Christian Semrau, Alexandra Merz **WS 02/03**

Kapitel II. Der Körper $\mathbb{Q}_p$

aus: Jean Pierre Serre: A course in arithmetics

Begleitmaterial zum Seminar
"Quadratische Formen über p-adischen Zahlen"
an der LMU München

Die folgenden Rechenbeispiele dienen der Veranschaulichung der p-adischen Zahlen $\mathbb{Q}_p$ und der p-adischen ganzen Zahlen $\mathbb{Z}_p$. Kenntnisse über den Aufbau von $\mathbb{Z}_p$ und $\mathbb{Q}_p$ (auch die Darstellbarkeit als Potenzreihe), die Definition der Rechenoperationen in $\mathbb{Q}_p$ sowie über das Rechnen mit natürlichen Zahlen in g-adischer Darstellung werden vorausgesetzt.

1 Darstellung

Die p-adischen ganzen Zahlen $\mathbb{Z}_p$, mit denen wir uns zunächst beschäftigen, werden hier in ihrer Potenzreihenform dargestellt mit führender Periode. Wir wählen hier durchgehend $p = 5$, damit wir genug Ziffern haben, um einigermaßen interessante Rechnungen durchzuführen. Natürliche Zahlen werden so dargestellt, wie man sie von der gewöhnlichen g-adischen Zahlendarstellung kennt, wobei g die Basis des Ziffernsystems ist. Zur Unterscheidung verwenden wir den Index 10 für Dezimalzahlen und eine unendlich lange Darstellung (bei natürlichen Zahlen eine Nuller-Periode) für 5-adische Zahlen.
$0_{10} = \ldots 000 = \overline{0}, \quad 4_{10} = \ldots 0004 = \overline{0}4, \quad 5_{10} = \overline{0}10, \quad 102_{10} = \overline{0}402.$

2 Addition

Natürliche Zahlen addiert man wie bei der schriftlichen Addition, wobei man auch hier Überträge zu beachten hat. Das sollte kein Problem sein.
$\overline{0}1 + \overline{0}2 = \overline{0}3, \quad \overline{0}2 + \overline{0}3 = \overline{0}10 = 5_{10}, \quad 24_{10} + 1_{10} = \overline{0}44 + \overline{0}1 = \overline{0}100 = 25_{10}$

Übung. Stelle die Zahlen 12_{10}, 54_{10} und 33_{10} zur Basis 5 dar und berechne die Summe der drei Zahlen.

Da jede Ziffernfolge eine p-adische Zahl darstellt, gibt es auch p-adische Zahlen, deren Potenzreihendarstellung nicht abbricht (keine Nuller-Periode hat). Eine einfache ist die Zahl $\overline{4} = \ldots 44444$. Welchen Wert hat sie? Das finden wir leicht heraus, wenn wir sie zu 1 addieren.

$\ldots 444444$	
$\ldots 000001$	+
$\ldots 111111$	(Übertrag)
$\ldots 000000$	

Zu diesem unendlich langen Übertrag-Durchreichen mache man sich klar: Es gibt keine Stelle, an der nicht die Ziffernsumme $4 + 0 + 1 = 10$ steht, durch welche diese Stelle den Wert 0 bekommt und einen Übertrag von 1 weitergibt. Da alle Ziffern 0 sind, ist das Ergebnis 0.
Aus dieser Rechnung folgt, dass $\overline{4}$ das additiv Inverse von 1 sein muss, also den Wert -1_{10} hat. Die Zahl -1_{10} hat in jedem $\mathbb{Z}_p$ die Form $\sum_{n=0}^{\infty}(p-1)p^n$.

Übung. Berechne $\overline{4}3 + \overline{0}2, \overline{4}40 + \overline{0}10, \overline{4001}1223344 + \overline{0443}3221101$.

Man erkennt, dass man eine Zahl negiert, indem man jede Ziffer von $p-1$ abzieht und zum Ergebnis dieser Operation die Zahl 1 addiert. (Im Computer wird diese Art der Darstellung negativer ganzer Zahlen benutzt, allerdings mit einer auf 16, 32 oder 64 begrenzten Binärstellenzahl. Dort heisst sie „Zweierkomplement“.) Durch diese Darstellung muss man beim Addieren nicht auf das Vorzeichen der Summanden achten (wobei in $\mathbb{Z}_p$ kein Vorzeichen mehr sinnvoll definiert werden kann, was man spätestens sieht, wenn wir die Quadratwurzel von -1 in $\mathbb{Z}_5$ berechnen).
Addieren wir noch ein paar unendlich lange Zahlen miteinander.
$\overline{2}22 + \overline{2}22 = \overline{4}44, \quad \overline{2}23 + \overline{2}23 = \overline{0}01, \quad \overline{2}22 + \overline{0}01 = \overline{2}23.$
Offenbar ist das Doppelte von $\overline{2}2$ gleich -1, also muss diese Zahl den Wert $\frac{-1}{2}$ haben. Ebenso ist $\overline{2}3$ eine Darstellung von $\frac{1}{2}$, denn sein Doppeltes ist $+1$. Das passt auch zur dritten Rechnung: $\frac{-1}{2} + 1 = \frac{1}{2}$. Wie man sieht, sind in den „p-adischen ganzen Zahlen“ nicht nur ganze Zahlen zu finden.

3 Multiplikation

Multiplizieren kann man die Zahlen wie man es gewohnt ist mit der schriftlichen Multiplikation, man muß nur die andere Basis beachten. Es kann bei der Multiplikation unendlich langer Zahlen vorkommen, dass sich die Überträge bis ins Unendliche fortsetzen. Die Anzahl der zu addierenden Zeilen steigt zwar mit der Anzahl der zu berechnenden Stellen, trotzdem steht jede Stelle des Produkts nach einer von den Faktoren unabhängigen endlichen Anzahl von Additionen und einstelligen Multiplikationen fest. (Anders als beim Dezimalsystem, wo man schon beim Addieren von zwei ziffernweise gegebenen Dezimalbrüchen nie vorher weiss, wie viele Stellen der Summanden man betrachten muss, um eine bestimmte Stelle der Summe zu ermitteln.)

```
 1123 * 301
------------
      1123
     3424
------------
    344023
============
```

```
 ...2222 * 2
-------------
   ...44444
=============

 ...2223 * 2
-------------
   ...00001
=============
```

```
 ...2223 * ...3333
-------------------
      ...2222224
     ...2222224
    ...2222224
   ...2222224
        ...
-------------------
     ...4141414
===================
```

```
 ...2223 * ...2223
-------------------
      ...2222224
     ...0000001
    ...0000001
   ...0000001
        ...
-------------------
     ...3333334
===================
```

An den Rechnungen im zweiten Block sehen wir noch einmal, dass $\overline{2}2 = (\frac{-1}{2})_{10}$ und $\overline{2}3 = (\frac{1}{2})_{10}$.

Übung. Berechne $\overline{1}11 * \overline{0}4$, $\overline{14} * \overline{0}13$, $\overline{0} - \overline{1}11$, $\overline{1}1 * \overline{1}1$ und ermittle die dezimalen Werte der beteiligten Zahlen.

Mir scheint, dass es in $\mathbb{Z}_p$ genauso schwierig ist, die Periodenlänge eines Produkts zu bestimmen, wie im Dezimalsystem.

4 Division

Die schriftliche p-adische Division unterscheidet sich von der Schulmethode durch die Arbeitsrichtung. Bei der Schulmethode fangen wir vorn an und arbeiten uns nach hinten über das Komma hinaus und erhalten vielleicht unendlich viele Nachkommastellen (oder haben einen Rest von 0 oder erkennen eine Periode). Bei den p-adischen Zahlen haben wir dagegen unendlich viele Vorkommastellen, daher kehren wir die Richtung um und fangen bei der Einerstelle an und arbeiten uns nach links (gegebenenfalls bis wir einen Rest 0 haben oder eine Periode erkennen).
Wenn die Division glatt aufgeht, dann funktioniert das auch im Dezimalsystem. Wir machen daher erst ein Beispiel mit Dezimalzahlen.

Schulmethode	„10-adisch“
1368 : 3 = 456	1368 : 3 = 456
-12	-18
16	135
-15	-15
18	12
-18	-12
0	0

Nun eine Berechnung in $\mathbb{Z}_5$.

Vielfache von 3	Division	Ergebnis
	1 : 3 = 132	
3 * 0 = 0	-11	Zwei Reste stimmen überein,
3 * 1 = 3	...444	wir haben also eine
3 * 2 = 11	-14	Periode gefunden.
3 * 3 = 14	...443	
3 * 4 = 22	-3	Damit ist $1 : 3 = \overline{132}$
	...444	

Wir haben nun $(\frac{1}{3})_{10} = \overline{132}$ in $\mathbb{Z}_5$ berechnet, indem wir 1 durch 3 geteilt haben. Genau so kann man nun beliebige p-adische Zahlen dividieren. (Wenn wir die Multiplikationen und Subtraktionen auf den einzelnen Stufen solange verzögern, bis die Stelle des Ergebnisses gebraucht wird, dann benötigen wir auch bei der Division für jede Stelle des Quotienten eine von Dividend und Divisor unabhängige endliche Anzahl von Rechenschritten.)
Eine kleine Neuheit bietet die Division durch p, die in $\mathbb{Z}_p$ nicht immer möglich ist. Zu diesem Zweck wird der Körper $\mathbb{Q}_p$ konstruiert, bei dem die Zahlen endlich viele Nachkommastellen haben können. Bei der Division durch p verschieben sich die Ziffern des Dividenden um eine Stelle nach rechts, es ist also $(\frac{1}{5})_{10}$ gleich $\overline{0}1 : \overline{0}10 = \overline{0}.1$ in $\mathbb{Q}_5$.

5 Wurzelziehen

Wie bei allen anderen Rechenarten ist es auch hier das Ziel, die Ziffern des Ergebnisses von rechts nach links zu berechnen. Bei Primzahlen $p > 2$ ist es für die Existenz einer Quadratwurzel einer p-adischen Einheit (eine Zahl, deren letzte Ziffer nicht 0 ist) notwendig und hinreichend, dass die letzte Ziffer ein Quadrat modulo p ist.
Diese letzte Ziffer ist auch die einzige, wo das Ziehen einer Quadratwurzel notwendig ist. Die restlichen Stellen ergeben sich durch das Lösen linearer Kongruenzen, deren Koeffizienten aus den bisher gewonnenen Stellen berechnet werden.

Wir bestimmen $\sqrt{-1}$ in $\mathbb{Z}_5$. Beachte, dass -1 zwei Quadratwurzeln hat, denn mit einer Wurzel ist auch das Negative eine Wurzel. Der Ausdruck $\sqrt{-1}$ ist also im Falle der Existenz nur „bis aufs Vorzeichen“ bestimmt (wie aber schon gesagt, gibt es keine positiven oder negativen p-adischen Zahlen). Ausserdem ist diese Zahl nicht periodisch. Man kann zeigen, dass jede periodische p-adische Zahl rational ist (indem man sie ähnlich wie im Dezimalsystem in einen gemeinen Bruch ganzer Zahlen umwandelt), und eine Quadratwurzel von -1 ist sicher nicht rational.
Achtung: Wir rechnen jetzt mit 5-adischen Zahlen ohne das gesondert zu markieren!
$(-1)_{10} = \overline{4}$, also lösen wir $x^2 \equiv 4 \pmod{10}$ und erhalten die zwei Lösungen $x = 2, x = 3$. Jede dieser beiden Zahlen führt zu einer Quadratwurzel von $\overline{4}$. Berechnen wir diejenige, deren letzte Ziffer die 2 ist.
$(10x + 2)^2 = 10^2x^2 + 10 \cdot 2 \cdot 2 \cdot x + 2^2 \equiv 44 \pmod{10^2}$
Die Einerziffern heben sich auf und der 10^2-Summand verschwindet, so können wir die Kongruenz durch 10 teilen: $2 \cdot 2 \cdot x \equiv 4 \pmod{10}$
Diese lineare Kongruenz liefert $x = 1$, also endet unser Ergebnis mit $\ldots 12$.
$(10^2x + 12)^2 = 10^4x^2 + 10^2 \cdot 2 \cdot 12 \cdot x + 12^2 \equiv 444 \pmod{10^3}$.
Da $12^2 = 144$, erhalten wir $2 \cdot 2 \cdot x + 1 \equiv 4 \pmod{10}$ mit der Lösung $x = 2$. Damit haben wir $\ldots 212$ als Ergebnis.
$(10^3x + 212)^2 \equiv 10^3 \cdot 2 \cdot 212 \cdot x + 212^2 \equiv 4444 \pmod{10^4}$.
Es ist $212^2 = (200 + 12)^2 = 40000 + 2 \cdot 200 \cdot 12 + 144 = 100444$, wir lösen $2 \cdot 2 \cdot x + 0 \equiv 4 \pmod{10}$ und haben $x = 1$ und damit $\sqrt{\overline{4}} = \ldots 1212$.
Auf 20 Stellen genau hat -1 die beiden Quadratwurzeln $\ldots 40423140223032431212$ und $\ldots 04021304221412013233$. Wie zu erwarten sind das genau die Negativen voneinander.

6 Das ganze in $\mathbb{Q}_2$

Kommt noch. Müssen erst ein bisschen damit spielen und rumrechnen. Es gibt keine Unterschiede bei Addition und Multiplikation. Ob die Division anders ist, werden wir sehen. Beim Wurzelziehen gibt es sicher was Neues.

Christian Semrau
Alexandra Merz
23.12.2002, letzte Aktualisierung: 05.08.2004