Musterlösung 14

p-Adische Zahlen

1. Sei p eine Primzahl. Zu jedem System von Ziffern $\alpha_i \in \{0, 1, \dots, p-1\}$ mit $\alpha_i = 0$ für alle $i \ll 0$ assoziieren wir die rationale p-adische Zahl

$$\sum_{i \in \mathbb{Z}} \alpha_i p^i \ \in \ \mathbb{Q}_p.$$

Jedes Element von $\mathbb{Q}_p$ besitzt eine eindeutige solche *Ziffernentwicklung*. Wir nennen die Ziffernfolge *schliesslich periodisch*, falls eine *Periode* $d > 0$ existiert, so dass für alle $i \gg 0$ gilt $\alpha_{i+d} = \alpha_i$.

Zeige, dass die p-adischen Zahlen mit schliesslich periodischer Ziffernfolge genau die rationalen Zahlen sind. (*Hinweis:* Bestimme zuerst die ganzen p-adischen Zahlen mit vollständig periodischer Ziffernfolge.)

Lösung:

(a) First consider a p-adic integer β whose digits β_i are completely periodic with period $d \geqslant 1$. Thus $\beta = \sum_{i \geqslant 0} \beta_i p^i$ mit $\beta_{i+d} = \beta_i$ für alle $i \geqslant 0$. Rearranging the terms and using the convergence of the geometric series, we obtain

$$\beta \ = \ \sum_{i=0}^{d-1} \sum_{j=0}^{\infty} \beta_{i+jd} p^{i+jd} \ = \ \sum_{i=0}^{d-1} \beta_i p^i \cdot \sum_{j=0}^{\infty} p^{jd} \ = \ \frac{B}{1-p^d}$$

with $B := \sum_{i=0}^{d-1} \beta_i p^i$. Thus β is a rational number with denominator dividing $1 - p^d$. Moreover, since the digits $\beta_0, \dots, \beta_{d-1}$ are arbitrary in $\{0, 1, \dots, p-1\}$, the number B is an arbitrary element of $\{0, 1, \dots, p^d - 1\}$. It follows that β is an arbitrary element of $\frac{1}{1-p^d}\mathbb{Z}$ satisfying $-1 \leqslant \beta \leqslant 0$.

(b) Next we vary d. We claim that the p-adic integers with completely periodic digit sequences are precisely the rational numbers $-1 \leqslant \beta \leqslant 0$ with $\mathrm{ord}_p(\beta) \geqslant 0$. By (a) we already know one direction, because $p \nmid 1 - p^d$. For the other direction consider any rational number $-1 \leqslant \beta \leqslant 0$ with $\mathrm{ord}_p(\beta) \geqslant 0$. Write $\beta = -\frac{a}{b}$ with relatively prime integers $0 \leqslant a \leqslant b > 0$. Then by assumption $\mathrm{ggT}(p, b) = 1$. Thus the residue class of p in $\mathbb{Z}/b\mathbb{Z}$ is a unit. As $(\mathbb{Z}/b\mathbb{Z})^\times$ is a finite group, each element has finite order; hence there exists an integer $d \geqslant 1$ with $p^d \equiv 1 \mod (b)$. Write $p^d - 1 = kb$ with $k \in \mathbb{Z}^{>0}$. Then

$$\beta \ = \ -\frac{a}{b} \ = \ -\frac{ka}{p^d - 1} \ = \ \frac{ka}{1-p^d}.$$

By construction ka is an integer satisfying $0 \leqslant ka \leqslant kb = p^d - 1$. It can therefore be written in the form $ka = \sum_{i=0}^{d-1} \beta_i p^i$ with digits $\beta_i \in \{0, 1, \dots, p-1\}$. The calculation in (a) thus shows that β has a completely periodic digit sequence, as desired.

(c) Now consider any rational p-adic number $\alpha = \sum_{i \in \mathbb{Z}} \alpha_i p^i$ whose digits satisfy $\alpha_{i+d} = \alpha_i$ for all $i \geqslant i_0$. Write

$$\alpha \;=\; \sum_{i<i_0} \alpha_i p^i + p^{i_0} \sum_{i \geqslant i_0} \alpha_i p^{i-i_0}.$$

Here the first sum is finite and therefore represents a rational number in $\mathbb{Z}[\frac{1}{p}]$. The second sum represents a rational number by (a). Thus α is rational. This proves that any element of $\mathbb{Q}_p$ with an eventually periodic digit sequence lies in $\mathbb{Q}$.

(d) Conversely consider an arbitrary rational number α. Choose $\ell \in \mathbb{Z}^{\geqslant 0}$ such that $\mathrm{ord}_p(p^\ell \alpha) \geqslant 0$.

Case 1: If $p^\ell \alpha > -1$, write $p^\ell \alpha = b + \beta$ with $b \in \mathbb{Z}^{\geqslant 0}$ and $-1 < \beta \leqslant 0$. Then $\mathrm{ord}_p(\beta) \geqslant \min\{\mathrm{ord}_p(p^\ell\alpha), \mathrm{ord}_p(b)\} \geqslant 0$. By (a) and (b) we can therefore write $\beta = \sum_{i \geqslant 0} \beta_i p^i = \frac{B}{1-p^d}$ with $B = \sum_{i=0}^{d-1} \beta_i p^i \in \{0, 1, \dots, p^d - 1\}$. Then the assumption $-1 < \beta$ is equivalent to $B \leqslant p^d - 2$. Choose an integer $e \geqslant 0$ such that $b \leqslant p^{de}$. Then $0 \leqslant b + Bp^{de} \leqslant (1+B)p^{de} \leqslant (p^d - 1)p^{de}$. On the other hand $0 \leqslant \sum_{j=0}^{e-1} Bp^{dj} \leqslant \sum_{j=0}^{e-1} (p^d - 1)p^{dj} \leqslant p^{de} - 1$. Thus

$$p^\ell \alpha \;=\; b + \beta \;=\; \Big(\sum_{j=0}^{e-1} Bp^{dj} + b + Bp^{de} \Big) + \sum_{j=e+1}^{\infty} Bp^{dj},$$

where the content of the parentheses is an integer $\geqslant 0$ and $\leqslant p^{d(e+1)} - 1$. It is therefore equal to $\sum_{i=0}^{de+d-1} \gamma_i p^i$ for certain digits $\gamma_i \in \{0, 1, \dots, p-1\}$. Thus $p^\ell \alpha$ has the digits γ_i for all $0 \leqslant i < d(e+1)$, and the periodic digits β_i for all $i \geqslant d(e+1)$. The digits of α are obtained by shifting these by ℓ positions to the right hand side. Thus α has an eventually periodic digit sequence, as desired.

Case 2: If $p^\ell \alpha < 0$, write $p^\ell \alpha = -b + \beta$ with $b \in \mathbb{Z}^{\geqslant 0}$ and $-1 \leqslant \beta < 0$. Then $\mathrm{ord}_p(\beta) \geqslant \min\{\mathrm{ord}_p(p^\ell\alpha), \mathrm{ord}_p(b)\} \geqslant 0$. By (a) and (b) we can therefore write $\beta = \sum_{i \geqslant 0} \beta_i p^i = \frac{B}{1-p^d}$ with $B = \sum_{i=0}^{d-1} \beta_i p^i \in \{0, 1, \dots, p^d - 1\}$. Then the assumption $\beta < 0$ is equivalent to $B \geqslant 1$. Choose an integer $e \geqslant 0$ such that $b \leqslant p^{de}$. Then $0 \leqslant -b + Bp^{de} \leqslant (p^d - 1)p^{de}$. On the other hand $0 \leqslant \sum_{j=0}^{e-1} Bp^{dj} \leqslant \sum_{j=0}^{e-1} (p^d - 1)p^{dj} \leqslant p^{de} - 1$. Thus

$$p^\ell \alpha \;=\; -b + \beta \;=\; \Big(\sum_{j=0}^{e-1} Bp^{dj} - b + Bp^{de} \Big) + \sum_{j=e+1}^{\infty} Bp^{dj},$$

where the content of the parentheses is an integer $\geqslant 0$ and $\leqslant p^{d(e+1)} - 1$. It is therefore equal to $\sum_{i=0}^{de+d-1} \gamma_i p^i$ for certain digits $\gamma_i \in \{0, 1, \dots, p-1\}$. Thus $p^\ell \alpha$

has the digits γ_i for all $0 \leqslant i < d(e+1)$, and the periodic digits β_i for all $i \geqslant d(e+1)$. The digits of α are obtained by shifting these by ℓ positions to the right hand side. Thus α has an eventually periodic digit sequence, as desired.

Together this proves that every rational number has an eventually periodic digit sequence.

2. Welche der folgenden Gleichungen hat eine Lösung?

   (a) $x^2 + x + 1 = 0$ in $\mathbb{Q}_5$

   (b) $x^2 + x + 1 = 0$ in $\mathbb{Q}_7$

   (c) $x^3 + y^3 = z^3$ mit $xyz \neq 0$ in $\mathbb{Q}_5$

   *(d) $x^3 + y^3 = z^3$ mit $xyz \neq 0$ in $\mathbb{Q}_3$

   Lösung: (a) Sei $\underline{a} \in \mathbb{Q}_5$ mit $\underline{a}^2 + \underline{a} + 1 = 0$. Dann ist jedenfalls $\underline{a} \neq 0$, also $d := \mathrm{ord}_5(\underline{a}) \in \mathbb{Z}$. Wir rechnen unter Benutzung der verschärften Dreiecksungleichung

   $$2d = \mathrm{ord}_5(\underline{a}^2) = \mathrm{ord}_5(-\underline{a} - 1) \geqslant \min\{\mathrm{ord}_5(-\underline{a}), \mathrm{ord}_5(-1)\} = \min\{d, 0\}.$$

   Dies ist nur möglich mit $d = 0$, also mit $\underline{a} \in \mathbb{Z}_5^\times$. Schreibe $\underline{a} = (a_n)_{n\geqslant 0}$ mit $a_n \in \mathbb{Z}/5^n\mathbb{Z}$. Dann ist jedes a_n eine Lösung der Gleichung $x^2 + x + 1 = 0$ in $\mathbb{Z}/5^n\mathbb{Z}$. Insbesondere ist a_1 eine Lösung in dem Körper $\mathbb{F}_5$. Die Werte des Polynoms $x^2 + x + 1$ an den Stellen $0, 1, 2, 3, 4 \in \mathbb{F}_5$ sind aber $1, 3, 2, 3, 1$. Also existiert keine Lösung in $\mathbb{F}_5$, und somit auch keine in $\mathbb{Q}_5$.

   (b) Die Gleichung $x^2 + x + 1 = 0$ ist äquivalent zu $x^3 = 1 \neq x$. Die Lösungen sind also genau die Elemente der Ordnung 3 in der Gruppe $\mathbb{Q}_7^\times$.

   Für jedes $n \geqslant 1$ ist $(\mathbb{Z}/7^n\mathbb{Z})^\times$ eine abelsche Gruppe der Ordnung $7^n - 7^{n-1} = 2 \cdot 3 \cdot 7^{n-1}$. Sie enthält also genau eine Untergruppe der Ordnung 3. Diese liegt nicht in der Untergruppe $1 + 7\mathbb{Z}/7^n\mathbb{Z} < (\mathbb{Z}/7^n\mathbb{Z})^\times$, weil letztere die Ordnung 7^{n-1} hat. Für jedes $1 \leqslant m \leqslant n$ liegt sie somit auch nicht im Kern der Projektionsabbildung $\mathrm{proj}_m^n \colon (\mathbb{Z}/7^n\mathbb{Z})^\times \to (\mathbb{Z}/7^m\mathbb{Z})^\times$. Also induziert proj_m^n einen Isomorphismus zwischen den jeweiligen Untergruppen der Ordnung 3. Das bedeutet, dass wir jedes Element der Ordnung 3 von $(\mathbb{Z}/7^m\mathbb{Z})^\times$ zu einem Element der Ordnung 3 von $(\mathbb{Z}/7^n\mathbb{Z})^\times$ hochheben können. Wir können daher eine Folge von Elementen $a_n \in (\mathbb{Z}/7^n\mathbb{Z})^\times$ der Ordnung 3 finden mit $\mathrm{proj}_m^n(a_n) = a_m$ für alle $1 \leqslant m \leqslant n$. Zusammen ist dann $\underline{a} := (a_n)_n \in \mathbb{Z}_7^\times$ ein Element der Ordnung 3, wie gewünscht.

   (c) Wir konstruieren eine Lösung der Gleichung $x^3 + y^3 = z^3$ mit $x := 1$ und $y := 5$. Für jede solche ist $z^3 = 1^3 + 5^3 = 126 \neq 0$ und somit $xyz \neq 0$. Wir brauchen also nur eine dritte Wurzel aus 126 in $\mathbb{Q}_5$.

   Wegen $126 \not\equiv 0 \mod (5)$ liegt die Restklasse $126 + 5^n\mathbb{Z}$ in der Einheitengruppe $(\mathbb{Z}/5^n\mathbb{Z})^\times$ für jedes $n \geqslant 1$. Dies ist eine abelsche Gruppe der Ordnung $5^n - 5^{n-1} =$

$4 \cdot 5^{n-1}$. Da diese Ordnung kein Vielfaches von 3 ist, besitzt die Gruppe keine Elemente der Ordnung 3. Also ist der Homomorphismus

$$(\mathbb{Z}/5^n\mathbb{Z})^\times \to (\mathbb{Z}/5^n\mathbb{Z})^\times,\ x \mapsto x^3$$

injektiv und somit bijektiv. Für jedes $n \geqslant 1$ existiert also ein eindeutiges Element $a_n \in (\mathbb{Z}/5^n\mathbb{Z})^\times$ mit $a_n^3 = 126 + 5^n\mathbb{Z}$. Aufgrund der Eindeutigkeit gilt dann auch $\mathrm{proj}_m^n(a_n) = a_m$ für alle $n \geqslant m \geqslant 1$. Zusammen ist dann $\underline{a} := (a_n)_n$ ein Element von $\mathbb{Z}_5^\times$ mit $\underline{a}^3 = 126 = 1^3 + 5^3$, wie gewünscht.

Aliter mit der binomischen Formel, unter Verwendung von Aufgabe 3:

(b) Existiert eine Lösung, so ist sie nach der Mitternachtsformel gleich $\frac{-1\pm\sqrt{-3}}{2}$. Es genügt also, ein Element der Form $\sqrt{-3} \in \mathbb{Q}_7$ zu finden, das heisst, eine Lösung der Gleichung $y^2 = -3$. Wegen $-3 \equiv 4 \equiv 2^2 \mod (7)$ ist schon 2 eine Lösung in $\mathbb{Z}/7\mathbb{Z}$. Wir schreiben also $y = 2z$ und suchen eine Lösung der Gleichung $z^2 = -\frac{3}{4} = 1 - \frac{7}{4}$ in $\mathbb{Q}_7$. Wie in der Vorlesung benutzen wir dafür die binomische Formel

$$\underline{a} \ := \ \sum_{m\geqslant 0} \tbinom{\frac{1}{2}}{m} \cdot \left(-\tfrac{7}{4}\right)^m.$$

Wegen $\binom{\frac{1}{2}}{m} \in \mathbb{Z}[\frac{1}{2}]$ hat der m-te Term die Ordnung $\mathrm{ord}_7(\ldots) \geqslant m$. Somit konvergiert die Reihe zu einem wohldefinierten Element in $\mathbb{Z}_7$. Wie in der Vorlesung, oder nach Aufgabe 3, erfüllt dieses die Gleichung $\underline{a}^2 = 1 - \frac{7}{4}$. Also hat die ursprüngliche Gleichung eine Lösung in $\mathbb{Q}_7$.

(c) Eine dritte Wurzel aus $1 + 5^3$ finden wir mit der binomischen Formel durch

$$z \ := \ \sum_{m\geqslant 0} \tbinom{\frac{1}{3}}{m} \cdot 5^{3m}.$$

Wegen $\binom{\frac{1}{3}}{m} \in \mathbb{Z}[\frac{1}{3}]$ hat der m-te Term die Ordnung $\mathrm{ord}_5(\ldots) \geqslant 3m$. Somit konvergiert die Reihe zu einem wohldefinierten Element in $\mathbb{Z}_5$. Nach Aufgabe 3 erfüllt dieses die Gleichung $z^3 = 1 + 5^3$, wie gewünscht.

(d) Analog zu (c) setzen wir $x := 1$ und $y := 3$ sowie

$$z \ := \ \sum_{m\geqslant 0} \tbinom{\frac{1}{3}}{m} \cdot 3^{3m},$$

müssen aber mit der Konvergenz aufpassen. Jedoch ist

$$\mathrm{ord}_3\Big(\binom{\frac{1}{3}}{m}\Big) \ = \ \mathrm{ord}_3\Big(\frac{\frac{1}{3}\cdot(\frac{1}{3}-1)\cdots(\frac{1}{3}-m+1)}{m!}\Big) \ = \ -m - \mathrm{ord}_3(m!).$$

Ausserdem gilt für jede Primzahl p und jede natürliche Zahl m

$$\mathrm{ord}_p(m!) \ = \ \sum_{k\geqslant 1} \Big\lfloor \frac{m}{p^k} \Big\rfloor,$$

was man durch Induktion über m beweist. Somit ist

$$\mathrm{ord}_p(m!) \;<\; \sum_{k\geqslant 1} \frac{m}{p^k} \;=\; \frac{m}{p-1},$$

und daher

$$\mathrm{ord}_3\Big(\binom{\frac{1}{3}}{m}\cdot 3^{3m}\Big) \;>\; -m-\frac{m}{2}+3m \;=\; \frac{3m}{2}.$$

Darum konvergiert die Reihe zu einem wohldefinierten Element in $\mathbb{Z}_3$. Analog zu Aufgabe 3 zeigt man, dass dieses die Gleichung $z^3 = 1+3^3$ erfüllt, wie gewünscht.

Bemerkung: Jedes der beiden Argumente für (c) lässt sich auf alle Primzahlen $p \neq 3$ verallgemeinern und liefert eine Lösung in $\mathbb{Q}_p$. Mit (d) sehen wir somit, dass für jede Primzahl p überhaupt eine Lösung in $\mathbb{Q}_p$ existiert. Ausserdem existiert eine Lösung in $\mathbb{R}$. Nach dem grossen Fermatschen Satz existiert aber keine Lösung in $\mathbb{Q}$.

*3. Zeige:

(a) Für jedes $\alpha \in \mathbb{Q}$ und jedes $m \in \mathbb{Z}^{\geqslant 0}$ liegt der Binomialkoeffizient $\binom{\alpha}{m}$ in $\mathbb{Z}[\alpha]$.

(b) Für alle $\alpha, \beta \in \mathbb{Q}$ und $m \in \mathbb{Z}^{\geqslant 0}$ gilt $\binom{\alpha+\beta}{m} = \sum_{n=0}^{m} \binom{\alpha}{n}\cdot\binom{\beta}{m-n}$ in $\mathbb{Q}$.

(c) Seien p eine Primzahl und $\alpha \in \mathbb{Q}\cap\mathbb{Z}_p$ sowie $\underline{a} \in p\mathbb{Z}_p$. Dann konvergiert die Reihe

$$A(\underline{a},\alpha) \;:=\; \sum_{m\geqslant 0} \tbinom{\alpha}{m}\cdot \underline{a}^m \;\in\; \mathbb{Z}_p.$$

(d) Für alle $\alpha, \beta \in \mathbb{Q}\cap\mathbb{Z}_p$ gilt $A(\underline{a},\alpha)\cdot A(\underline{a},\beta) = A(\underline{a},\alpha+\beta)$.

(e) Schreibe $\alpha \in \mathbb{Q}\cap\mathbb{Z}_p$ in der Form $\alpha = \frac{r}{s}$ mit $r \in \mathbb{Z}$ und $s \in \mathbb{Z}^{>0}$ und $p \nmid s$. Dann gilt $A(\underline{a},\alpha)^s = (1+\underline{a})^r$. Lose gesprochen gilt also "$A(\underline{a},\frac{r}{s}) = (1+\underline{a})^{\alpha}$."

Lösung: (a) Schreibe $\alpha = \frac{r}{s}$ mit $r \in \mathbb{Z}$ und $s \in \mathbb{Z}^{>0}$ und $\mathrm{ggT}(r,s) = 1$. Nach Serie 1 Aufgabe 7 gilt dann $\mathbb{Z}[\alpha] = \mathbb{Z}[\frac{1}{s}]$. Wir müssen also zeigen, dass $\mathrm{ord}_p(\binom{\alpha}{m}) \geqslant 0$ ist für jede Primzahl $p \nmid s$. Betrachte irgendeine ganze Zahl $N \gg 0$. Dann ist $\mathrm{ggT}(s,p^N) = 1$ und nach dem Chinesischen Restsatz existieren ganze Zahlen t,u mit $ts+up^N = 1$. Daraus folgt $\alpha = \frac{r}{s} = tr + \frac{ur}{s}\cdot p^N$, also $\alpha \equiv tr \mod p^N\mathbb{Z}[\frac{1}{s}]$. Dies impliziert

$$\binom{\alpha}{m} \;=\; \frac{\alpha\cdot(\alpha-1)\cdots(\alpha-m+1)}{m!} \;\equiv\; \frac{tr\cdot(tr-1)\cdots(tr-m+1)}{m!} \;=\; \binom{tr}{m}$$

modulo $\frac{p^N}{m!}\mathbb{Z}[\frac{1}{s}]$. Dabei ist jedenfalls $\binom{tr}{m} \in \mathbb{Z}$. Haben wir $N \geqslant \mathrm{ord}_p(m!)$ gewählt, so gilt auch $\mathrm{ord}_p(\frac{p^N}{m!}) \geqslant 0$. Als Summe zweier rationaler Zahlen mit $\mathrm{ord}_p(\ldots) \geqslant 0$ gilt daher auch $\mathrm{ord}_p(\binom{\alpha}{m}) \geqslant 0$, wie gewünscht.

(b) For any complex numbers α and z with $|z| < 1$ we have

$$(1+z)^\alpha \;:=\; \exp(\alpha \cdot \log(1+z)) \;\overset{!}{=}\; \sum_{m \geqslant 0} \tbinom{\alpha}{m} \cdot z^m$$

by the binomial theorem. Thus for any further complex number β we have

$$\begin{array}{ccc} (1+z)^\alpha \cdot (1+z)^\beta & = & \Big(\sum_{n \geqslant 0} \tbinom{\alpha}{n} \cdot z^n\Big) \cdot \Big(\sum_{k \geqslant 0} \tbinom{\beta}{k} \cdot z^k\Big) = \sum_{m \geqslant 0} \Big(\sum_{n=0}^{m} \tbinom{\alpha}{n} \tbinom{\beta}{m-n}\Big) \cdot z^m \\ \| & & \\ (1+z)^{\alpha+\beta} & = & \sum_{m \geqslant 0} \tbinom{\alpha+\beta}{m} \cdot z^m \end{array}$$

The desired equation thus follows from the identity theorem for convergent power series.

(c) By (a) we have $\binom{\alpha}{m} \in \mathbb{Z}[\alpha] \subset \mathbb{Z}[\frac{1}{s}]$ for all $m \geqslant 0$. In particular we have $\mathrm{ord}_p(\binom{\alpha}{m}) \geqslant 0$. By assumption we also have $\mathrm{ord}_p(\underline{a}) \geqslant 1$. Thus $\mathrm{ord}_p(\binom{\alpha}{m}\underline{a}^m) \geqslant m$, and so the series converges in $\mathbb{Z}_p$.

(d) For any two $\alpha, \beta \in \mathbb{Q} \cap \mathbb{Z}_p$ we have

$$\begin{array}{ccc} A(\underline{a}, \alpha+\beta) = \sum_{m \geqslant 0} \binom{\alpha+\beta}{m} \cdot \underline{a}^m & \overset{\text{(b)}}{=\!=} & \sum_{m \geqslant 0} \Big(\sum_{n=0}^{m} \tbinom{\alpha}{n} \tbinom{\beta}{m-n}\Big) \cdot \underline{a}^m \\ & & \| \\ A(\underline{a}, \alpha) \cdot A(\underline{a}, \beta) & = & \Big(\sum_{n \geqslant 0} \tbinom{\alpha}{n} \cdot \underline{a}^n\Big) \cdot \Big(\sum_{k \geqslant 0} \tbinom{\beta}{k} \cdot \underline{a}^k\Big) \end{array}$$

in $\mathbb{Z}_p$ because convergent sums in $\mathbb{Z}_p$ can be rearranged arbitrarily.

(e) By induction (d) implies that $A(\underline{a}, \alpha)^\ell = A(\underline{a}, \ell\alpha)$ for all $\ell \in \mathbb{Z}^{\geqslant 1}$. In particular we have $A(\underline{a}, \alpha)^s = A(\underline{a}, s\alpha) = A(\underline{a}, r)$. If $r \geqslant 0$, we have $\binom{r}{m} = 0$ for all $m > r$ and hence $A(\underline{a}, r) = (1+\underline{a})^r$ by the binomial theorem. If $r < 0$, from (c) and the preceding case we deduce that $A(\underline{a}, r) \cdot A(\underline{a}, -r) = A(\underline{a}, 0) = 1$ and hence $A(\underline{a}, r) = A(\underline{a}, -r)^{-1} \overset{!}{=} \big((1+\underline{a})^{-r}\big)^{-1} = (1+\underline{a})^r$. In both cases we conclude that $A(\underline{a}, \alpha)^s = (1+\underline{a})^r$, as desired.

Bemerkung: (b) haben wir bewiesen mittels Analysis über $\mathbb{R}$ oder $\mathbb{C}$, und das Resultat haben wir in (d) eingesetzt in eine Formel über $\mathbb{Q}_p$. Ein faszinierendes Wechselspiel zwischen klassischer und p-adischer Analysis.

**4. Für welche Primzahlen p besitzt die Gleichung $x^2 = 2015$ eine Lösung in $\mathbb{Q}_p$? (*Hinweis*: Googeln Sie „quadratisches Reziprozitätsgesetz“.)