

Kann man die Gleichung $-\frac{1}{2}=1+3+9+27+\dots$ sinnvoll interpretieren? Ein Einstieg zu p -adischen Zahlen

von Fritz Schweiger, Salzburg

Zusammenfassung. Zählen ist eine Grundtätigkeit des Menschen. Die kulturelle Evolution hat den Umgang mit natürlichen Zahlen um weitere Zahlbereiche angereichert. Man gelangt so über ganze Zahlen und rationale Zahlen zu den mathematisch anspruchsvollen Bereichen der reellen und komplexen Zahlen. Aber man hat auch p -adische Zahlen erfunden (oder gefunden?). Der Aufsatz könnte doch einige Leser und Leserinnen interessieren. Gedacht ist an SchülerInnen, die ein schönes Thema für eine Fachbereichsarbeit suchen oder an LehrerInnen, die ihren Wahlpflichtkurs aufpolieren wollen. Man könnte den Aufsatz auch jemandem in die Hand drücken, der die gute, aber wagemutige Idee hat, Mathematik zu studieren.

Der nachstehende Aufsatz ist mathematisch anspruchsvoll, aber vielleicht erreicht er doch einige Leser und Leserinnen. Gedacht ist an SchülerInnen, die ein schönes Thema für eine Fachbereichsarbeit suchen oder an LehrerInnen, die ihren Wahlpflichtkurs aufpolieren wollen. Man könnte den Aufsatz auch jemandem in die Hand drücken, der die gute, aber wagemutige Idee hat, Mathematik zu studieren, denn die Kluft zwischen Schule und Universität wird seit den Tagen von Felix Klein wohl beklagt, ist aber wohl Realität. Last but not least hoffe ich auch, dass die Neugierde etwas Neuartiges verstehen zu wollen, nicht ganz erloschen ist.

Die wohl wichtigste Reihe der Analysis ist die geometrische Reihe. Bekanntlich gilt

$$\frac{1}{1-a} = 1 + a + a^2 + a^3 + \dots \quad (1)$$

für alle reellen und komplexen Zahlen a mit $|a| < 1$ im folgenden Sinn:

$$\lim_{n \rightarrow \infty} (1 + a + a^2 + \dots + a^{n-1}) = \frac{1}{1-a}.$$

Dies bedeutet: Zu jedem $\epsilon > 0$ gibt es ein $N(\epsilon)$, sodass für alle $n \geq N(\epsilon)$ die Abschätzung

$$\left| 1 + a + a^2 + \dots + a^{n-1} - \frac{1}{1-a} \right| < \epsilon \quad (2)$$

richtig ist.

Setzt man in (1) $a = 1$, so erhält man rechts $\lim_{n \rightarrow \infty} \sum_{k=0}^{n-1} a^k = \infty$, also die

„Gleichung“ $\frac{1}{0} = \infty$, die zwar etwas unpräzise, aber intuitiv richtig ist. Bedenklicher wird die Sache, wenn man in (1) nun $a = -1$ setzt. Dies ergibt

$$\frac{1}{2} = 1 - 1 + 1 - 1 + \dots \quad (3)$$

Da die Partialsummen rechts zwischen 1 und 0 „schwanken“, ist die Reihe $\sum_{k=0}^{\infty} (-1)^k$ nicht konvergent. Genauer: Es ist $s_{2m} = 0$ und $s_{2m+1} = 1$, $m \geq 0$. Ein Statistiker wird daher einfach den Mittelwert bilden:

$$c_n = \frac{s_0 + s_1 + \dots + s_n}{n+1}. \quad (4)$$

Ist $n = 2m$, so erhält man $c_{2m} = \frac{1}{2} - \frac{1}{2m+1}$. Ist $n = 2m+1$, so erhält man $c_{2m+1} = \frac{1}{2}$. Daher ist $\lim_{n \rightarrow \infty} c_n = \frac{1}{2}$ und die Gleichung (3) ist als Mittelwert gerechtfertigt.

Dieser Gedanke lässt sich im folgenden Sinne ausbauen: Die unendliche Reihe $\sum_{k=0}^{\infty} a_k$ heißt *Cesàro konvergent*, wenn

$$\lim_{n \rightarrow \infty} \frac{s_0 + s_1 + \dots + s_n}{n+1}$$

existiert (dabei sei wie üblich $s_n = \sum_{k=0}^n a_k$). Es ist leicht zu sehen, dass jede Reihe, die (im gewöhnlichen Sinn) konvergent ist, auch Cesàro-konvergent ist. Es handelt sich daher um eine *Erweiterung* des Konvergenzbegriffs.

Nun wollen wir aber noch kühner werden. Wir setzen $a = 2$. Dann erhalten wir

$$-1 = 1 + 2 + 4 + 8 + 16 + \dots \quad (5)$$

Diese Gleichung scheint nun vollends Unsinn zu sein, da hilft auch kein Cesàromittel! Eine besonders fatale Wendung erhält die Sache durch folgende Überlegung: Angenommen, die Reihe rechts konvergiert. Es gelte etwa

$$s = 1 + 2 + 4 + 8 + 16 + \dots = \sum_{n=0}^{\infty} 2^n.$$

Dann gilt doch $2s + 1 = s$. Dies führt aber wiederum auf $s = -1$. Sofern die rechte Seite von (5) einen Sinn hat und man die üblichen Rechenregeln (d.h. die Rechenregeln eines Körpers) anwenden darf, so ist tatsächlich $s = -1$ die einzig vernünftige Antwort! Einen Ausweg bietet daher die Frage, ob man nicht erneut den Konvergenzbegriff verändern kann. Auf Kurt Hensel geht die Idee der p -adischen Zahlen zurück, die hier weiterhilft.

Im Konvergenzbegriff steckt bekanntlich der Betrag. Die Betragsfunktion ist eine Abbildung von \mathbb{Q} nach \mathbb{Q} (bzw. von \mathbb{R} nach \mathbb{R}) mit den Eigenschaften

- $|x| \geq 0$ und $|x| = 0$ genau dann, wenn $x = 0$.
- $|x + y| \leq |x| + |y|$
- $|xy| = |x||y|$.

Wir fixieren nun eine Primzahl p und stellen fest: Ist x eine von Null verschiedene rationale Zahl, so lässt sie sich in der Form

$$x = p^\alpha \frac{r}{s}$$

schreiben, wobei $\alpha \in \mathbb{Z}$ und $\frac{r}{s}$ ein gekürzter Bruch ist, dessen Zähler und Nenner nicht durch p teilbar sind.

Dann definieren wir die p -adische Bewertung wie folgt:

- $|0|_p := 0$
- $|x|_p := p^{-\alpha}$, wenn x wie oben beschrieben dargestellt ist.

Sei nun $x = p^\alpha \frac{r}{s}$ und $y = p^\beta \frac{u}{w}$ etwa. Der Satz von der Eindeutigkeit der Primfaktorzerlegung sichert nun

$$xy = p^{\alpha+\beta} \frac{ru}{sw},$$

also gilt $|xy|_p = |x|_p |y|_p$.

Sei weiters etwa $\alpha \leq \beta$. Dann ist

$$x + y = p^\alpha \frac{r}{s} + p^\beta \frac{u}{w} =$$

$$p^\alpha \left(\frac{r}{s} + p^{\beta-\alpha} \frac{u}{w} \right) = p^\alpha \left(\frac{rw + p^{\beta-\alpha} su}{sw} \right).$$

Ist $\alpha < \beta$, so ist p kein Teiler von $rw + p^{\beta-\alpha} su$. Dann ist $x + y = p^\alpha \frac{m}{n}$ und daher

$$|x + y|_p = |x|_p = \max(|x|_p, |y|_p).$$

Ist aber $\alpha = \beta$, so ist es denkbar, da p ein Teiler von $rw + su$ ist, und daher gilt

$$x + y = p^\gamma \frac{m}{n},$$

wobei $\gamma \geq \alpha$, d.h.

$$|x + y|_p \leq |x|_p = \max(|x|_p, |y|_p).$$

Auf jeden Fall gilt

$$|x + y|_p \leq |x|_p + |y|_p.$$

Es ist nicht unwichtig, aus dem Beweis mitzunehmen, dass für $|x|_p \neq |y|_p$ jedenfalls $|x + y|_p = \max(|x|_p, |y|_p)$ gilt!

Interpretiert man $|x|_p$ als neuen Abstand vom Nullpunkt, so erhält man eine merkwürdige Situation, die wir für $p = 7$ illustrieren wollen:

$|\frac{2}{49}|_7 = 49$, d.h. liegt weit weg! $|\frac{2}{5}|_7 = 1$, d.h. $\frac{2}{5}$ liegt auf dem Rand der 7-adischen „Einheitskugel“ $E = \{x \in \mathbb{Q} : |x|_7 \leq 1\}$. $|\frac{7}{2}|_7 = \frac{1}{7}$, d.h. $\frac{7}{2}$ liegt näher an $x = 0$ als $\frac{2}{49}$ oder $\frac{2}{5}$!

Es ist nun leicht zu überlegen, dass $|x - y|_p = p^{-\alpha}$, $\alpha \geq 1$ gleichbedeutend mit $x - y = p^\alpha k$, also mit $x \equiv y \pmod{p^\alpha}$ ist.

Wichtig ist folgende Beobachtung: Ist $|x - y|_p = p^{-\alpha}$ und $x' = x + tp^\alpha$, so ist

ebenfalls $|x' - y|_p = p^{-\alpha}$.

Der neue Abstand erlaubt nun, einen neuen Konvergenzbegriff zu definieren. Wir sagen

$$p - \lim_{n \rightarrow \infty} x_n = x,$$

wenn gilt: Zu jedem $\epsilon > 0$ gibt es ein $N(\epsilon)$, sodass für alle $n \geq N(\epsilon)$ gilt $|x_n - x|_p < \epsilon$.

Dazu nun zwei Beispiele!

$$2 - \lim_{n \rightarrow \infty} (1 + 2 + 4 + \dots + 2^n) = -1$$

Da $s_n = 2^n - 1$, erhält man $|s_n - (-1)|_2 = 2^{-n}$.

Ähnlich zeigt man, dass

$$7 - \lim_{n \rightarrow \infty} (1 + 7 + 49 + \dots + 7^n) = -\frac{1}{6}$$

gilt.

Aus diesen Beispielen gewinnt man den folgenden Satz.

Satz: Für jede Primzahl p gilt im Sinne der p -Konvergenz

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

Daraus folgt weiters:

Satz: Für jede Primzahl p gilt im Sinne der p -Konvergenz

$$\begin{aligned} -1 &= p - 1 + (p - 1)p + (p - 1)p^2 + \\ &\quad (p - 1)p^3 + \dots \end{aligned}$$

Bekanntlich ist das Problem, die Gleichung $x^2 = 2$ zu lösen, ein erster Schritt zur Erweiterung von \mathbb{Q} zum Körper \mathbb{R} der reellen Zahlen. Wegen $1 = 1^2 < 2 < 2^2 = 4$, ist $x_0 = 1$ eine (schlechte) Näherung für die gesuchte Zahl $\sqrt{2}$. Da $1,96 = 1,4^2 < 2 < 1,5^2 = 2,25$ ist eine bessere Näherung. Da $1,9881 = 1,41^2 < 2 < 1,42^2 = 2,0164$, ist $x_1 = 1 + \frac{4}{10} + \frac{1}{10^2}$ eine noch bessere Näherung. Auf diese Weise lässt sich eine Folge von Werten

$$x_n = 1 + \frac{\epsilon_1}{10} + \frac{\epsilon_2}{10^2} + \dots + \frac{\epsilon_n}{10^n}$$

herstellen, für die gilt

$$|x_n - x_{n+m}| < 10^{-n} \tag{6}$$

d.h. die Folge $(x_n), n \in \mathbb{N}$, ist eine Cauchyfolge und

$$\lim_{n \rightarrow \infty} x_n^2 = 2. \tag{7}$$

Da nun \mathbb{R} ein vollständiger Körper ist, hat die Cauchyfolge (x_n) , $n \in \mathbb{N}$, einen Grenzwert α und man setzt zu Recht $\alpha = \sqrt{2}$.

Geht so etwas mit p-Grenzwerten? Man kann es ja zumindest versuchen!

Wir wollen die Gleichung $x^2 = 2$ durch eine Folge rationaler Zahlen näherungsweise für $p = 7$ lösen.

Soll x_0 ein guter Startwert sein, so ist $|x_0^2 - 2|_7 < 1$ eine vernünftige Forderung. Also verlangen wir gleich $|x_0^2 - 2|_7 \leq \frac{1}{7}$, d.h. $x_0^2 \equiv 2 \pmod{7}$. Eine Lösung ist $x_0 = 3$. Nun ist für diesen Wert $|x_0^2 - 2|_7 \leq \frac{1}{7}$, aber es ist $|x_0^2 - 2|_7 > \frac{1}{49}$. Es ist daher naheliegend, in der Restklasse von 3 modulo 7 nach einer besseren Lösung Ausschau zu halten, also $x_1 = 3 + 7\epsilon_1$ anzusetzen. Dann erhält man

$$x_1^2 - 2 = 9 + 7.6\epsilon_1 + 7^2\epsilon_1^2 - 2 = 7(1 + 6\epsilon_1 + 7\epsilon_1^2).$$

Wenn 49 ein Teiler von $x_1^2 - 2$ gelten soll, genügt es daher zu fordern, dass 7 ein Teiler von $1 + 6\epsilon_1$ ist. Man sieht leicht, dass $\epsilon_1 = 1$ gewählt werden kann, also ist $x_1 = 10$ eine bessere Näherung, denn es ist nach Konstruktion $|x_1^2 - 2|_7 \leq \frac{1}{49}$. Dadurch ermutigt, probiert man $x_2 = 10 + 49\epsilon_2$. Will man erreichen, dass 343 ein Teiler von $x_2^2 - 2$ wird, so reicht $7/(2 + 20\epsilon_2)$. Dies leistet $\epsilon_2 = 2$. Somit ist $x_2 = 10 + 2.49$ eine erneute Verbesserung, und es gilt nun $|x_2^2 - 2|_7 \leq \frac{1}{343}$. Das Schema ist nun leicht erkennbar: Hat man

$$x_n = \epsilon_0 + 7\epsilon_1 + 7^2\epsilon_2 + \dots + 7^n\epsilon_n$$

mit $|x_n^2 - 2|_7 \leq \frac{1}{7^{n+1}}$ (gleichbedeutend mit $x_n^2 - 2 = 7^{n+1}z_n$) schon gefunden, so setzt man $x_{n+1} = x_n + 7^{n+1}\epsilon_{n+1}$. Dann ist

$$x_{n+1}^2 - 2 = 7^{n+1}(z_n + 2x_n\epsilon_{n+1} + 7^{n+1}\epsilon_{n+1}^2)$$

sicher durch 7^{n+1} teilbar, wenn $7/(z_n + 2x_n\epsilon_{n+1})$ gilt. Man muss also die Diophantische Gleichung

$$z_n + 2x_n\epsilon_{n+1} = 7\eta_{n+1}$$

lösen, wobei $\epsilon_{n+1} \in \{0, 1, 2, 3, 4, 5, 6\}$ gewählt werden muss. Bei kleinen Zahlen kommt man mit Ausprobieren der 7 Möglichkeiten durch; bei größeren Zahlen (oder vor allem, wenn wir statt $p = 7$ eine größere Primzahl wählen!) kann man Lösungen mittels des Euklidischen Algorithmus finden. Dafür eignet sich der Einsatz eines Computers!

Bevor wir „in der Theorie“ weitermachen, lohnt es sich, weitere Beispiele zu betrachten.

Wählt man den Startwert y_0 , so erhält man mit derselben Methode eine Folge von Näherungen $y_0 = 4, y_1 = 39, y_2 = 235, \dots$. Man kann eine Kontrolle verwenden: Es muss $x_n + y_n \equiv 0 \pmod{7^{n+1}}$ gelten!

Wir untersuchen (für $p=7$) die Gleichung $x^2 = 4$. Da der Startwert eine genaue Lösung darstellt, erhält man vom Startwert ausgehend keine Verbesserung; es ist stets $x_n = 2$. Beginnt man aber mit $y_0 = 5$, so erhält man die Folge $y_0 = 5, y_1 = 47, y_2 = 341, \dots$. Wiederum muss $x_n + y_n \equiv 0 \pmod{7^{n+1}}$ gelten. Man könnte in Vertrauen auf formales Rechnen diese Folge auch so erhalten. Es ist

$$-1 = 6 + 6.7 + 6.7^2 + 6.7^3 + \dots$$

Daher ist

$$\begin{aligned} -2 &= 12 + 12 \cdot 7 + 12 \cdot 7^2 + 12 \cdot 7^3 + \dots = \\ &5 + 13 \cdot 7 + 12 \cdot 7^2 + 12 \cdot 7^3 + \dots = \\ &5 + 6 \cdot 7 + 13 \cdot 7^2 + 12 \cdot 7^3 + \dots = \\ &5 + 6 \cdot 7 + 6 \cdot 7^2 + 13 \cdot 7^3 + \dots \end{aligned}$$

Daraus erhält man die Näherungen $y_0 = 5, y_1 = 5 + 42 = 47, y_2 = 47 + 294 = 341, \dots$

Ebenso kann man versuchen, die Gleichung $x^3 = 6$ für $p = 7$ näherungsweise zu lösen. Der Startwert $x_0 = 3$ ergibt eine Verbesserung $x_1 = 24$ usw.. Kehren wir zu unserem Beispiel $x^2 = 2$ zurück. Unser Algorithmus produziert nach Wahl eines geeigneten Startwertes ($x_0 = 3$ oder $x_0 = 4$) eine Folge ganzer Zahlen (x_n) mit den Eigenschaften:

$$|x_n - x_{n+m}| < 7^{-n-1}$$

und

$$7 - \lim_{n \rightarrow \infty} x_n^2 = 2.$$

Was fehlt, ist ein *vollständiger Körper*, der die Grenzwerte aller Cauchyfolgen (bezüglich der 7-Konvergenz) enthält. Die Beispiele legen nun nahe, es mit „Zahlen“ der Form

$$x = \frac{\epsilon_{-w}}{7^w} + \frac{\epsilon_{-w+1}}{7^{w-1}} + \dots + \frac{\epsilon_{-1}}{7} + \epsilon_0 + 7\epsilon_1 + 7^2\epsilon_2 + \dots$$

zu versuchen, denn das Problem von führt ja auch im Reellen zu einem unendlichen Dezimalbruch $\sqrt{2} = 1,41\dots$. Wir definieren daher

$$\mathbb{Q}_7 = \left\{ x = \sum_{i=w}^{\infty} \epsilon_i 7^i, 0 \leq \epsilon_i \leq 6 \right\}. \quad (8)$$

Addition und Multiplikation dieser 7-adischen Zahlen geschieht nun formal, wobei man allerdings die neuen Ziffern durch Überträge auf die Einschränkung $\epsilon_i \in \{0, 1, \dots, 6\}$ bereinigen muss!

$$\begin{aligned} x &= \frac{2}{7} + 4 + 3 \cdot 7 + 2 \cdot 7^2 + 1 \cdot 7^3 + \dots, \\ y &= \frac{6}{7} + 4 + 2 \cdot 7 + 5 \cdot 7^2 + 4 \cdot 7^3 + \dots \end{aligned}$$

Dann ist

$$\begin{aligned} x + y &= \frac{8}{7} + 8 + 5 \cdot 7 + 7 \cdot 7^2 + 5 \cdot 7^3 + \dots \\ &= \frac{1}{7} + 9 + 5 \cdot 7 + 7 \cdot 7^2 + 5 \cdot 7^3 + \dots = \end{aligned}$$

$$\frac{1}{7} + 2 + 6 \cdot 7 + 0 \cdot 7^2 + 6 \cdot 7^3 + \dots$$

Ebenso rechnet man nach

$$\begin{aligned} xy &= \frac{12}{49} + \frac{32}{7} + 38 + 42 \cdot 7 + \dots \\ &= \frac{12}{49} + \frac{4}{7} + 6 \cdot 7 + \dots \end{aligned}$$

Die 7-adische Bewertung lässt sich nun auf die Menge \mathbb{Q}_7 fortsetzen.

Definition: Ist $x = \sum_{i=w}^{\infty} \epsilon_i 7^i$, $\epsilon_w \neq 0$, so sei $|x|_7 := 7^{-w}$.

Ist $x \neq 0$, so lässt sich rekursiv ein Inverses x^* bestimmen. Dazu ein Beispiel!

Sei

$$x = \frac{2}{7} + 4 + 3 \cdot 7 + 2 \cdot 7^2 + 1 \cdot 7^3 + \dots$$

Da $|xx^*|_7 = |1|_7 = 1$ gelten soll und $|x|_7 = 7$ gilt, muss $|x^*|_7 = \frac{1}{7}$ sein. Daher setzen wir an

$$x^* = \eta_1 7 + \eta_2 7^2 + \eta_3 7^3 + \dots$$

und erhalten

$$1 = xx^* = 2\eta_1 + (4\eta_1 + 2\eta_2)7 + (3\eta_1 + 4\eta_2 + 2\eta_3)7^2 + \dots \quad (9)$$

Die Kongruenz $1 \equiv 2\eta_1 \pmod{7}$ ist zuerst zu lösen. Dies ergibt $\eta_1 = 4$. Dies wird oben eingesetzt und es verbleibt als nächste Kongruenz $0 \equiv 17 + 2\eta_2 \pmod{7}$. Hier findet man $\eta_2 = 2$. weiters findet man $\eta_3 = 6$. Somit ist

$$x^* = 4 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \dots$$

Es lohnt sich für das Anfangsstück die Probe zu machen.

Man kann mittels vollständiger Induktion beweisen, dass diese Verfahren (formales Ausmultiplizieren und rekursives Lösen) immer zielführend ist. Damit ist der Beweis für den zentralen Satz skizziert.

Satz: Die Menge aller p -adischen Zahlen

$$\mathbb{Q}_p := \left\{ x = \sum_{i=w}^{\infty} \epsilon_i p^i, \epsilon_i \in \{0, 1, \dots, p-1\} \right\}$$

ist ein Körper.

Auf Grund des rekursiven Verfahrens haben wir gezeigt, dass $x^2 = 2$ zwei Lösungen in \mathbb{Q}_7 besitzt:

$$\xi = 3 + 1 \cdot 7 + 2 \cdot 7^2 + \dots,$$

$$\eta = 4 + 5 \cdot 7 + 4 \cdot 7^2 + \dots$$

Nach dem Lehrsatz von Viète muss $\xi + \eta = 0$ gelten. Dies stimmt auch, wie man durch Addieren und Bilden der Überträge erkennt.

Satz: Der Körper \mathbb{Q}_p ist ein Erweiterungskörper von \mathbb{Q} .

Beweis: Wir notieren vier Schritte.

1. $0 \in \mathbb{Q}_p$
2. Ist n eine natürliche Zahl, so besitzt n eine Darstellung der Gestalt

$$n = \epsilon_0 + \epsilon_1 p + \dots + \epsilon_s p^s.$$

3. Ist $z = -n$, so multiplizieren wir $-1 = p - 1 + (p - 1)p + (p - 1)p^2 + \dots$ mit $n = \epsilon_0 + \epsilon_1 p + \dots + \epsilon_s p^s$ und erhalten eine Darstellung für z .
4. Daher ist $\mathbb{Z} \subseteq \mathbb{Q}_p$. Da aber \mathbb{Q}_p ein Körper ist, muss $\mathbb{Q} \subseteq \mathbb{Q}_p$ gelten.

Es ist übrigens nicht allzu schwierig zu beweisen, dass \mathbb{Q}_p ein vollständiger Körper ist: Jede p -Cauchyfolge hat einen p -Grenzwert in \mathbb{Q}_p . Aber leider ist \mathbb{Q}_p keineswegs algebraisch abgeschlossen! So enthält \mathbb{Q}_p keine Zahl mit $x^2 = 3$. Da die Kongruenz $x^2 \equiv 3 \pmod{7}$ nicht lösbar ist, gibt es keinen geeigneten Startwert für die Konstruktion einer Näherungsfolge! Eine Zahl x der Form $x = \sum_{i=0}^{\infty} \epsilon_i p^i$ müsste $x = \epsilon_0$ als Lösung liefern!

Zur Abrundung sei noch festgelegt: Ist $x = \sum_{i=w}^{\infty} \epsilon_i p^i$, $\epsilon_w \neq 0$, so sei $|x|_p := p^{-w}$.

Eine hübsche Übungsaufgabe für Algebrahungrige ist nun folgendes Ergebnis:

Satz: Sei $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ die Menge der *ganzen p -adischen Zahlen*. Dann gilt

1. \mathbb{Z}_p ist ein Integritätsbereich
2. Sei $p\mathbb{Z} := \{w \in \mathbb{Z} : p/w\}$ und $I_p := \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Dann ist $p\mathbb{Z}$ ein Ideal in \mathbb{Z} und I_p ein Ideal in \mathbb{Z}_p .
3. Für die Restklassenringe gilt die Isomorphie

$$\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p/I_p.$$

Das nachstehende Ergebnis verallgemeinert ein bekanntes Ergebnis über \mathbb{Q} als Teilmenge von \mathbb{R} .

Satz: Sei $x \in \mathbb{Q}_p$. Dann ist $x \in \mathbb{Q}$ genau dann, wenn die Entwicklung $x = \sum_{i=w}^{\infty} \epsilon_i p^i$ periodisch wird.

Beweis: Da $x \in \mathbb{Q}$ genau dann gilt, wenn $p^w x \in \mathbb{Q}$ gilt, genügt es den Fall $|x|_p = 1$ zu betrachten.

Sei $x = \sum_{i=0}^{\infty} \epsilon_i p^i$ und $\epsilon_i = \epsilon_{i+s}$, $i = 0, 1, 2, \dots$ (d.h. x hat eine rein periodische Entwicklung, was keine Einschränkung ist). Dann ist

$$x = \sum_{i=0}^{s-1} \epsilon_i p^i + p^s x,$$

also

$$x = \frac{\sum_{i=0}^{s-1} \epsilon_i p^i}{1 - p^s},$$

d. h. eine rationale Zahl.

Etwas mühseliger ist die andere Richtung des Beweises. Sei x eine rationale Zahl mit $|x|_p = 1$. Dann schreiben wir $x = \frac{A}{B}$ mit $\text{ggT}(A, p) = \text{ggT}(B, p) = 1$ und $B \geq 1$.

Sei nun

$$\frac{A}{B} = \epsilon_0 + \epsilon_1 p + \epsilon_2 p^2 + \dots$$

Dann ist

$$\frac{1}{p} \left(\frac{A}{B} - \epsilon_0 \right) = \frac{A - \epsilon_0 B}{pB} = \frac{A'}{B}$$

(denn es wurde ϵ_0 ja so gewählt, dass $A - \epsilon_0 B$ durch p teilbar ist!). Dann ist $|A'| \leq \frac{|A|}{p} + \frac{|\epsilon_0 B|}{p} \leq \frac{|A|}{p} + B$.

Die Wiederholung des Verfahrens zeigt nun

$$\frac{1}{p} \left(\frac{A'}{B} - \epsilon_0 \right) = \frac{A' - \epsilon_0 B}{pB} = \frac{A''}{B}$$

mit $|A''| \leq \frac{|A'|}{p} + \frac{|\epsilon_0 B|}{p} \leq \frac{|A|}{p^2} + B(1 + \frac{1}{p})$. Mittels Induktion erkennt man daher

$$\begin{aligned} \frac{1}{p^n} \left(\frac{A}{B} - (\epsilon_0 + \epsilon_1 p + \epsilon_2 p^2 + \dots + \epsilon_{n-1} p^{n-1}) \right) \\ = \frac{A^{(n)}}{B}, \end{aligned}$$

wobei

$$|A^{(n)}| \leq \frac{|A|}{p^n} + B \left(1 + \frac{1}{p} + \dots + \frac{1}{p^{n-1}} \right) \leq \frac{|A|}{p^n} + \frac{pB}{p-1}.$$

Daher kann es nur endlich viele verschiedene ganze Zahlen $A^{(n)}$ geben, und es muss für ein Paar n und m die Beziehung $A^{(n)} = A^{(n+m)}$ gelten, d.h. die Entwicklung wird periodisch.

Literaturhinweis: F. Q. Gouvêa: *p-adic Numbers*. Springer-Verlag 1991.