Einheiten und Quadrate in den p-adischen Zahlen

Proseminar: Quadratische Formen
Universität Bielefeld – SS 2018 – Dr. Jan Geuenich

Johannes Krah

14. Mai 2018

1 Approximation von Loesungen p-adischer Gleichungen

Zur Erinnerung: Wir betrachen den Ring $\mathbb{Z}_p = \{(x_n)_{n\geq 1} | \forall n : x_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ und } x_n = can(x_{n+1})\}$, sowie seinen Quotientenkoerper $\mathbb{Q}_p$ und Bewertungsfunktion ν_p mit $x = p^{\nu_p(x)}u, u \in \mathbb{Z}_p^\times$.

Lemma 1.1. *Sei $f \in \mathbb{Z}_p[X]$ ein Polyonom mit seiner Ableitung f'. Sei weiter $x \in \mathbb{Z}_p, n, k \in \mathbb{N}_0$ mit $2k < n, f(x) \equiv 0 \ (mod\ p^n), \nu_p(f'(x)) = k$. Dann existiert eine Stelle $y \in \mathbb{Z}_p$, so dass*

$$f(y) \equiv 0 \ (mod\ p^{n+1}), \nu_p(f'(y)) = k, y \equiv x \ (mod\ p^{n-k}). \tag{1.1}$$

Beweis. Betrachten wir zunaechst ein beliebiges $y \in \mathbb{Z}_p$ der Form $y = x + p^{n-k}z$ mit $z \in \mathbb{Z}_p$. Durch Anwendung der Taylorformel 1.3 auf f am Entwicklungspunkt x erhalten wir:

$$f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a \text{ wobei } a \in \mathbb{Z}_p. \tag{1.2}$$

Nach Voraussetzung ist nun $f(x) = p^n b, b \in \mathbb{Z}_p$ und $f'(x) = p^k c, c \in \mathbb{Z}_p^\times$. Waehlen wir nun geschickt $z \in \mathbb{Z}_p$ erhalten wir:

$$b + zc \equiv 0 \ (\text{mod } p). \tag{1.3}$$

Dies koennen wir in oben gewonnene Form von $f(y)$ einsetzen:

$$f(y) = p^n(b + zc) + p^{2n-2k}a \equiv 0 \ (\text{mod } p^{n+1}), \tag{1.4}$$

da nach Voraussetzung auch $2n - 2k > n$ ist. Wenden wir noch einmal 1.3 auf f' am Entwicklungspunkt x an, erhalten wir.

$$f'(y) \equiv p^k c \ (\text{mod } p^{n-k}). \tag{1.5}$$

Da nach Voraussetzung $n - k > k$ ist nach Konstruktion von ν_p

$$\nu_p(f'(y)) = k. \tag{1.6}$$

□

Satz 1.2. *Sei nun $f \in \mathbb{Z}_p[X_1, ..., X_m], x = (x_1, ..., x_m) \in (\mathbb{Z}_p)^m, n, j \in \mathbb{N}, k \in \mathbb{N}_0$, so dass $j \leq m$. Wenn nun*

$$2k < n, f(x) \equiv 0 \ (mod\ p^n), \nu_p\Big(\frac{\partial f}{\partial X_j}(x)\Big) = k. \tag{1.7}$$

Dann hat f eine Nullstelle $y \in (\mathbb{Z}_p)^m$, die der Gleichung $y \equiv x \ (mod\ p^{n-k})$ genuegt.

Beweis. Wir behandeln zunaechst den Fall $m = 1$. Dafuer konstruieren wir eine Folge $(x_n)_{n\geq 0} \subseteq \mathbb{Z}_p$, vermoege $x_0 := x$ und x_1, so dass

$$x_1 \equiv x_0 \pmod{p^{n-k}}, f(x_1) \equiv 0 \pmod{p^{n+1}}, \nu_p(f'(x_1)) = k, \tag{1.8}$$

indem wir Lemma 1.1 anwenden.
Induktives Anwenden von 1.1 ergibt unsere Folge mit

$$x_{q+1} \equiv x_q \pmod{p^{n+q-k}}, f(x_q) \equiv 0 \pmod{p^{n+q}}, \nu_p(f'(x_q)) = k, \tag{1.9}$$

Anhand der Defintion von ν_p sieht man leicht, dass dies eine Cauchy-Folge ist, welche wegen der Vollstaendigkeit von $\mathbb{Z}_p$ gegen ein $y \in \mathbb{Z}_p$ konvergiert. Fuer $y = \lim_{n\to\infty} x_n$ gilt dann:

$$y \equiv x \pmod{p^{n-k}}, f(y) = 0, \nu_p(f'(y)) = k. \tag{1.10}$$

Behandeln wir nun den Fall $m > 1$. Dieser reduziert sich aber zum Fall $m = 1$, indem wir alle $x_i, i \neq j$ festhalten. Präziser: Wir setzen gerade für alle $X_i, i \neq j$ unsere $x_i \in \mathbb{Z}_p$ ein, erhalten mit obigem Teil ein $y_j \in \mathbb{Z}_p$ mit $y_j \equiv x_j \pmod{p^{n-k}}$ und $f((x_1, ...x_{j-1}, y_j, x_{j+1}, ..., x_m)) = 0$. Umbenennen von $y_i := x_i$, falls $i \neq j$ liefert dann gesuchtes $y = (y_1, ..., y_m)$. □

Satz 1.3. ***(Taylorformel)*** *Sei R ein Integritaetsbereich. $f \in R[X]$ ein Polynom mit $f^{(n)}$ der n-ten formalen Ableitung, $a \in R$, dann gilt:*

$$f(x) = \sum_{k=0}^{\deg f} \frac{f^{(k)}(a)}{k!}(x-a)^k \tag{1.11}$$

Beweis. Ohne Einschraekung koennen wir $f(x) = x^n$ annehmen, da obige Formel R-Linearitaet erhaelt. So gilt dann mit dem Binomischen Lehrsatz:

$$x^n = (a + x - a)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}(x-a)^k \tag{1.12}$$

woraus die Behauptung folgt. □

2 Die multiplikative Gruppe von $\mathbb{Q}_p$

2.1 Struktur der Einheitengruppe

Schreiben wir nun $\mathbb{U} := \mathbb{Z}_p^\times$ und fuer alle $n \in \mathbb{N} : \mathbb{U}_n := 1 + p^n\mathbb{Z}_p = \ker \epsilon_n$ wobei ϵ_n die kanonische Projektion $\mathbb{U} \to (\mathbb{Z}/p^n\mathbb{Z})$ ist. Da nun $\mathbb{U}\,/\,\mathbb{U}_1 \cong \mathbb{F}_p^\times$ ist $\mathbb{U}\,/\,\mathbb{U}_1$ zyklisch von Ordnung $p-1$.
Man sieht $\mathbb{U} = \varprojlim \mathbb{U}\,/\,\mathbb{U}_n$ und fuer $n \geq 1$ ist

$$\mathbb{U}_n\,/\,\mathbb{U}_{n+1} \to \mathbb{Z}/p\mathbb{Z} \text{ mit } (1+p^n x) \mapsto (x \bmod p) \tag{2.1}$$

ein Isomorphismus, vermoege

$$(1+p^n x)(1+p^n y) \equiv 1 + p^n(x+y) \pmod{p^{n+1}}$$

Man sieht per Induktion nach n, dass $|\,\mathbb{U}_1\,/\,\mathbb{U}_n\,| = p^{n-1}$.

Lemma 2.1. *Betrachten wir eine exakte Sequenz von abelschen Gruppen:*

$$0 \to A \to E \to B \to 0 \tag{2.2}$$

Seien ferner A und B endlich mit Ordnungen a und b, welche zueinander teilerfremd seien.
Dann ist fuer $B' := \{x \in E | bx = 0\}$ gerade $E = A \oplus B'$, zudem ist B' die einzige Untergruppe von E, welche isomorph zu B ist.

Beweis. Da $ggT(a,b) = 1$ und $\mathbb{Z}$ ein Hauptidealring ist, finden wir $r, s \in \mathbb{Z}$, so dass $ar + bs = 1$. Ist nun $x \in A \cap B'$, dann ist $ax = bx = 0$, jedoch ist $(as+br)x = x$. Also $x = 0$, und damit $A \cap B' = 0$. Vielmehr koennen wir alle $x \in E$ schreiben als $x = 1x = arx + bsx$. Da nun $bE \subseteq A$, ist $bsx \in A$.
Andererseits $abE = 0$ und damit $arx \in B'$. So koennen wir $E = A \oplus B'$ einsehen.
Da obige Sequenz exakt ist, ist die Projektion $E \to B$ surjektiv. Und so dann:

$$B' \cong (A \oplus B')/A \cong B \tag{2.3}$$

Nehmen wir nun an es existiert eine Untergruppe $B'' \subseteq E$ mit $B'' \cong B$. Da $b = |B|$ muss gelten $B'' \subseteq B'$. Da ferner B endliche Ordnung hat, folgt Gleichheit. □

Satz 2.2. *Mit der Notation wie oberhalb gilt: $\mathbb{U} = V \times \mathbb{U}_1$ mit $V = \{x \in \mathbb{U} \,|\, x^{p-1} = 1\}$, welche die einzige Untergruppe von $\mathbb{U}$ isomorph zu $\mathbb{F}_p^\times$ ist.*

Beweis. Wir wenden Lemma 2.1 auf die nachfolgende Sequenz an:

$$1 \to \mathbb{U}_1 / \mathbb{U}_n \to \mathbb{U} / \mathbb{U}_n \to \mathbb{F}_p^\times \to 1 \tag{2.4}$$

Dies ist moeglich, denn wir haben gesehen, dass $|\,\mathbb{U}_1 / \mathbb{U}_n\,| = p^{n-1}$ und $|\mathbb{F}_p^\times| = p-1$.
Wir erhalten, dass $\mathbb{U} / \mathbb{U}_n$ eine eindeutige Untergruppe V_n mit $V_n \cong \mathbb{F}_p^\times$ enthaelt. Die kanonische Projektion

$$\mathbb{U} / \mathbb{U}_n \to \mathbb{U} / \mathbb{U}_{n-1} \tag{2.5}$$

bildet V_n isomorph auf V_{n-1} ab.
Da nun $\mathbb{U} = \varprojlim \mathbb{U} / \mathbb{U}_n$ erhalten wir eine Untergruppe V von $\mathbb{U}$ mit $V \cong \mathbb{F}_p^\times$. □

Korollar 2.3. *Der Koerper $\mathbb{Q}_p$ enthaelt die $p-1$-ten Einheitswurzeln.*

2.2 Struktur der Gruppe $\mathbb{U}_1$

Lemma 2.4. *Sei $x \in \mathbb{U}_n \setminus \mathbb{U}_{n+1}$, wobei $n \geq 1$. Ist nun $p \neq 2$ oder falls $p = 2, n \geq 2$ erhalten wir $x^p \in \mathbb{U}_{n+1} \setminus \mathbb{U}_{n+2}$.*

Beweis. Nach Voraussetzung ist $x = 1 + kp^n$ mit $k \not\equiv 0 \pmod p$. Mit dem binomischen Lehrsatz ist dann gerade

$$x^p = \sum_{i=0}^{p} \binom{p}{i} (kp^n)^{p-i} = 1 + kp^{n+1} + \cdots + k^p p^{np} \tag{2.6}$$

Die mittleren Exponenten sind dabei alle $\geq 2n+1 \geq n+2$. Aus den Voraussetzungen folgt weiter $np \geq n+2$. Also

$$x^p \equiv 1 + kp^{n+1} \pmod{p^{n+2}}, \tag{2.7}$$

daher ist $x^p \in \mathbb{U}_{n+1} \setminus \mathbb{U}_{n+2}$. □

Satz 2.5. *Ist $p \neq 2$ gilt $\mathbb{U}_1 \cong \mathbb{Z}_p$.*
Ist $p = 2$, dann ist $\mathbb{U}_1 \cong \{\pm 1\} \times \mathbb{U}_2$ und $\mathbb{U}_2 \cong \mathbb{Z}_p$.

Beweis. Wir behandeln zunaechst den Fall $p \neq 2$. Wir waehlen $\alpha \in \mathbb{U}_1 \setminus \mathbb{U}_2$ (z. Bsp. $\alpha = 1 + p$). Wiederholtes anwenden von Lemma 2.4 liefert $\alpha^{p^i} \in \mathbb{U}_{i+1} \setminus \mathbb{U}_{i+2}$.
Sei nun α_n die kanonische Projektion von α in $\mathbb{U}_1 / \mathbb{U}_n$. Dann ist $\alpha_n^{p^{n-2}} \neq 1$ und $\alpha_n^{p^{n-1}} = 1$.
Wir haben bereits gesehen, dass $|\,\mathbb{U}_1 / \mathbb{U}_n\,| = p^{n-1}$, daher wird $\mathbb{U}_1 / \mathbb{U}_n$ zyklisch erzeugt von α_n.
Betrachten wir nun den Isomorphismus $\theta_{n,\alpha} : \mathbb{Z} / p^{n-1}\mathbb{Z} \xrightarrow{\sim} \mathbb{U}_1 / \mathbb{U}_n, z \mapsto \alpha_n^z$. Dann kommutiert nachfolgendes Diagramm:

$$\begin{array}{ccc} \mathbb{Z} / p^n \mathbb{Z} & \xrightarrow{\theta_{n+1,\alpha}} & \mathbb{U}_1 / \mathbb{U}_{n+1} \\ \downarrow & & \downarrow \\ \mathbb{Z} / p^{n-1} \mathbb{Z} & \xrightarrow{\theta_{n,\alpha}} & \mathbb{U}_1 / \mathbb{U}_n \end{array}$$

So sehen wir, dass $\theta_{n,\alpha}$ einen Isomorphismus $\theta_\alpha : \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z} \xrightarrow{\sim} \mathbb{U}_1 = \varprojlim \mathbb{U}_1/\mathbb{U}_n$ und die Behauptung ist klar.
Sei nun $p = 2$. Waehlen wir nun $\alpha \in \mathbb{U}_2 \setminus \mathbb{U}_3$ mit $\alpha \equiv 5 \pmod 8$. Waehle wie im ersten Fall den Isomorphismus

$$\theta_{n,\alpha} : \mathbb{Z}/2^{n-2}\mathbb{Z} \xrightarrow{\sim} \mathbb{U}_2/\mathbb{U}_n \tag{2.8}$$

und erhalte wie oberhalb einen Isomorphismus $\theta_\alpha : \mathbb{Z}_2 \xrightarrow{\sim} \mathbb{U}_2$.
Weiter erhalten wir aus dem Homomorphismus

$$can : \mathbb{U}_1 \twoheadrightarrow \mathbb{U}_1/\mathbb{U}_2 \cong \mathbb{Z}/2\mathbb{Z} \tag{2.9}$$

einen Isomorphismus $\{\pm 1\} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$. Daraus erhalten wir: $\mathbb{U}_1 \cong \{\pm 1\} \times \mathbb{U}_2$. □

Satz 2.6. *Es gilt im Fall $p \neq 2$:*

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \tag{2.10}$$

Falls $p = 2$:

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} \tag{2.11}$$

Beweis. Wir haben bereits gesehen, dass sich jede Einheit in $\mathbb{Q}_p$ eindeutig schreiben laesst als $p^n u$ mit $u \in \mathbb{U}$ und $n \in \mathbb{Z}$. Daher erhalten wir

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{U} \tag{2.12}$$

Mit Satz 2.2 erhalten wir ferner, dass

$$\mathbb{U} \cong V \times \mathbb{U}_1 \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{U}_1 \tag{2.13}$$

und mit Satz 2.5 sehen wir die andere behauptete Isomorphie von $\mathbb{U}_1$. □

2.3 Quadrate in $\mathbb{Q}_p^\times$

Satz 2.7. *Sei $p \neq 2$ und mit $n \in \mathbb{Z}, u \in \mathbb{U}$ sei $x = p^n u \in \mathbb{Q}_p^\times$.*
Dann ist x ein Quadrat genau dann, wenn $n \in 2\mathbb{Z}$ und die Projektion $\bar{u} \in \mathbb{F}_p^\times$ von u ein Quadrat ist.

Beweis. Schreiben wir mit Satz 2.2 $u = (v, u_1) \in V \times \mathbb{U}_1$. Da nach Satz 2.6

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times V \times \mathbb{U}_1, \tag{2.14}$$

erhalten wir, dass z genau dann ein Quadrat ist, wenn n gerade ist und v und u_1 Quadrate sind. Nun ist ja aber $\mathbb{U}_1 \cong \mathbb{Z}_p$ und 2 ist in invertierbar in $\mathbb{Z}_p$ sind bereits alle Elemente in $\mathbb{U}_1$ Quadrate. Da ferner $V \cong \mathbb{F}_p^\times$ folgt die Behauptung. □

Korollar 2.8. *Ist $p \neq 2$, dann ist die Gruppe $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ ist vom Typ $(2,2)$ und hat die Repraesentanten $\{1, p, u, up\}$ mit $u \in \mathbb{U}$ mit $\left(\frac{u}{p}\right) = -1$.*

Satz 2.9. *Ein $x = 2^n u \in \mathbb{Q}_2^\times$ ist genau dann ein Quadrat, wenn $n \in 2\,\mathbb{Z}$ und $u \equiv 1 \pmod 8$.*

Beweis. Wir haben gesehen, dass im Fall $p = 2$ gerade $\mathbb{U} \cong \{\pm 1\} \times \mathbb{U}_2$ gilt. Somit ist u ein Quadrat genau dann, wenn $u \in \mathbb{U}_2$ und ein Quadrat in $\mathbb{U}_2$ ist.
Betrachten wir nun den Isomorphismus aus Satz (2.5) $\theta : \mathbb{Z}_2 \xrightarrow{\sim} \mathbb{U}_2$, der $2^n\,\mathbb{Z}_2$ auf $\mathbb{U}_{n+2}$ abbildet. Mit $n = 1$ sehen wir, dass die Quadrate von $\mathbb{U}_2$ gerade in $\mathbb{U}_3$ liegen. Wegen $2^3 = 8$ folgt dann die Behauptung. □

Korollar 2.10. *Die Gruppe $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ ist vom Typ $(2, 2, 2)$ mit den Raepresentanten $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.*

3 Quellen

1. J.-P. Serre: A Course in Arithmetic, Springer 1973.
2. Felix Fontein: The Hasse Derivate, 12.08.2009, abgerufen am 05.03.2018.