kongruenzbetrachtungen wäre eine zahlentheoretische Herleitung auch möglich. Eine schöne topologische Herangehensweise ist die Konstruktion von \mathbb{Q}_p als Vervollständigung der rationalen Zahlen \mathbb{Q} , analog zur Konstruktion der reellen Zahlen \mathbb{R} als Kompletterierung von \mathbb{Q} . Bei Interesse mag vielleicht ein Zusatz hierfür folgen.

6 Literatur und Links

Bücher

- [1] [George Bachman, *Introduction to \$p\$ -adic Numbers and Valuation Theory*, Academic Press, New York, 1964](#)
- [2] [Fernando Q. Gouvea, *\$p\$ -adic numbers*, Springer, 1993](#)
- [3] [Kurt Hensel, *Theorie der algebraischen Zahlen*, Teubner, 1908](#) (online lesbar)
- [4] [Kurt Hensel, *Zahlentheorie*, Göschen, 1913](#) (online lesbar)
- [5] [Kurt Mahler, *Lectures on Diophantine Approximations*, Notre Dame, 1961](#) (online lesbar)
- [6] [Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer, 1992](#)

Skripte

- [7] [A. J. Baker, *An Introduction to \$p\$ -adic Numbers and \$p\$ -adic Analysis*, Glasgow, 2004](#)
- [8] [Ç.K. Koç, *A Tutorial on \$p\$ -adic Arithmetic*, Oregon, 2002](#)
- [9] [K. Mathiak, *Bewertungstheorie*, Braunschweig, 1993](#)

Weblinks

- [10] [PARI/GP](#)
- [11] [MathWorld: \$p\$ -adic numbers](#) u.a.
- [12] [PlanetMath: \$p\$ -adic integers, \$p\$ -adic exponential and \$p\$ -adic logarithm](#)