2 p-adische Zahlen

2.1 Der Ring $\mathbb{Z}_p$ und sein Quotientenkörper $\mathbb{Q}_p$

Sei $p \in \mathbb{N}$ eine im Folgenden fest gewählte Primzahl.

Genauso wie eine natürliche Zahl $m \in \mathbb{N}$ bezüglich der Basis 10 dargestellt werden kann, ist das auch bezüglich der Basis p möglich. Jede natürliche Zahl besitzt also eine p-adische Entwicklung der Form

$$m = a_0 + a_1 p + \ldots + a_n p^n$$

wobei die Koeffizienten a_i in $\{0, 1, \ldots, p-1\}$ liegen. Die Darstellung ist damit eindeutig.

Beispiel 2.1. Diese Darstellung finden wir durch sukzessives Dividieren mit Rest. Für $n = 216$ erhalten wir für $p = 5$

$$216 = 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3.$$

Um nun auch negative und sogar gebrochene Zahlen darstellen zu können, gehen wir zu unendlichen Reihen über, wir betrachten also Objekte der Form

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \ldots$$

mit $0 \leq a_i < p$ für $i \in \mathbb{N}_0$.

Bemerkung 2.2. $\sum_{i=0}^{\infty} a_i p^i$ ist rein formal gemeint, d.h. bezeichnet einfach die Folge der Partialsummen

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

Um nun die ganzen p-adischen Zahlen zu definieren, betrachten wir die Folgen der Restklassen

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

Zwischen den Ringen $\mathbb{Z}/p^n\mathbb{Z}$ existieren kanonische Projektionen

$$\begin{aligned} \phi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} &\to \mathbb{Z}/p^n\mathbb{Z} \\ \overline{a} &\mapsto a \bmod p^n, \end{aligned}$$

d.h. es entsteht eine Folge

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\phi_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\phi_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\phi_3} \ldots.$$

Ein solches System wird projektives System genannt, genauer:

Definition 2.3. Ein projektives System ist eine Folge von Mengen $(D_n)_{n\in\mathbb{N}}$ und eine Folge von Abbildungen $(p_n)_{n\in\mathbb{N}}$ mit $p_n \colon D_{n+1} \to D_n$

$$D_1 \xleftarrow{p_1} D_2 \leftarrow \ldots \leftarrow D_n \xleftarrow{p_n} D_{n+1} \leftarrow \ldots.$$

Die Teilmenge

$$D = \varprojlim (D_n, p_n) = \left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} D_n \mid p_n(a_{n+1}) = a_n \forall n \in \mathbb{N} \right\}$$

heißt projektiver Limes des Systems.

Bemerkung 2.4. Falls die D_n Ringe und die p_n Ringhomomorphismen sind, wird $\varprojlim (D_n, p_n)$ zum Teilring des Produktrings $\prod_{n=1}^{\infty} D_n$ (leicht nachzurechnen).

Definition 2.5 (Ganze p-adische Zahlen)**.** Der projektive Limes des Systems $(\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$

$$\mathbb{Z}_p \coloneqq \varprojlim (\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$$

heißt der Ring der ganzen p-adischen Zahlen.

Notation: Setze im Folgenden $A_n \coloneqq \mathbb{Z}/p^n\mathbb{Z}$. Außerdem bezeichne $\pi_n \colon \mathbb{Z}_p \to A_n$ die kanonische Projektion.

Bemerkung 2.6.

1. Per Definition ist $x \in \mathbb{Z}_p$ also ein Element $x \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ mit der „Kompatibilitätsbedingung":
$$x_{n+1} \equiv x_n \pmod{p^n}.$$
2. Die Inklusion
$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p, a \mapsto (a \bmod p, a \bmod p^2, \ldots)$$
ist ein injektiver Ringhomomorphismus. Damit wird $\mathbb{Z}$ zum Teilring von $\mathbb{Z}_p$.
3. $\mathbb{Z}_p$ erbt als Teilring nun also die komponentenweise Addition und Multiplikation des Produktrings $\prod_{n=1}^{\infty} A_n$, d.h. für $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$ gilt
$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}} \quad (a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (a_n \cdot b_n)_{n\in\mathbb{N}}.$$

Lemma 2.7. Es ist π_n surjektiv und $\ker \pi_n = p^n\mathbb{Z}_p \ \forall n \in \mathbb{N}$. Insbesondere gilt

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z} = A_n.$$

Beweis. Die Surjektivität ist klar. Z.z.: $\ker \pi_n = p^n\mathbb{Z}_p$. Sei dazu $x \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$. Also $\pi_n(p^n x) = 0$. Damit $p^n\mathbb{Z}_p \subseteq \ker \pi_n$.

Sei nun $x = (x_m)_{m\in\mathbb{N}} \in \ker \pi_n$ und $m \geq n$. Wegen Kompatibilität folgt

$$x_m \equiv x_n \pmod{p^n} \equiv 0 \pmod{p^n}.$$

Also folgt $x_m \in p^n A_m$.

Es ist (nachrechnen)

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \cong p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m.$$

Das heißt es ex. ein eindeutiges $y_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Es bleibt zu zeigen, dass $p^n y = x$.

Z.z.: $x = p^n y$. Für $m \leq n$ ist $x_m = 0 = p^n y_m$. Für $m > n$ ist wegen Kompatibilität

$$p^n y_m = p^n y_{m+n-n} \equiv x_{m+n} \pmod{p^{m+1}} \equiv x_m \pmod{p^m}.$$

Also $x = p^n y$. Insgesamt folgt also $\ker \pi_n = p^n\mathbb{Z}_p$. Die behauptete Isomorphie folgt jetzt direkt aus dem Homomorphiesatz. □

Lemma 2.8. Für $u \in \mathbb{Z}_p$ sind äquivalent

(i) $u \in \mathbb{Z}_p^\times$

(ii) $p \nmid u$

(iii) $0 \neq u_1 \in \mathbb{Z}/p\mathbb{Z}$

Beweis. (ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (ii). Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann $\exists v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u_1 v_1} \equiv 1 \pmod p$ also insbesondere $p \nmid u_1 \implies \overline{u_1} \neq 0$.

Sei umgekehrt $\overline{u_1} \neq 0$. Wegen Kompatibilität folgt damit $p \nmid u_n \ \forall n \in \mathbb{N}$, denn ang. $p \mid u_n$ für ein $n \in \mathbb{N}$. Dann folgt

$$0 \equiv u_n \pmod p \equiv u_1 \pmod p \quad \lightning.$$

Da p prim folgt insbesondere $(p^n, u_n) = 1$. Also ex. nach euklid. Alg. $a, b \in \mathbb{Z}$, s.d. $1 = ap^n + bu_n$, also $1 = \overline{bu_n}$ mit $\overline{b} \in A_n$. Also $\overline{u_n} \in A_n^\times$ und damit $v \coloneqq (\dots \overline{u_n}^{-1}, \overline{u_{n-1}}^{-1}, \dots, \overline{u_1}^{-1}) = u^{-1} \in \mathbb{Z}_p$. □

Lemma 2.9. Für $x \in \mathbb{Z}_p \setminus \{0\}$ ex. $n \in \mathbb{N}_0$ und $u \in \mathbb{Z}_p^\times$, s.d.

$$x = p^n u.$$

Diese Darstellung ist eindeutig.

Beweis. (i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein $n \in \mathbb{N}_0$ maximal, s.d. $x_n = \pi_n(x) = 0$. Also ist $x \in \ker \pi_n$, insbesondere ex. nach 2.7 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$. Ang.: $p \mid u$, dann ist $\pi_1(u) = 0$ also ex. wieder nach 2.7 ein $v \in \mathbb{Z}_p$ mit $u = pv$. Dann ist aber

$$\pi_{n+1}(x) = \pi_{n+1}(p^n u) = \pi_{n+1}(p^{n+1} v) = 0.$$

Widerspruch zur Maximalität von n.

(ii) Eindeutigkeit: Sei $x = p^n u = p^m v$ mit $u, v \in \mathbb{Z}_p^\times$ und $n, m \in \mathbb{N}_0$. Sei o.E. $n \geq m$. Es ist $\pi_n(x) = \pi_n(p^n)\pi_n(u) = 0$ also auch $0 = \pi_n(x) = \pi_n(p^m)\pi_n(v)$. Da $v \in \mathbb{Z}_p^\times$ ist $\pi_n(v) \in A_n^\times$, also kein Nullteiler. Also folgt $\pi_n(p^m) = 0$ und damit $p^m \equiv 0 \pmod{p^n}$, also $m \geq n$. Insgesamt also $m = n$.

Nun gilt weiter $x = p^n u = p^n v$, also $p^n(u - v) = 0$. Ang. $u - v \neq 0$. Dann ist nach (i) $u - v = p^k w$ mit $k \in \mathbb{N}_0$ und $w \in \mathbb{Z}_p^\times$. Also $0 = p^n(u - v) = p^{n+k} w$. Da $w \in \mathbb{Z}_p^\times$ also kein Nullteiler, folgt $0 = p^{n+k} \in \mathbb{Z}$ $\lightning$.

□

Definition 2.10 (p-Bewertung)**.** Für $x \in \mathbb{Z}_p \setminus \{0\}$ sei $x = p^n u$ mit $u \in \mathbb{Z}_p^\times$. Dann setze

$$v_p(x) \coloneqq n$$

und setze $v_p(0) \coloneqq \infty$. $v_p(x)$ heißt die p-Bewertung von x.

Bemerkung 2.11. Wegen 2.9 ist die p-Bewertung wohldefiniert. Per Konvention setze $n + \infty = \infty$ und $\infty > n$ für $n \in \mathbb{N}_0$. Es ist leicht nachzurechnen, dass für $x, y \in \mathbb{Z}_p$ gilt

$$v_p(xy) = v_p(x) + v_p(y), \quad v_p(x + y) \geq \min(v_p(x), v_p(y)).$$

Korollar 2.12. $\mathbb{Z}_p$ ist nullteilerfrei.

Beweis. Seien $x, y \in \mathbb{Z}_p$ mit $xy = 0$. Dann folgt

$$\infty = v_p(0) = v_p(xy) = v_p(x) + v_p(y).$$

Also $v_p(x) = \infty$ oder $v_p(y) = \infty$, also $x = 0$ oder $y = 0$. □

Definition 2.13. Der Quotientenkörper der ganzen p-adischen Zahlen $\mathbb{Z}_p$ heißt Körper der p-adischen Zahlen

$$\mathbb{Q}_p \coloneqq Q(\mathbb{Z}_p).$$

Bemerkung 2.14. 1. Ein Element $x = \frac{a}{b} \in \mathbb{Q}_p^\times$ mit $a, b \in \mathbb{Z}_p$, $b \neq 0$ kann eindeutig als $x = p^r w$ mit $r \in \mathbb{Z}$ und $w \in \mathbb{Z}_p^\times$ dargestellt werden, denn nach 2.9 ist

$$x = \frac{a}{b} = \frac{p^n u}{p^m v} = p^{n-m} \underbrace{uv^{-1}}_{\in \mathbb{Z}_p^\times}.$$

Damit setzt sich die Definition von v_p auf $\mathbb{Q}_p$ fort. Es gilt $v_p(x) \geq 0 \iff x \in \mathbb{Z}_p$.

2. Nach (1) ist also $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.

Bemerkung 2.15. 1. $\mathbb{Q}_p$ kann auch als Vervollständigung von $\mathbb{Q}$ bezüglich der p-adischen Metrik $d(\cdot, \cdot)$ definiert werden (analog zu $\mathbb{R}$ als Vervollständigung von $\mathbb{Q}$ bezüglich $|\cdot|$).

2. Es ist leicht nachzurechnen, dass $d(\cdot, \cdot)$ die ultrametrische Ungleichung (auch starke Dreiecksungleichung) erfüllt, d.h.

$$d(x, z) \leq \max(d(x, y), d(y, z))$$

für $x, y, z \in \mathbb{Q}_p$. Damit folgt das eine Folge $(a_n)_{n \in \mathbb{N}} \subseteq \mathbb{Q}_p$ genau dann konvergiert, wenn $\lim_{n \to \infty}(u_{n+1} - u_n) = 0$ (was in $\mathbb{R}$ bezüglich $|\cdot|$ falsch ist).

2.2 p-adische Gleichungen

Lemma 2.16. Sei $D_1 \leftarrow D_2 \leftarrow \ldots$ ein projektives System und $D = \varprojlim (D_n, p_n)$ sein inverser Limes. Falls $D_n \neq \emptyset$ und endlich folgt $D \neq \emptyset$.

Beweis. Sei zunächst $p_n \colon D_{n+1} \to D_n$ surjektiv. Dann ex. für alle $x_n \in D_n$ ein $x_{n+1} \in D_{n+1}$, s.d. $p_n(x_{n+1}) = x_n$. Da $D_1 \neq \emptyset$ folgt $D \neq \emptyset$ induktiv.

Im Allgemeinen bezeichne für $m, n \in \mathbb{N}$:

$$D_{n,m} \coloneqq (p_n \circ \ldots \circ p_{n+m-1})(D_{n+m}).$$

Da $D_{n+m} \neq \emptyset$ folgt $D_{n,m} \neq \emptyset$ und da D_k endlich folgt $\#p_k(D_{k+1}) \leq \#D_{k+1}$ $\forall k \in \mathbb{N}$. D.h. $\#D_{n,m}$ ist monoton fallend in m bei festem n. Da $D_{n,m} \neq \emptyset$ wird die Folge stationär, d.h. es ex. ein $m_0 \in \mathbb{N}$, s.d. $D_{n,m_0} = D_{n,m}$ $\forall m \geq m_0$. Sei E_n dieser Grenzwert.

Es ist leicht nachzurechnen, dass $p_n(E_{n+1}) = E_n$. Also sind die Einschränkungen $p_n|_{E_{n+1}} \colon E_{n+1} \to E_n$ surjektiv, $E_n \neq \emptyset$ und endlich, also folgt nach der Vorüberlegung $\varprojlim (E_n, p_n|_{E_n}) \neq \emptyset$, also insbesondere $D \neq \emptyset$. □

Satz 2.17. Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ Polynome in den ganzen p-adischen Zahlen. Dann sind äquivalent:

(i) Die $f^{(i)}$ haben eine gemeinsame Nullstelle in $(\mathbb{Z}_p)^m$.

(ii) Für $n \in \mathbb{N}$ haben die Polynome $f^{(i)} \pmod{p^n}$ eine gemeinsame Nullstelle in $(A_n)^m$.

Beweis. Sei $D = \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\} \subseteq (\mathbb{Z}_p)^m$ und
$D_n \coloneqq \{ \text{ gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m \colon (A_{n+1})^m \to (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet. Dann ist $(D_n, (\phi_n)^m)$ ein projektives System mit $D = \varprojlim (D_n, (\phi_n)^m)$.

Sei nun $D \neq \emptyset$ und $x \in D$. Dann ist $\pi_n(x) \in D_n$ $\forall n \in \mathbb{N}$. Seien umgekehrt $D_n \neq \emptyset$ $\forall n \in \mathbb{N}$. Da $D_n \subseteq A_n$ endlich folgt mit 2.16 $D \neq \emptyset$. □

Definition 2.18. Ein Element $x = (x_1, \ldots, x_m) \in (\mathbb{Z}_p)^m$ (bzw. $(A_n)^m$) heißt primitiv, falls ein $x_i \in \mathbb{Z}_p^\times$ (bzw. $\in A_n^\times$) ist.

Wir möchten nun betrachten, unter welchen Umständen eine Lösung $\pmod{p^n}$ zu einer echten Lösung in $\mathbb{Z}_p$ entwickelt werden kann. Dazu verwenden wir die p-adische Version des Newton Verfahrens.

Lemma 2.19 (Henselsches Lemma)**.** Sei $f = a_m X^m + \ldots + a_0 \in \mathbb{Z}_p[X]$ und $f' = a_m m X^{m-1} + \ldots + a_1 \in \mathbb{Z}_p[X]$ seine Ableitung. Weiter sei $x \in \mathbb{Z}_p$, s.d. $f(x) \equiv 0 \pmod{p^n}$ für ein $n \in \mathbb{N}$ und $v_p(f'(x)) = k$ mit $0 \leq 2k < n$. Dann existiert ein $y \in \mathbb{Z}_p$, s.d.

$$f(y) \equiv 0 \pmod{p^{n+1}}, v_p(f'(y)) = k \text{ und } y \equiv x \pmod{p^{n-k}}.$$

Beweis. Nach Voraussetzung ist $f(x) = p^n b$ und $f'(x) = p^k c$ mit $b \in \mathbb{Z}_p$ und $c \in \mathbb{Z}_p^\times$. Dann setze $z := -bc^{-1}$ und $y := x + p^{n-k}z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

$$a_i y^i = a_i \sum_{j=0}^{i} \binom{i}{j} x^{i-j}(p^{n-k}z)^j = a_i x^i + a_i i x^{i-1} p^{n-k} z + p^{2n-2k} z^2 R_i$$

für $R_i \in \mathbb{Z}_p$. Aufsummieren und addieren von a_0 liefert mit $R \in \mathbb{Z}_p$ eine „Taylorentwicklung":

$$f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-2k} z^2 R$$

Einsetzen liefert

$$\begin{aligned} f(y) &= p^n b - p^{n-k} b c^{-1} p^k c + p^{2n-2k} z^2 R \\ &= p^{2n-2k} z^2 R \\ &\equiv 0 \pmod{p^{n+1}}, \end{aligned}$$

da $2k < n \implies 2n - 2k \geq n + 1$. Anwenden der „Taylorentwicklung" auf f' liefert

$$\begin{aligned} f'(y) &= f'(x) + p^{n-k} z f''(x) + p^{2n-2k} z^2 R \\ &= p^k c + p^{n-k} z f''(x) + p^{2n-2k} z^2 R \\ &= p^k (\underbrace{c + p^{n-2k} z f''(x) + p^{2n-3k} z^2 R}_{=:s}). \end{aligned}$$

Es ist $n - 2k > 0$ und $2n - 3k > 0$, aber $c \in \mathbb{Z}_p^\times$, also $p \nmid s$ und damit $s \in \mathbb{Z}_p^\times$ und $v_p(f'(y)) = k$. □

Zum Studium der quadratischen Formen benötigen wir noch die auf m Variablen verallgemeinerte Version des Henselschen Lemmas.

Satz 2.20. Sei $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ und $x = (x_i) \in (\mathbb{Z}_p)^m$, s.d. $f(x) \equiv 0 \pmod{p^n}$. Weiter existiere ein $1 \leq j \leq m$, s.d. $v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k$ mit $0 \leq 2k < n$. Dann existiert eine Nullstelle $y \in (\mathbb{Z}_p)^m$ von f mit $y \equiv x \pmod{p^{n-k}}$.

Beweis. Sei zunächst $m = 1$. Mit 2.19 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

$$f(x^{(1)}) \equiv 0 \pmod{p^{n+1}},\ v_p(f'(x^{(1)})) = k \text{ und } x^{(1)} \equiv x^{(0)} \pmod{p^{n-k}}.$$

Wende 2.19 nun auf $x^{(1)}$ und $n+1$ an. Induktiv erhält man eine Folge $(x^{(q)})_{q \in \mathbb{N}}$ mit den Eigenschaften

$$x^{(q+1)} \equiv x^{(q)} \pmod{p^{n+q-k}} \text{ und } f(x^{(q)}) \equiv 0 \pmod{p^{n+q}}.$$

Es gilt nun $v_p(x^{(q+1)} - x^{(q)}) \geq n + q - k$, also $d(x^{(q+1)}, x^{(q)}) \xrightarrow{q \to \infty} 0$. Also ist $x^{(q)}$ eine Cauchy Folge und konvergiert gegen ein $y \in \mathbb{Z}_p$. Dann gilt

$$0 = \lim_{q \to \infty} f(x^{(q)}) = f(\lim_{q \to \infty} x^{(q)}) = f(y)$$

und $y \equiv x \pmod{p^{n-k}}$.

Sei nun $m > 1$. Ersetze in f die Variablen X_i durch x_i für $i \neq j$. Dann sei $g \in \mathbb{Z}_p[X_j]$ das entstandene Polynom in einer Variablen. Wende nun den Fall für $m = 1$ auf g an. Dann erhalten wir ein $y_j \in \mathbb{Z}_p$ mit $y_j \equiv x_j \pmod{p^{n-k}}$ und $g(y_j) = 0$. Setze nun $y_i := x_i$ für $i \neq j$. Dann ist $y \equiv x \pmod{p^{n-k}}$ und

$$f(y) = f(y_1, \ldots, y_m) = f(x_1, \ldots, x_{j-1}, y_j, x_{j+1}, \ldots, x_m) = g(y_j) = 0.$$

□

Aus dem letzten Satz können wir einfache Schlussfolgerungen für quadratische Formen ziehen.

Korollar 2.21. Sei $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ und $x \in \mathbb{Z}_p$ mit

$$f(x) \equiv 0 \pmod{p}$$

und es sei mind. eine partielle Ableitung $\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \pmod{p}$, dann hebt sich x zu einer echten Nullstelle.

Beweis. Das ist der Fall $n = 1$ und $k = 0$ in 2.20. □

Korollar 2.22. Sei $p \neq 2$ und $f = \sum_{i=1}^{m} \sum_{j=1}^{m} a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \ldots, X_m]$ eine quadratische Form mit $a_{ij} = a_{ji}$ und sei $p \nmid \det(a_{ij})$. Sei weiter $a \in \mathbb{Z}_p$. Dann hebt sich jede primitive Lösung der Gleichung $f(x) \equiv a \pmod{p}$ zu einer echten Lösung.

Beweis. Mit 2.21 g.z.z., dass mind. eine partielle Ableitung $\pmod{p}$ nicht verschwindet. Sei $A = (a_{ij}) \in \mathbb{Z}_p^{m \times m}$. Da $\det(a_{ij}) \not\equiv 0 \pmod{p}$ folgt $\det(a_{ij}) \in \mathbb{F}_p^\times$ und damit $\ker A = \{0\}$. Es gilt weiter

$$\frac{\partial f}{\partial X_i} = 2 \sum_{j=1}^{m} a_{ij} X_j \text{ also } \begin{pmatrix} \partial_{X_i} f(x) \\ \vdots \\ \partial_{X_m} f(x) \end{pmatrix} = 2Ax.$$

Da x primitiv ist $x \neq 0 \in \mathbb{F}_p^m$ und damit mind. eine partielle Ableitung $\not\equiv 0 \pmod{p}$. □