Die p-adischen Zahlen

Definition *p-adische Zahlen*

Sei $p \in \mathbb{P}$. Wir definieren die *ganzen p-adischen Zahlen* als

$$\mathbb{Z}_p := \{(x_k) \in \prod_{k=0}^{\infty} \mathbb{Z}/p^{k+1}\mathbb{Z} \mid x_{k+1} \equiv x_k \mod p^{k+1}\}.$$

Ferner definieren wir $\epsilon : \mathbb{Z} \to \mathbb{Z}_p$ mit $x \mapsto (x)_{k \in \mathbb{N}_0} = (x, x, x, \ldots)$.

Bsp: In $\mathbb{Z}_3$ erhalten wir

- $\epsilon_3(-1) = (-1, -1, -1, -1, -1, \ldots) = (2, 8, 26, 80, 242, \ldots)$.
- $\epsilon_3(101) = (101, 101, 101, \ldots) = (2, 2, 20, 20, 101, 101, \ldots)$.
- Aus dem Beispiel auf der Folie zuvor erhalten wir in $\mathbb{Z}_7$
$$\sqrt{\epsilon_7(2)} = (3, 10, 108, 2166, 4567, \ldots).$$

Reduzierte und Potenzreihen-Darstellung

Definition Reduzierte und Potenzreihen-Darstellung

Ein $(x_k) \in \mathbb{Z}_p$ ist in *reduzierter Darstellung* falls $0 \leq x_k < p^{k+1}$.
Sei (x_k) in reduzierter Darstellung und $x_{-1} := 0$. Die *Potenzreihen-Darstellung* von (x_k) ist $\sum_{k=0}^{\infty} c_k p^k$ mit $c_k := \frac{x_k - x_{k-1}}{p^k}$.

Anmerkungen:

- Aus $x_k \equiv x_{k-1} \mod p^k$ folgt $p^k | x_k - x_{k-1}$ bzw. $c_k \in \mathbb{Z}$.
- Gleichfalls gilt $x_k = c_k p^k + x_{k-1}$.
- Wegen $0 \leq x_k < p^{k+1}$ und $0 \leq x_{k-1} < p^k$ folgt $0 \leq c_k < p$.

Bsp: Für die Beispiele zuvor erhalten wir folgende Potenzreihen.

- $101 = 2 \cdot 3^0 + 2 \cdot 3^2 + 1 \cdot 3^4$.
- $-1 = \sum_{i=0}^{\infty} 2 \cdot 3^i$. Für alle $p \in \mathbb{P}$ gilt $-1 = \sum_{i=0}^{\infty} (p-1)p^i$, da $\sum_{i=0}^{\infty}(p-1)p^i = \sum_{i=0}^{\infty} p^{i+1} - \sum_{i=0}^{\infty} p^i = \sum_{i=1}^{\infty} p^i - \sum_{i=0}^{\infty} p^i = (-1)$.
- $\sqrt{\epsilon_7(2)} = (3, 1, 2, 6, 2, \ldots)$.

Addition und Multiplikation in $\mathbb{Z}_p$

Addition und Multiplikation in $\mathbb{Z}_p$:

- Wir addieren und multiplizieren Potenzreihen wie gewöhnlich.
- Durch Überträge bringen wir die Koeffizienten wieder in $[0, p-1]$.
- **Bsp:** Berechne das Doppelte von $(1 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2) = 25$.

$$\begin{array}{rrrrl} & 2 \cdot 3^0 + & 4 \cdot 3^1 + & 4 \cdot 3^2 & \\ = & 2 \cdot 3^0 + & (3+1) \cdot 3^1 + & (3+1) \cdot 3^2 & \\ = & 2 \cdot 3^0 + & 1 \cdot 3^1 + & 2 \cdot 3^2 & +1 \cdot 3^3 = 50. \end{array}$$

- **Bsp:** Berechne $(3 \cdot 5^0 + 2 \cdot 5^1)(4 \cdot 5^0 + 1 \cdot 5^1) = 13 \cdot 9$.

$$\begin{array}{rrrrl} & (3 \cdot 4) \cdot 5^0 + & (3 \cdot 1 + 2 \cdot 4) \cdot 5^1 + & (2 \cdot 1) \cdot 5^2 & \\ = & (2 \cdot 5 + 2) \cdot 5^0 + & (2 \cdot 5 + 1) \cdot 5^1 + & 2 \cdot 5^2 & \\ = & 2 \cdot 5^0 + & 3 \cdot 5^1 + & 4 \cdot 5^2 & = 117. \end{array}$$

- $(\mathbb{Z}_p, +, \cdot)$ ist ein kommutativer Ring.

Hensels Lemma

Lemma von Hensel

Sei $f \in \mathbb{Z}_p[X]$ und $\tilde{x} \in \mathbb{Z}_p$ mit $f(\tilde{x}) \equiv 0 \mod p^k$ für ein $k \in \mathbb{N}$. Für ein $a \in \mathbb{Z}$ gilt $f(\tilde{x} + ap^k) \equiv 0 \mod p^{k+1}$ gdw $f'(\tilde{x})a \equiv -\frac{f(\tilde{x})}{p^k} \mod p$.

Beweis:

- Sei $d = \mathrm{grad}(f)$. Wir schreiben f als Polynom in $X - \tilde{x}$, d.h.
$$f(X - \tilde{x}) = \sum_{i=0}^{d} c_i (X - \tilde{x})^i \text{ mit } c_i \in \mathbb{Z}_p.$$
- Es folgt $f(\tilde{x}) = c_0$ und $f'(\tilde{x}) = c_1$. Damit gilt
$$f(\tilde{x} + ap^k) = \sum_{i=0}^{d} c_i (ap^k)^i \equiv f(\tilde{x}) + f'(\tilde{x})ap^k \mod p^{k+1}.$$
- Wir erhalten also $f(\tilde{x} + ap^k) \equiv 0 \mod p^{k+1}$ gdw
$$f'(\tilde{x})ap^k \equiv -f(\tilde{x}) \mod p^{k+1} \Leftrightarrow f'(\tilde{x})a \equiv -\frac{f(\tilde{x})}{p^k} \mod p.$$

Existenz der Liftungen

Korollar

Sei $f \in \mathbb{Z}_p[X]$ und $\tilde{x} \in \mathbb{Z}_p$ mit $f(\tilde{x}) \equiv 0 \mod p$ und $f'(\tilde{x}) \not\equiv 0 \mod p$. Dann existiert ein eindeutiges $x \in \mathbb{Z}_p$ mit $f(x) = 0$ und $x \equiv \tilde{x} \mod p$.

Anmerkungen:

- Aus Hensels Lemma folgt die Eindeutigkeit von $a \mod p$.
- Die Bedingung $f(\tilde{x}) \equiv 0 \mod p$ und $f'(\tilde{x}) \not\equiv 0 \mod p$ bedeutet, dass $\tilde{x}$ eine einfache Nullstelle von f ist.
- Damit lässt sich jede einfache Nullstelle von f modulo p eindeutig zu einer Nullstelle von f in $\mathbb{Z}_p$, d.h. modulo aller p^k, liften.

Beispiel: Liften modulo 7

Bsp: Wir berechnen alle Nst von $f(X) = X^3 + X^2 + 4X + 1 \bmod 49$.

- Wir bestimmen zunächst die Lösungen modulo 7. Es gilt $f(1) = 7 \equiv 0 \bmod 7$, $f(2) = 21 \equiv 0 \bmod 7$ und $f(3) = 49 \equiv 0 \bmod 7$.
- Damit sind $1, 2$ und 3 alle Nullstellen modulo 7.
- Für die Ableitung $f'(X) = 3X^2 + 2X + 4$ gilt
$$f'(1) \equiv 2 \bmod 7,\ f'(2) \equiv (-1) \bmod 7 \text{ und } f'(3) \equiv 2 \bmod 7.$$
- Damit können wir alle Nullstellen anheben. Wir berechnen $\bmod 7$ $a_1 \equiv -\frac{7}{7} \cdot 2^{-1} \equiv 3$, $a_2 \equiv -\frac{21}{7} \cdot (-1)^{-1} \equiv 3$ und $a_3 \equiv -\frac{49}{7} \cdot 2^{-1} \equiv 0$.
- Damit erhalten wir modulo 49 genau die drei Nullstellen.
$$x_1 = 1 + 3 \cdot 7 = 22,\ x_2 = 2 + 3 \cdot 7 = 23 \text{ und } x_3 = 3 + 0 \cdot 7 = 3.$$

Beispiel: Liften modulo 2

Bsp: Wir berechnen alle Nullstellen von $f(X) = X^2 + 7 \bmod 16$.

- Modulo 2 ist 1 die einzige Nst. Es gilt aber $f'(X) = 2X \equiv 0 \bmod 2$.
- Nach Hensels Lemma kann eine Nullstelle $\tilde{x} \bmod 2^k$ in diesem Fall angehoben werden gdw $\frac{f(\tilde{x})}{2^k} \equiv 0 \bmod 2$.
- Falls $\tilde{x}$ angehoben wird, dann zu $\tilde{x}$ *und* $\tilde{x} + p^k$.
- Für $k = 1$ gilt $\frac{f(1)}{2} = \frac{8}{2} = 4 \equiv 0 \bmod 2$.
- D.h. wir erhalten die Nullstellen 1 und 3 modulo 4.
- Für $k = 2$ gilt $\frac{f(1)}{4} = \frac{8}{4} \equiv 0 \bmod 2$ und $\frac{f(3)}{4} = \frac{16}{4} \equiv 0 \bmod 2$.
- D.h. wir erhalten die vier Nullstellen $1, 5, 3$ und 7 modulo 8.
- Für $k = 3$ gilt modulo 2
$$\frac{f(1)}{8} = \frac{8}{8} \equiv 1,\ \frac{f(3)}{8} = \frac{16}{8} \equiv 0,\ \frac{f(5)}{8} = \frac{32}{8} \equiv 0 \text{ und } \frac{f(7)}{8} = \frac{56}{8} \equiv 1.$$
- D.h. 3 wird modulo 16 zu 3 und 11 geliftet und 5 zu 5 und 13.
- Für $k > 3$ kann man zeigen, dass stets 2 Nst angehoben werden.
- Dies führt schließlich zu zwei 2-adischen Lösungen
$$x_1 = (1, 1, 5, 5, \ldots) \text{ und } x_2 = (1, 3, 3, 11, \ldots).$$

Lösen von Gleichungen modulo n

Algorithmus Lösen von Gleichungen modulo n

EINGABE: $n = \prod_{i=1}^{s} p_i^{e_i}$, Polynom $f(X) \in \mathbb{Z}[X]$

1. For $i = 1, \ldots, s$: Bestimme Nullstellen von $f(X) \bmod p_i$.
   1. For $j = 2, \ldots, e_i$: Lifte Nullstellen modulo p_i^j.
2. Setze Nullstellen modulo $p_1^{e_1}, \ldots, p_s^{e_s}$ mittels CRT zusammen.

AUSGABE: Alle Nullstellen von $f(X)$ modulo n

Bsp: Wir bestimmen alle Nullstellen von $f(X) = X^2 + 7 \bmod 2^3 \cdot 11$.

- Modulo 8 kennen wir bereits die Lösungen $1, 3, 5, 7$.
- Modulo 11 gilt $f(X) \equiv X^2 - 4$, d.h. die Lösungen sind $2, -2 \equiv 9$.
- Damit erhalten wir in $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ die Lösungen
  $$(1,2), (1,9), (3,2), (3,9), (5,2), (5,9), (7,2) \text{ und } (7,9).$$
- Modulo 88 sind dies alle 8 Lösungen
  $$57, 9, 35, 75, 13, 53, 79 \text{ und } 31.$$