Die p-adischen Zahlen

Felix Baaden, Andreas Schmidt

10. Mai 2007

1 Einführung in die p-adischen Zahlen (Felix Baaden)

Sei p von nun an immer eine Primzahl

Motivation:

Wir können die natürliche Zahl $n = 137$ auch mit Hilfe einer Primzahl $p = 3$ schreiben.

$$\begin{aligned} 137 &= 2 * 3^0 + 0 * 3^1 + 0 * 3^2 + 2 * 3^3 + 1 * 3^4 \\ &= \sum_{i=1}^{\infty} a_i 3^i \end{aligned}$$

wobei $a_0 = 2$, $a_1 = 0$, $a_2 = 0$, $a_3 = 2$, $a_4 = 1$, $a_n = 0$ $(\forall n \geq 5)$.

Die Konstruktion der Zahl 137 geschah hier über eine Potenzreihe. Die Darstellung der Zahl 137 heißt p-adische Entwicklung von 137. Neben dieser analytischen Betrachtung kann man die p-adischen Zahlen auch algebraisch über den projektiven Limes erzeugen. Dies soll im Folgenden geschehen. Dazu brauchen wir aber zuerst folgenden Satz:

Satz 1:

Die Restklassen $a(modp^n)$ werden in eindeutiger Darstellung durch

$$a \equiv a_0 + ap + a_2 p^2 + \ldots + a_{n-1} p^{n-1} (modp^n) \tag{1}$$

gegeben wobei $0 \leq a_i < p \quad$ für $i = 0, \ldots, n-1$

Beweis (mit vollstandiger Induktion):

Sei $n = 1$. Dann gilt $a \equiv a_0(modp)$. Die Darstellung ist eindeutig.
Nehmen wir die Behauptung für $n-1$ bewiesen an, so haben wir eine eindeutige Darstellung

$$a \equiv a_0 + ap + a_2 p^2 + \ldots + a_{n-2} p^{n-2} + g p^{n-1}$$

mit einer ganzen Zahl g. Ist $g \equiv a_{n-1}(modp)$ mit $0 \leq a_{n-1} < p$, so ist a_{n-1} durch a eindeutig bestimmt und es gilt die Kongruenz des Satzes. $\square$

Vorüberlegungen:

Unser Ziel ist es, mit Hilfe der algebraischen Zahlentheorie den Ring der ganzen p-adischen Zahlen $\mathbf{Z}_p$ zu definieren. Dazu brauchen wir einige Vorüberlegungen:
Wir betrachten die Kongruenzen aus Satz 1 nun für ein $k < n$. Wir erhalten daher den Ausdruck $a \equiv a_0 + ap + a_2p^2 + \ldots + a_{k-1}p^{k-1}(modp^k)$. Der Summand $a_kp^k + \ldots a_{n-1}p^{n-1}$ entfällt dabei. Wir können nun jeder Restklasse $modp^n$ eindeutig eine Restklasse $modp^k$ zuordnen. Jedes Element aus $\mathbf{Z}/p^n\mathbf{Z}$ bestimmt also ein Element aus $\mathbf{Z}/p^k\mathbf{Z}$. Wir betrachten jetzt die p-adischen Zahlen nicht mehr wie oben motiviert als Potenzreihen, sondern sehen sie jetzt als Folgen der Restklassen

$$\overline{x_n} = x_n(modp^n) \in \mathbf{Z}/p^n\mathbf{Z} \tag{2}$$

Sei $\mathbf{A_n} := \mathbf{Z}/p^n\mathbf{Z}$, wobei $n \in \mathbf{N}$. Dann existiert eine Abbildung Φ, für die gilt
$\Phi_k^n : \mathbf{A_n} \to \mathbf{A_k} \quad (k < n)$. Wir erhalten einen Homomorphismus (die Abbildung ist strukturerhaltend; sie bildet Addition in Addition und Multiplikation in Multiplikation ab). Es gilt

(i) $\forall n \geq 1$ ist Φ_n^n die identische Abbildung

(ii) Für $k \leq m \leq n$ ist $\Phi_k^n = \Phi_k^m \circ \Phi\_m^n$

Also bestimmt $\mathbf{A_n}$ in eindeutiger Weise ein Element von $\mathbf{A_{n-1}}$, also $\Phi_n : \mathbf{A_n} \to \mathbf{A_{n-1}}$.
Der Homomorphismus ist surjektiv. Sein Kern ist $p^{n-1}A_n$ (denn wenn man z.B. $p = 5$ und $n = 2$ setzt, so erhält man $\mathbf{A_2} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \ldots, \overline{24}\}$ bzw. $\mathbf{A_1} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, also werden $\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}$ auf die Null abgebildet. Der Kern von $\Phi_2 : \mathbf{A_2} \to \mathbf{A_1}$ ist also $5A_2$; dadurch werden Kern und Surjektivität sofort klar).
Somit erhalten wir eine unendliche Folge von Restklassenringen und Homomorphismen

$$\ldots \to \mathbf{A_n} \xrightarrow{\Phi_n} \mathbf{A_{n-1}} \xrightarrow{\Phi_{n-1}} \ldots \xrightarrow{\Phi_3} \mathbf{A_2} \xrightarrow{\Phi_2} \mathbf{A_1}$$

Man spricht hier von einem sogenannten projektiven System. Die in (2) definierte Folgen von Restklassen

$$\overline{x_n} = x_n(modp^n) \in \mathbf{Z}/p^n\mathbf{Z}$$

liegen in verschiedenen Ringen $\mathbf{Z}/p^n\mathbf{Z}$, sie sind aber, wie eben gesehen, miteinander verbunden, und es gilt

$$\Phi(\overline{x_n}) = \overline{x_{n-1}}$$

Um nun endlich den Ring der ganzen p-adischen Zahlen $\mathbf{Z}_p$ definieren zu können, fehlt uns noch die Definition des projektiven Limes.
Im direkten Produkt

$$\prod_{n=1}^{\infty} \mathbf{Z}/p^n\mathbf{Z} = \{(x_n)_{n\in\mathbf{N}} | x_n \in \mathbf{Z}/p^n\mathbf{Z}\}$$

betrachten wir jetzt alle Elemente $(x_n)_{n\in\mathbf{N}}$ mit der Eigenschaft

$$\Phi_n(x_{n+1}) = x_n \quad \forall n = 1, 2, \ldots$$

Diese Menge heißt der projektive Limes der Ringe $\mathbf{Z}/p^n\mathbf{Z}$ und wird mit $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$ bezeichnet. Es gilt also

$$\varprojlim \mathbf{Z}/p^n\mathbf{Z} = \{(x_n)_{n\in\mathbf{N}} \in \prod_{n=1}^{\infty} \mathbf{Z}/p^n\mathbf{Z} \mid \Phi(x_{n+1}) = x_n, \quad n = 1, 2, \ldots\}$$

Der projektive Limes hat jetzt folgenden Vorzug

$$\varprojlim \mathbf{Z}/p^n\mathbf{Z} \subseteq \prod_{n=1}^{\infty} \mathbf{Z}/p^n\mathbf{Z}$$

Er wird also zu einem Teilring des direkten Produktes $\prod_{n=1}^{\infty} \mathbf{Z}/p^n\mathbf{Z}$. Darin sind Multiplikation und Addition komponentenweise definiert. Somit erhalten wir den Ring der ganzen p-adischen Zahlen $\mathbf{Z}_p$. Wir fassen das eben gesehene nochmals in folgender wichtigen Definition zusammen:

Definition 1

Man nennt $\mathbf{Z}_p$ den Ring der ganzen p-adischen Zahlen und definiert ihn als den projektiven Limes des Systems (A_n, Φ_n) und schreibt

$$\mathbf{Z}_p = \varprojlim (A_n, \Phi_n) \tag{3}$$

Ein Element x aus $\mathbf{Z}_p$ schreibt man in der Form $x = (\ldots, x_n, \ldots, x_1)$ mit $x_n \in A_n$ und $\Phi(x_n) = x_{n-1}$ für $n \geq 2$.

Wir finden sogar in $\mathbf{Z}_p$ die ganzen Zahlen $a \in \mathbf{Z}$ wieder; diese hatten sich nämlich durch die Kongruenzen aus (1) ergeben. Bei der Identifizierung in (3) geht daher $\mathbf{Z}$ in die Menge der Tupel

$$(\ldots, a(modp^3), a(modp^2), a(modp)) \in \prod_{n=1}^{\infty} \mathbf{Z}/p^n\mathbf{Z}$$

über und somit wird $\mathbf{Z}$ zu einem Teilring von $\mathbf{Z}_p$.
Somit gilt also

$$\mathbf{Z} \subseteq \mathbf{Z}_p = \varprojlim \mathbf{Z}/p^n\mathbf{Z} \subseteq \prod_{n=1}^{\infty} \mathbf{Z}/p^n\mathbf{Z}$$

Beispiel 1

Sei $p = 3$ Wir können die Zahl 8 mit Hilfe von Definition 1 darstellen

$$\begin{aligned} 8 &\equiv 2(mod \quad 3) \\ &\equiv 2 + 2 * 3(mod \quad 3^2) \\ &\equiv 2 + 2 * 3(mod \quad 3^3) \end{aligned}$$

Wir erhalten also $x = (\ldots, 2 + 2 * 3(mod 3^3), 2 + 2 * 3(mod 3^2), 2(mod 3))$

Eigenschaften von $\mathbf{Z}_p$

Proposition 1

Die Sequenz $0 \to \mathbf{Z}_p \xrightarrow{p^n} \mathbf{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$ ist exakt. Dabei soll $\varepsilon_n : \mathbf{Z}_p \to A_n$ eine Funktion sein, die einer ganzen p-adischen Zahl x seine n-te Komponente x_n zuordnet.

Beweis

Erinnerung: Um zu zeigen, dass diese Sequenz exakt ist, müssen wir einerseits zeigen, dass p^n injektiv und ε_n surjektiv ist. Andererseits müssen wir zeigen, dass $Kern(p^n) = Bild(\varepsilon_n)$ ist.

Sei nun $x = (x_n)$ eine ganze p-adische Zahl und $px = p + \ldots + p = 0$ (p Summanden). Für jede Komponente ist dann $px_{n+1} = 0$ für alle n und x_{n+1} ist von der Form $p^n y_{n+1}$ mit $y_{n+1} \in A_{n+1}$; da nach Definition gilt $\phi(x_{n+1}) = x_n$ sieht man, dass x_n durch p^n teilbar ist, also null ist. Die Multiplikation mit p, also auch mit p^n ist in $\mathbf{Z_p}$ daher injektiv.
Dass der Projekthomomorphismus ε_n injektiv ist, ist klar. Wir müssen also noch zeigen, dass $Kern(\varepsilon_n) = Bild(p^n)$ ist.
Ist $x = (\ldots, x_3, x_2, x_1) \in Kern(\varepsilon_n)$, dann ist $\varepsilon_n(x) = x_n = 0$, aber auch $x_{n-1} = \phi(x_n) = 0$, also $x_1 = x_2 = \ldots = x_n = 0$. Außerdem gilt $\phi_n^m(x_m) = x_n = 0$ für jedes $m \geq n$, d.h. $x_m \in Kern(\phi_n^m) = p^n A_m$, also $x_m = p^n x_m^{'}$ für alle $m \geq n + 1$. Es liegt offenbar $x^{'} = (\ldots, x_{n+2}^{'}, x_{n+1}^{'}, 0, \ldots, 0, 0)$ in $\mathbf{Z_p}$; es ist $x = p^n x^{'}$. □

Proposition 2

Ein Element aus $\mathbf{Z}_p$ ist genau dann invertierbar, wenn u nicht durch p teilbar ist.

Beweis

$\Leftarrow$
Es sei u nicht durch p teilbar. Es sei u_m die m-te Komponente von u in A_n. Nach Voraussetzung gilt $(u, p) = 1$. Also ist u_n prime Restklasse und besitzt daher ein Inverses u_n^{-1}. Dann gilt

$$u^{-1} = (\ldots, u_n^{-1}, \ldots, u_2^{-1}, u_1^{-1})$$

u ist also invertierbar.

$\Rightarrow$
Sei u invertierbar. u ist nur dann durch p teilbar, wenn $u \in Bild(p) = Kern(\varepsilon_n)$. Da u eine Einheit ist, ist auch $\varepsilon_n(u)$ eine Einheit, also $\varepsilon_n(u) \neq \overline{0}$, also ist u nicht durch p teilbar. $\square$

Proposition 3

Es sei $\mathbf{U}$ die Gruppe der invertierbaren Elemente von $\mathbf{Z}_p$. Jedes von Null verschiedene Element aus $\mathbf{Z}_p$ lässt sich eindeutig in der Form $p^n u$ ($u \in \mathbf{U}$ und $n \geq 0$) schreiben. (Man nennt ein Element aus $\mathbf{U}$ p-adische Einheit).

Beweis

Ist x eine von Null verschiedene ganze p-adische Zahl. Dann existiert eine größte ganze Zahl n, so dass $x_n = \varepsilon_n(x)$ Null ist, aber $x_{n+1} \neq \overline{0}$. Dann gilt $a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} + \ldots = p^n(a_n + a_{n+1} p + a_{n+2} p^2 + \ldots)$. Dann ist $(a_n + a_{n+1} p + a_{n+2} p^2 + \ldots)$ offensichtlich nicht durch p teilbar, liegt also nach Proposition 2 in $\mathbf{U}$. Daher erhält man die gewünschte Zerlegung $p^n u$ mit $u \in \mathbf{U}$.
Die Eindeutigkeit ist durch die Zerlegung klar. $\square$

Notation

Sei x eine ganze von null verschiedene p-adische Zahl. x lässt sich nach Proposition 3 in der Form $x = p^n u$ schreiben. Wir nennen die natürliche Zahl n p-adische Bewertung von x und setzen $\nu_p(x) = n$. Man setzt formal $\nu_p(0) = \infty$. Dann erhält man eine Funktion

$$\nu_p : \mathbf{Q} \to \mathbf{Z} \cup \{\infty\}$$

mit den folgenden Eigenschaften

(i) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$

(ii) $\nu_p(x + y) \geq min\{\nu_p(x)\, \nu_p(y)\}$

wobei $x + \infty = \infty, \quad \infty + \infty = \infty$ und $\infty > x$ gelten soll.

Beweis

(i) $\nu_p(xy) = \nu_p(p^n u p^m v) = \nu_p(p^{n+m} uv) = n + m$

(ii) Sei o.b.d.A. $n < m$. $\nu_p(p^n u + p^m v) = \nu_p(p^n(u + v p^{m-n})) \geq min\{\nu_p(p^n u), \nu_p(p^m u)\}$ $\square$

Proposition 4

Auf $\mathbf{Z}_p$ wird durch

$$d(x, y) = \exp(-\nu_p(x - y))$$

eine Metrik definiert. Dadurch wird $\mathbf{Z}_p$ zu einem metrischen Raum, in dem Konvergenzen definiert sind. (Anmerkung: Das Problem an der Motivation war, dass die Reihen nicht konvergieren. Mit Hilfe dieser Definition ist es uns aber nun auch möglich eine Konvergenz für hohe n festzustellen.

Der Körper $\mathbf{Q_p}$

In der Motivation hatten wir die ganzen p-adischen Zahlen über eine Potenzreihe dargestellt. In Analogie zu den Laurentreihen $f(z) = \sum_{\nu=-\infty}^{\infty} a_\nu (z-a)^\nu$ erweitern wird die ganzen p-adischen Zahlen durch die formalen Reihen

$$f(z) = \sum_{\nu=-m}^{\infty} a_\nu p^\nu = a_{-m}p^{-m} + \ldots + a_{-1}p^{-1} + a_0 + a_1 p + \ldots$$

wobei m eine ganze Zahl und $0 \leq a_\nu < p$ ist. Diese Reihen nennen wir nun die p-adischen Zahlen und bezeichnen ihre Gesamtheit mit $\mathbf{Q_p}$. Für eine beliebige Zahl $f \in \mathbf{Q_p}$ schreiben wir

$$f = \frac{f}{g} p^{-m} \quad g, h \in \mathbf{Z} \quad (gh, p) = 1$$

und wenn $a_0 + a_1 p + a_2 p^2 + \ldots$ die p-adische Entwicklung von $\frac{g}{h}$ ist, so ordnen wir f die p-adische Zahl $a_0 p^{-m} + a_1 p^{-m+1} + ... + a_m + a_{m+1}p + \ldots \in \mathbf{Q_p}$ als p-adische Entwicklung zu. So erhalten wir eine kanonische Abbildung $\mathbf{Q} \to \mathbf{Q_p}$, die $\mathbf{Z}$ in $\mathbf{Z_p}$ überführt und injektiv ist und identifizieren nun $\mathbf{Q}$ mit dem Bild in $\mathbf{Q_p}$, sodass $\mathbf{Q} \subseteq \mathbf{Q_p}$ und $\mathbf{Z} \subseteq \mathbf{Z_p}$ wird, un erhalten für jede rationale Zahl $f \in \mathbf{Q}$ eine Gleichheit $f = \sum_{\nu=-m}^{\infty} a_\nu p^\nu$.
Da nun jedes Element $f \in \mathbf{Q_p}$ als $f = p^{-m} g \quad g \in \mathbf{Z_p}$ dargestellt werden kann, dehnt sich sowohl Addition als auch Multiplikation in $\mathbf{Z_p}$ auf $\mathbf{Q_p}$ aus. $\mathbf{Q_p}$ wird zum Quotientenkörper von $\mathbf{Z_p}$. Folgen wir nun dem gleichen Muster wie in der Identifizierung nach Definition 3, so erhalten wir $\mathbf{Q}$ als Teilkörper $\mathbf{Q_p}$ der p-adischen Zahlen.

Definition 2

Der Körper der p-adischen Zahlen $\mathbf{Q_p}$ ist der Quotientenkörper des Rings $\mathbf{Z_p}$.

Man sieht sofort, dass $\mathbf{Q_p} = \mathbf{Z_p}[p^{-1}]$. Jedes Element $x \in (\mathbf{Q_p})^*$ kann man als $p^{n'}u'$ mit $n' \in \mathbf{Z}, u' \in \mathbf{U}$ schreiben (Überlegung: $\frac{p^n u}{p^m v} = p^{n-m}\frac{u}{v} = p^{n'}u'$). n' heißt wiederum p-adische Bewertung von x. Wir schreiben wiederum $\nu_p(x)$. Es gilt $\nu_p(x) \geq 0$ nur wenn $x \in \mathbf{Z_p}$ ist.

Proposition 5

Für $x \in \mathbf{Q_p}$ definieren wir den p-Betrag durch

$$|x|_p = (\frac{1}{e})^{v_p(x)}$$

Dieser hat folgende nützliche Eigenschaften:

(i) $|x|_p > 0$

(ii) $|xy|_p = |x|_p |y|_p$

(iii) $|x+y|_p \leq max(|x|_p, |y|_p)$ (ultrametrische Gleichung)

Beweis

(i) klar

(ii) $|xy|_p = (\frac{1}{p})^{\nu_p(xy)} = (\frac{1}{p})^{\nu_p(x)+\nu_p(y)} = (\frac{1}{p})^{\nu_p(x)}(\frac{1}{p})^{\nu_p(y)} = |x|_p|y|_p$

(iii) $|x+y|_p = (\frac{1}{p})^{\nu_p(x+y)} \leq (\frac{1}{p})^{max\{\nu_p(x),\nu_{p(y)}\}}$

Proposition 6

Der Körper $\mathbf{Q_p}$, mit der Metrik, die durch $d(x,y) = e^{-\nu_p(x-y)}$ definiert ist, ist lokal kompakt und enthält $\mathbf{Z_p}$ als offenen Unterring; der Körper $\mathbf{Q}$ ist dicht in $\mathbf{Q_p}$.

Dies ist klar.

Abschlussbemerkung

Zum Schluss soll nochmals auf die ganzen p-adischen Zahlen zurückgekommen werden. Man kann die ganzen p-adischen Zahlen auch noch so auffassen:

$$\mathbf{Z_p} = \{\sum_{n=0}^{\infty} a_n p^n | 0 \leq a_n \leq p\}$$

$$\mathbf{U} = \mathbf{Z_p^\times} = \{\sum_{n=0}^{\infty} a_n p^n | a_0 \neq 0\} = \{x \in \mathbf{Z_p} | px\}$$

$$\mathbf{U} = \mathbf{Z_p^\times} \mapsto (\mathbf{Z}/p^n\mathbf{Z})^\times$$

2 Gleichungen über den p-adischen Zahlen (Andreas Schmidt)

Sei $f \in \mathbf{Z}_p[X_1, \ldots, X_m]$ und $f_n \in \mathbf{A}_n[X_1, \ldots, X_m]$ das *mod p* reduzierte Polynom von f

Proposition:
Seien $f^{(i)} \in \mathbf{Z}_p[X_1, \ldots, X_m]$ eine Menge von Polynomen mit Koeffizienten in $\mathbf{Z}_p$. Dann sind äquivalent

1. $f^{(i)}$ haben gemeinsame Nullstelle in $(\mathbf{Z}_p)^m$
2. $f_n^{(i)}$ haben gemeinsame Nullstelle in $(\mathbf{A}_n)^m \ \forall\ n > 2$

Lemma:
Sei $...D_n \to D_{n-1} \to \ldots \to D_1$ ein projektives System und $D = \lim_{\leftarrow} D_n$ der projektive Limes dieses Systems. Die D_n seien endlich und nichtleer
$\Rightarrow D$ ist nichtleer

Beweis (Lemma):
Die Aussage ist klar, falls alle $p_n : D_n \to D_{n-1}$ surjektiv sind, da für alle $x_{n-1} \in D_{n-1}$ ein $x_n \in D_n$ existiert so dass $p(x_n) = x_{n-1}$. Somit ist mit $n \to \infty$ auch der Limes nicht leer.
Falls die Abb. nicht surjektiv sind, kann man sie entsprechend verkleinern, so dass sie dies werden. Sei also $D_{n,p}$ das Bild von D_{n+p} in D_n. Diese $D_{n,p}$ sind eine Familie von absteigenden nichtleeren endlichen Teilmengen von D_n. Für p ausreichend großwerden diese stationär (werden also nicht mehr größer). Daher konvergieren sie gegen eine Menge $E_n \subseteq D_n, E_n \neq \emptyset$. Die eingeschränkten Abbildungen $p_n : E_n \to E_{n-1}$ sind surjektiv.

□

Beweis(Proposition):
Setze $D = \{$die gemeinsamen Nullstellen von $f^{(i)}\}$ und setze $D_n = \{$die gemeinsamen Nullstellen von $f_n^{(i)}\}$. Die D_n sind endlich, daraus folgt mit dem Lemma die eine Richtung. Anderst herum gilt falls D endlich ist, dass trivialerweise die Projektionen endlich und nicht leer sind.

□

Ziel ist es jetzt von einer Lösung der Gleichung $f(x) = 0 mod\ (p^n)$ zu einer echten Lösung in $\mathbf{Z}_p$ zu gelangen. Ein wichtiges Hilfsmittel ist dazu das Newton Lemma für p-adische Zahlen. Es besagt, dass unter bestimmten Vorraussetzungen eine existierende Nullstelle der Gleichung $f(x) = 0 mod\ (p^n)$ immer verbessert werden kann, indem man eine Lösung $mod\ p^{n+1}$ findet. Es ist klar, dass diese etwas feiner ist, da die Restklassen $mod\ p^{n+1}$ mehr sind, als die $mod\ p^n$

Lemma (Newton-Methode):
Sei $f \in \mathbf{Z}_p[X]$, $f^{'}(x)$ die Ableitung, $x \in \mathbf{Z}_p$, $n,\ k \in \mathbf{Z}$
mit $0 \leq 2k < n,\ f(x) \equiv 0 (mod\ p^n),\ v_p(f^{'}(x)) = k$

Dann existiert ein $y \in \mathbf{Z}_p$ so dass

$$f(x) \equiv 0 (mod\ p^n), \quad v_p(f^{'}(x)) = k, \quad y \equiv x (mod p^{n-k})$$

Beweis: Definiere $y = x + p^{n-k}z$ für ein $z \in \mathbf{Z}_p$.
Wir betrachten die Taylor Entwicklung um x

$$f(y) = f(x) + p^{n-k} z f^{'}(x) + p^{2(n-k)} a; \quad a \in \mathbf{Z}_p$$

Nach Vorraussetzung können wir schreiben $f(x) = p^n b, b \in \mathbf{Z}_p$ und $f^{'}(x) = p^k c, c \in \mathbf{U}$ also c eine Einheit. Damit können wie z so wählen, dass gilt

$$b + zc \equiv 0 (mod p)$$

da c invertierbar.

$$\begin{aligned} \Rightarrow f(y) &= p^n b + p^{n-k} z p^k c + p^{2(n-k)} a \\ &= p^n (b + zc) + p^{2n-2k} a \\ &\equiv 0\ (mod p^{n+1}) \end{aligned}$$

da $2n-2k > n$. Für den letzten Teil des Beweises betrachten wir noch die Taylorentwicklung um $f^{'}(x)$

$$\begin{aligned} f^{'}(y) &= f^{'}(y) + p^{n-k}za \quad a \in \mathbf{Z}_p \\ &= p^k c + p^{n-k}za \\ &= p^k(c + p^{n-2k}za) \end{aligned}$$

da c Einheit folgt $v_p(f^{'}(x)) = k$

□

Dies erlaubt uns das zentrale Ergebnis zu formulieren

Satz:
Sei $f \in \mathbf{Z}_p[X_1, \ldots, X_m]$; $x \in (\mathbf{Z}_p)^m$, $n,\ k \in \mathbf{Z}$
mit $0 \leq 2k < n,\ f(x) \equiv 0(mod\ p^n)$ und es existiert ein $j \in \{1, \ldots, m\}$ so dass

$$v_p(\frac{\partial f}{\partial X_j}) = k$$

Dann existiert $y \in (Z_p)^m$ so dass

$$y \equiv 0\ (modp^{n-k}) \ \text{ und } \ f(y) = 0$$

Beweis:
Wir betrachten zunächst den Fall $m = 1$. Durch Anwendung des Newton Lemmas lässt sich ausgehend von einem Startwert x^0 sukzessiv eine Folge konstruieren in der die p Potenzen immer weiter erhöht werden

$$x^{q+1} \equiv x^q(mod\ p^{n+q-k}) \quad \text{mit} \quad f(x^q) \equiv 0(mod\ p^{n+q})$$

Dies ist eine Cauchy Folge bezüglich der zuvor definierten Metrik in $\mathbf{Z}_p$. Diese konvergiert in $\mathbf{Z}_p$. Sei y der Grenzwert dann gilt

$$f(y) = 0 \quad \text{und} \quad y \equiv x(mod\ p^{n-k})$$

Der Fall $m > 1$ folgt einfach aus dem ersten. Wir betrachten dazu das Polynom $f^* \in \mathbf{Z_p}[X_j]$ indem man $X_i = x_i$ setzt für $i \neq j$. Dazu findet man eine Lösung y_j wie oben. Setze dann $y_i = x_i$ für $i \neq j$; damit gilt

$$f(y) = 0 \quad \text{und} \quad y \equiv x(mod\ p^{n-k})$$

□

Mit Hilfe des Satzes lassen sich einige einfache Folgerungen für Nullstellen von quadratischen Formen formulieren.

Korollar 1:
Jede einfache, $(mod\ p)$ reduzierte Nullstelle eines Polynoms lässt sich auf eine Nullstelle in $\mathbf{Z}_p$ "hochheben" bzw. "liften".
(Nullstellen heißen einfach, falls mindestens eine partielle Ableitung $\neq 0$)

Beweis: $n = 1, k = 0$ im obigen Satz

□

Definition:
Ein $x \in (\mathbf{Z}_p)^m$ heißt **primitiv**, falls es ein x_i gibt, welches invertierbar ist.

Korollar 2:
Sei $p \neq 2$; $f(x) = \sum a_{ij} X_i X_j$, mit $a_{ij} = a_{ji}$ eine quadratische Form mit $\det(a_{ij})$ invertierbar; Sei $a \in \mathbf{Z}_p$ dann gilt:
Jede primitive Lösung von $f(x) = a(mod\ p)$ kann hochgehoben werden zu einer echten Lösung in $\mathbf{Z}_p$.
Beweis:
Mit Korollar 1 muss lediglich gezeigt werden, dass nicht alle partiellen Ableitungen verschwinden. Betrachte

$$\frac{\partial f}{\partial X_i} = 2 \sum_j a_{ij} X_j$$

da $\det(a_{ij}) \neq 0(mod\ p)$ und mindestens ein x_i nicht durch p teilbar folgt die Behauptung.

□

Korollar 3:
Sei $p = 2$ und die Vorraussetzungen sonst wie in Korollar 2. Dann gilt:
Falls x primitive Lösung von $f(x) \equiv a(mod\ 8)$ und nicht alle partiellen Ableitungen $mod\ 4$ verschwinden, dann kann man x auf eine echte Lösung hochheben.
Beweis:
Dies ist der Fall $n = 3$ und $k = 1$ im Satz. Der Beweis verfolgt analog zu Korollar 2, wobei durch die "2" in der Ableitung die Vorraussetzungen entsprechend angepasst wurden (daher $mod\ 4$)

□