Modularität und Fermats letzter Satz

Ausarbeitung zum Vortrag im Seminar zur Kryptographie

von

Christian Geyer

27.06.2011

Betreuer:
Dr. M. Barakat

Technische Universität Kaiserslautern
Fachbereich Mathematik
AG Algebra, Geometrie und Computeralgebra

Vorwort

Fermats letzter Satz ist einer der großen Sätze der Mathematik. Viele Mathematiker haben sich mit der Lösbarkeit der Gleichung $x^n + y^n = z^n$ über $\mathbb{Z}$ beschäftigt, vollständig bewiesen wurde er jedoch erst in den letzten Jahren des 20.Jahrhunderts.

In dem Beweis von Fermats letzten Satz spielen viele Teilgebiete der Mathematik eine Rolle, vor allem die Zahlentheorie, die Algebra und die Funktionentheorie. Daher ist der Beweis sehr umfangreich und wird in dieser Ausarbeitung nicht vollständig geführt. Insbesondere das Kernstück, der Modularitätssatz für elliptischen Kurven, würde den Rahmen des Seminarvortrags sprengen.

Wer sich für eine ausführlichere Darstellung und eine tiefergehende Behandlung des Beweises interessiert, kann in [Cor] und [Coa] mehr Details nachlesen. Insbesondere [Cor] ist empfehlenswert, jedoch nicht leicht zu lesen, da hier viele der an dem Beweis beteiligten Mathematiker jeweils ihren Anteil am Beweis darstellen.

Im Anhang findet man alle für den Vortrag wichtigen Definitionen und Aussagen aus der Funktionentheorie und über p-adische Zahlen. Dort findet man zudem Hinweise auf weiterführende oder umfangreichere Literatur zu dem jeweiligen Thema.

Inhaltsverzeichnis

Bezeichnungen

Folgende Bezeichnungen werden verwendet:

$\mathbb{1}$	die Einheitsmatrix
$\mathbb{K}$	ein Körper mit $\text{char}(\mathbb{K}) = 0$
$\mathbb{N}$	Menge der natürlichen Zahlen mit $0 \in \mathbb{N}$
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{Z}_{>0}$	Menge der positiven ganzen Zahlen ($\equiv \mathbb{N}^+$)
$\mathbb{Q}$	Menge der rationalen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{C}$	Menge der komplexen Zahlen
$\mathbb{P} := \{p \in \mathbb{Z}_{>0} \mid p \; irreduzibel\}$	Menge aller Primzahlen
$\mathcal{H} := \{z \in \mathbb{C} \mid \text{Im}(z) \geq 0\}$	die obere Halbebene
$\mathbb{F}_p$	Körper mit p Elementen
$\overline{K}$	algebraischer Abschluss eines Körpers K
$\mathbb{Z}_p$	Menge der ganzen p-adischen Zahlen
$\mathbb{Q}_p$	Menge der p-adischen Zahlen
$\mathcal{O}_p$	Ring, der die p-adischen Zahlen enthält
PFZ	Primfaktorzerlegung
GL_n	Menge aller invertierbaren $n \times n$-Matrizen
$\text{SL}_n \subset GL_n$	die spezielle Lineare Gruppe
$\text{Gal}(L/K)$	die Galois-Gurppe der Körpererweiterung L/K
$E[m]$	Menge aller m-Torsionspunkte der eliptischen Kurve E

1 Fermats letzter Satz

1.1 Spezialfälle

In diesem Kapitel betrachten wir zunächst ein paar einfache Spezialfälle, welche nur geringe mathematische Kenntnisse benötigen und daher auch im Mathematikunterricht der Sekundarstufe behandelt werden können.

Lemma 1.1. ***Lösbarkeit für*** $n \in \{1, 2\}$
Für $n \in \{1, 2\}$ *existieren* $x, y, z \in \mathbb{Z}\backslash\{0\}$ *welche die Gleichung*

$$x^n + y^n = z^n \tag{1}$$

lösen.

Beweis:
Der Fall $n = 1$ ist trivial, da $(\mathbb{Z}, +, \cdot)$ ein Ring ist.
Für den Fall $n = 2$ betrachte $u, v \in \mathbb{Z}_{>0}$ mit $u > v$, $u - v \equiv 1 \pmod 2$ und $\text{ggt}(u, v) = 1$.
definiere $x := u^2 - v^2$, $y := 2uv$ und $z := u^2 + v^2$, dann sind $x, y, z \geq 0$ teilerfremd und

$$x^2 + y^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2 = (u^2 + v^2)^2 = z^2 \tag{2}$$

somit haben wir Lösungen gefunden. □

Bemerkung 1.2. ***phytagoreische Zahlentripel***
Ein Tripel $(x, y, z) \in \mathbb{Z}^3$*, welches die Gleichung* $x^2+y^2 = z^2$ *erfüllt heißt* ***pythagoreisches Zahlentripel (PZT)****. Im Beweis des Satzes wurde ein teilerfremdes PZT konstruiert. Solche teilerfremden PZT haben die Eigenschaft, dass* z *und genau eine der beiden Zahlen* x, y *ungerade sind. Zudem erhält man aus den teilerfremden PZT unendlich viele Lösungen der Gleichung* $x^2 + y^2 = z^2$*, indem man für* $a \in \mathbb{Z}\backslash\{0\}$ *das Tripel* (ax, ay, az) *bildet. Die Beweise hierfür findet man z.B. in [Ma].*

Um die folgenden Spezialfälle zu zeigen, benötigen wir noch die folgenden kleinen Hilfsmittel:

Lemma 1.3. *Das Gleichungssystem*

$$x^2 + y^2 = z^2 \tag{3}$$
$$x^2 - y^2 = w^2 \tag{4}$$

ist nicht über $\mathbb{Z}$ *lösbar.*

Beweis:siehe [Her] S. 9ff.

□

Lemma 1.4. *Die Fläche eines ganzzahligen, rechtwinkligen Dreiecks ist nie eine Quadratzahl*

Beweis:
Gegeben sei ein rechtwinkliges Dreieck mit der ganzzahligen Hypothenuse c und den ganzzahligen Katheten a, b sowie oBdA $\text{ggt}(a, b, c) = 1$.
Angenommen die Dreiecksfläche wäre eine Quadratzahl, d.h.

$$A_\Delta = \frac{1}{2}bc \stackrel{!}{=} \alpha^2 \tag{5}$$

für ein $\alpha \in \mathbb{Z}$. Das Tripel $(a, b, c) \in \mathbb{Z}^3$ ist ein teilerfremdes PZT und folglich existieren $u, v \in \mathbb{Z}$ mit $u > v$, $\text{ggt}(u, v) = 1$ und $u - v \equiv 0 \pmod 2$, so dass

$$a = 2uv, \quad b = u^2 - v^2, \quad c = u^2 + v^2 \tag{6}$$

damit erhält man:

$$\alpha^2 = \frac{1}{2}(2uv)(u^2 - v^2) = uv(u - v)(u + v) \tag{7}$$

ferner sind $u, v, u - v, u + v$ paarweise teilerfremd. Daher müssen diese Zahlen Quadratzahlen sein, d.h.

$$u = \varphi^2, \quad v = \eta^2, \quad u + v = \mu^2, \quad u - v = \xi^2 \tag{8}$$

für geeignete $\varphi, \eta, \mu, \xi \in \mathbb{Z}$. Dies liefert das Gleichungssystem

$$\varphi^2 - \eta^2 = \xi^2 \tag{9}$$
$$\varphi^2 + \eta^2 = \mu^2 \tag{10}$$

nach Lemma 1.3 existiert für dieses System jedoch keine Lösung über $\mathbb{Z}$ ↯

□

Satz 1.5. *Der Fall $n = 3$*
Es gibt kein Tripel $(x, y, z) \in \mathbb{Z}^3$ mit $xyz \neq 0$ welches die Gleichung $x^3 + y^3 = z^3$ erfüllt.

Beweis:
Der Beweis ist länglich, weshalb wir ihn hier nicht ausführen. Die Idee ist, dass man wieder oBdA teilerfremde Lösungen der Gleichung $x^3 + y^3 = z^3$ betrachtet und zeigt, dass es zu einer gegebenen Lösung immer eine kleiner Lösung geben muss. Da $\mathbb{N}$ aber nach unter

beschränkt ist, kann es jedoch nur endlich viele Lösungen geben, d.h. es muss eine kleinste Lösung geben. $\lightning$
Die Details des Beweises kann man in [Her] auf S. 12ff. nachlesen.

□

Damit kommen wir zum Fall $n = 4$.

Satz 1.6. *Der Fall $n = 4$*
Es gibt kein Tripel $(x, y, z) \in \mathbb{Z}^3$ mit $xyz \neq 0$ welches die Gleichung $x^4 + y^4 = z^4$ erfüllt.

Beweis:
Sei $(a, b, c) \in \mathbb{Z}^3$ mit $xyz \neq 0$ eine Lösung der Gleichung $x^4 + y^4 = z^4$, dann gilt:

$$(c^4 + b^4)^2 = (c^4 - b^4)^2 + 4c^4b^4 = (c^4 - b^4)^2 + (2c^2b^2)^2 \tag{11}$$

dies entspricht der Gleichung für den Fall für $n = 2$, welche für rechtwinklige Dreiecke erfüllt wird. Für das zugehörige rechtwinklige Dreieck gilt:

$$A_\Delta = \frac{1}{2}(c^4 - b^4)(2c^2b^2) = (c^4 - b^4)c^2b^2 \tag{12}$$

dies lässt sich mit $a^4 = c^4 - b^4$ umformen zu

$$A_\Delta = a^4c^2b^2 = (a^2cb)^2 \tag{13}$$

was jedoch nach Lemma 1.4 nicht möglich ist $\lightning$

□

1.2 Der allgemeine Fall

Die allgemeine Aussage

$$\forall n \geq 3 \nexists\, x, y, z \in \mathbb{Z}\backslash\{0\} :\ x^n + y^n = z^n \tag{14}$$

war lange Zeit unbewiesen. Zwar gab es immer wieder Beweisversuche, diese waren aber meist fehlerhaft. Im Laufe der Zeit wurden immer mehr Spezialfälle gezeigt, den endgültigen Beweis lieferte jedoch erst Andrew Wiles 1995 in dem er die Vermutung von Taniyama-Shimura bewies und somit, dank der Vorarbeit vieler Mathematiker, Fermats letzten Satz als Folgerung erhielt.

Einen Teil dieses langen Weges bis zum Beweis des Satzes wollen wir nun nachvollziehen. Fangen wir ganz einfach an:

Lemma 1.7. *Um Fermats letzten Satz zu zeigen, genügt es die Fälle* $n \in \{1, 2, 3, 4\}$ *und* $n \in \mathbb{P}\backslash\{2\}$ *zu betrachten.*

Beweis:
Ist $n \in \mathbb{N}$ mit $n \geq 3$, so wird n entweder von 4 oder von $p \in \mathbb{P}\backslash\{2\}$ geteilt. Daher gilt:

$$x^n + y^n = z^n \;\Leftrightarrow\; \begin{cases} (x^m)^4 + (y^m)^4 = (z^m)^4 \;\text{für } 4|n \\ (x^m)^p + (y^m)^p = (z^m)^p \;\text{für } p|n \end{cases} \tag{15}$$

□

Einer der Mathematiker, welche einen Teil der Vorarbeit leisteten, war Gerhard Frey. Mit seiner Vorarbeit wollen wir uns nun beschäftigen.

Lemma 1.8. *Sei* $p \in \mathbb{P}$ *ungerade und seien* $a, b, c \in \mathbb{Z}\backslash\{0\}$ *mit* $a^p + b^p = c^p$*, dann existieren* $a', b', c' \in \mathbb{Z}\backslash\{0\}$ *mit* $a'^p + b'^p = c'^p$ *sowie* $\mathrm{ggt}(a', b', c') = 1$ *und* $b \equiv 0 \pmod 2$*,* $a \equiv 3 \pmod 4$

Beweis:Ist $\mathrm{ggt}(a, b, c) = h \neq 1$, dann gilt

$$\left(\frac{a}{h}\right)^p + \left(\frac{b}{h}\right)^p = \left(\frac{c}{h}\right)^p \tag{16}$$

also ist auch $(a', b', c') := \left(\frac{a}{h}, \frac{b}{h}, \frac{c}{h}\right) \in \mathbb{Z}$ eine Lösung der diophantischen Gleichung mit $a'b'c' \neq 0$ und $\mathrm{ggt}(a', b', c') = 1$.
Ferner gibt es nur einen möglichen Fall, nämlich b' gerade und a', c' ungerade, denn a', b', c' gerade ist auf Grund der Teilerfremdheit nicht möglich und in den anderen Fällen sind genau zwei der drei Zahlen a', b', c' ungerade, so dass wir wegen $-z^p = (-z)^p$ durch ggf. umbenennen diese Fälle in den Fall mit b' gerde überführen können. Also gilt $b' \equiv 0 \pmod 2$.
Gilt nun $a' \equiv 3 \pmod 4$, so sind wir fertig. Anderenfalls gilt $a' \equiv 1 \pmod 4$. Dann betrachte das Tripel $(-a', -b', -c')$, welches natürlich auch eine Lösung ist. Nun gilt aber: $-b' \equiv 0 \pmod 2$ und $-a' \equiv -1 = 3 \pmod 4$

□

Damit können wir einen Zusammenhang zwischen (potentiellen) Lösungen der Gleichung 1 und elliptischen Kurven herstellen.

Definition 1.9. *Frey-Kurve*
Sei $p \in \mathbb{P}$ ungerade, dann heißt die elliptische Kurve

$$E_{Frey}: \ y^2 = x(x - a^p)(x + b^p) \tag{17}$$

mit $a, b \in \mathbb{Z}$ teilerfremd und $b \equiv 0 \pmod 2$, $a \equiv 3 \pmod 4$, ***Frey-Kurve****. Ihre Diskriminante ist gegeben durch*

$$\Delta = (a^p(-b^p)(a^p + b^p))^2 \tag{18}$$

Warum wir genau diese Kurve betrachten, ist zunächst nicht offensichtlich. In der Tat steckt dahinter jede Menge Theorie, mit der man ohne Probleme eine Vorlesung im Umfang von 4 SWS füllen könnte. Gerhard Frey beschäftigte sich ausführlich mit dem Zusammenhang zwischen diophantischen Gleichungen und elliptischen Kurven[1] und schlug daher die Betrachtung der Kurve E_{Frey} vor. Der für uns wichtige Teil seiner Arbeit ist die folgende, hier nicht bewiesene Aussage:

Bemerkung 1.10. *(Diskriminante von E_{Frey})*
Exististiert eine Lösung von $x^p + y^p = z^p$ über $\mathbb{Z}$, so existiert die Kurve E_{Frey}. In diesem Fall wird (18) zu $\Delta = (abc)^{2p}$. Jedoch muss dieser Ausdruck aus „technischen Gründen[2]“ modifiziert werden, so dass die ***minimale Diskriminante*** *folgende Form erhält*

$$\Delta = 2^{-8}(abc)^{2l} \tag{19}$$

[1] siehe z.B. [Fr]
[2] siehe Bemerkung 2.5

2 Der Modularitätssatz

In diesem Kapitel wollen wir die Grundlagen für den Beweis von Fermats letztem Satz legen. Dazu betrachten wir, falls nicht anders definiert, immer elliptische Kurven über dem Grundkörper $\mathbb{Q}$.

2.1 Grundlegende Begriffe

Bemerkung 2.1. *Eigenformen*
Sei E eine Elliptische Kurve über einem Körper $\mathbb{K}$ so kann man jede elliptische Kurve durch Variablentransformation auf die Form

$$E: \ y^2 = x^3 + Ax + B \tag{20}$$

bringen. Insbesondere kann jede elliptische Kurve über $\mathbb{Q}$ auf diese Form mit $A, B \in \mathbb{Z}$ gebracht werden.
Ferner muss E glatt sein, d.h. falls E gegeben durch $y^2 = f(x)$ gilt (vgl. [Ba]):

$$E \text{ glatt } \Leftrightarrow \operatorname{disc}(f) \neq 0 \Leftrightarrow f \text{ hat keine mehrfache Nullstelle} \tag{21}$$

Definition 2.2. *gute und schlechte Reduktion*
Sei $p \in \mathbb{P}$. Wir reduzieren die Gleichung (20) modulo p.

*a) Falls $E \mod p$ eine elliptische Kurve ist, sagt man E hat eine **gute Reduktion** $\mod p$.*

*b) Falls $E \mod p$ eine mehrfache Nullstelle hat, sagt man E hat eine **schlechte Reduktion** $\mod p$.*

*i) Wenn E eine dreifache Nullstelle besitzt, so sagt man E hat eine **additive Reduktion** $\mod p$.*

*ii) Wenn E eine zweifache Nullstelle besitzt, so sagt man E hat eine **multiplikative Reduktion** $\mod p$.*

Im Falle der multiplikativen Reduktion hat E

- ***zerfallende** multiplikative Reduktion, wenn die Steigungen der Tangenten an E im singulären Punkt aus $\mathbb{F}_p$ sind*
- *sonst **nicht-zerfallende** multiplikative Reduktion*

Bemerkung 2.3. *Primzahlen mit guter und schlechter Reduktion*
Die Primzahlen $p \in \mathbb{P}$, welche die Bedingung a) der Definition erfüllen nennt man Primzahlen mit guter Reduktion, diejenigen, welche b) erfüllen Primzahlen mit schlechter Reduktion. Entsprechend sind auch die Bezeichnungen in i) bzw. ii) Primzahlen mit additiver bzw. multiplikativer Reduktion.

Das finden potentieller Primzahlen mit schlechter Reduktion ist relativ einfach. Wie es genau Funktioniert zeigt uns das folgende Lemma

Lemma 2.4. *Primzahlen mit schlechter Reduktion*
Sei E eine elliptische Kurve und Δ die zugehörige Diskriminante, dann gilt:

$$E \text{ hat schlechte Reduktion modulo } p \;\Rightarrow\; p|\Delta \tag{22}$$

Beweis:
Sei I eine Indexmenge, $\{a_i \mid i \in I\}$ die Menge aller Nullstellen von E und p eine Primzahl mit schlechter Reduktion, d.h. E hat eine mehrfache Nullstelle modulo p, dann gilt:

$$\Delta = \prod_{i<j}(a_i - a_j) \equiv 0 \bmod p \tag{23}$$

also gilt $p|\Delta$

□

Diese Aussage scheint schwach zu sein, da sie nur ein notwendiges Kriterium liefert. Unter gewissen Bedingungen lässt sie sich jedoch noch zu einer notwendigen und hinreichenden Bedingung erweitern

Bemerkung 2.5. *notwendiges und hinreichendes Kriterium für schlechte Reduktion*

a) *Für elliptische Kurven der Form $y^2 = x^3+Ax+B$ mit $A, B \in \mathbb{Z}$ gibt es meist mehrere mögliche Werte für A, B welche die selbe Kurve definieren. Man kann zeigen, dass es immer eine Wahl von $A, B \in \mathbb{Z}$ gibt, so dass für alle $p \in \mathbb{P}$ die Anzahl der verschiedenen Nullstellen von E mod p größtmöglich ist. Die Gleichung dieser Wahl nennt man **minimale Weierstrassgleichung** von E und die zugehörige Diskriminante Δ heißt **Minimaldiskriminante** von E.*

b) *Ersetzt man in Lemma 2.4 die Diskriminante durch die Minimaldiskriminante, so gilt die Äquivalenz.*

Schauen wir uns dieses Kriterium einmal anhand einem Beispiel an.

Beispiel 2.6. *Betrachte E gegeben durch*

$$y^2 = x^3 - 270000x + 128250000$$

dann gilt $\Delta = -2^8 3^{12} 5^{12} 11$, also hat E höchstens bei $2, 3, 5, 11$ schlechte Reduktion. Durch die Variablentransformation $x = 25x_1$, $y = 125y_1$ erhält man

$$y_1^2 = x_1^3 - 432x_1 + 8208$$

mit $\Delta = -2^8 3^{12} 11$, d.h. E hat eine gute Reduktion modulo 5. Um die weiteren Primzahlen zu untersuchen müssen wir generalisierte Weierstarssgleichungen betrachten. Eine solche liefert die Transformation $x_1 = 9x_2 - 12$, $y_1 = 27y_2$. Wir erhalten

$$y_2^2 = x_2^3 - 4x_2^2 + 16$$

mit der Diskriminante $\Delta = -2^8 11$, so dass E auch modulo 3 eine gute Reduktion besitzt. Eine letzte Substitution liefert uns das endgültige Resultat. Setze $x_2 = 4x_3$, $y_2 = 8y_3 + 4$, dann hat E die Form

$$y_3^2 + y_3 = x_3^3 - x_3^2$$

Diese Gleichung ist nicht-singulär modulo 2, folglich besitzt E auch modulo 2 eine gute Reduktion.
Man kann zeigen, dass man durch Variablentransformation kein besseres Ergebnis erzielen kann, d.h. die minimale Weierstrassgleichung ist gegeben durch

$$y_3^2 + y_3 = x_3^3 + x_3^2$$

Folglich hat E nur modulo 11 eine schlechte Reduktion.

Oft ist man an elliptischen Kurven mit möglichst guten Eigenschaften, d.h. deren Reduktionen modulo der verschiedenen Primzahlen „*so gut wie möglich*“ sind, interessiert. Aus Lemma 2.4 und Bemerkung 2.5 b) folgt jedoch, dass es zu jeder elliptischen Kurve mindestens eine Primzahl mit schlechter Reduktion gibt. Daher bedeutet in diesem Sinne die Formulierung „*so gut wie möglich*“, dass man nach Möglichkeit keine Primzahlen mit additiver Reduktion haben möchte. Elliptische Kurven, die diese Bedingung erfüllen, sind von besonderer Bedeutung und erhalten daher einen eigenen Namen:

Definition 2.7. *semistabile Kurven*
Eine elliptische Kurve heißt ***semistabil****, wenn sie für alle $p \in \mathbb{P}$ eine gute oder multiplikative Reduktion besitzt.*

Die für uns interessante Kurve E_{Frey} besitzt, wie folgendes Lemma zeigt, zum Glück diese gute Eigenschaft.

Lemma 2.8. *Sei $p \in \mathbb{P}$, dann ist E_{Frey} semistabil.*

Beweis:
Wir zeigen, dass E_{Frey} keine additive Reduktion modulo einer Primzahl l haben kann. Sei dazu $\alpha := a^p$ und $\beta := -b^p$. Betrachte dann das kubische Polynom

$$f = x(x-\alpha)(x-\beta) \tag{24}$$

Dieses Polynom kann keine dreifache Nullstelle mod l haben, denn:
Sei f_l die Reduktion von f mod l und $c \in \mathbb{Z}$ dreifache Nullstelle von f mod l, dann gilt:

$$x(x-\bar{\alpha})(x-\bar{\beta}) = f_l = x^3 - 3x^2\bar{c} + 3x\bar{c}^2 - \bar{c}^3 \tag{25}$$

da beide Seiten identisch sind, die linke Seite jedoch keinen konstanten Summanden enthält, muss $c \equiv 0 \bmod l$ gelten.
$\Rightarrow l|c \;\Rightarrow x^3 = f_l = x^3 - \bar{\alpha}x^2 - \bar{\beta}x^2 + \bar{\alpha}\bar{\beta}x$
$\Rightarrow l|\alpha$ und $l|\beta$ $\quad\lightning$ im Widerspruch zu $\mathrm{ggt}(\alpha,\beta) = 1$ □

Definition 2.9. *Sei $p \in \mathbb{P}$, dann definiere*

$$a_p = \begin{cases} p+1-\#E(\mathbb{F}_p) & \text{falls gute Reduktion mod p} \\ 0 & \text{falls additive Reduktion mod p} \\ 1 & \text{falls zerfallende multiplikative Reduktion mod p} \\ -1 & \text{falls nicht-zerfallende multiplikative Reduktion mod p} \end{cases} \tag{26}$$

und setze für $n = \prod_j p_j^{n_j}$ PFZ

$$a_n := \prod_j a_{p_j}^{n_j} \tag{27}$$

sowie für $\tau \in \mathcal{H}$ und $q = \mathrm{e}^{2\pi\mathrm{i}\tau}$

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n \tag{28}$$

Bemerkung 2.10. *Man beachte:*

a) Die Reihe $f_E(\tau)$ konvergiert und stellt nichts anderes als eine kodierung der Anzahl der Punkte auf E modulo der verschiedenen Primzahlen dar.

b) Die Abbildung

$$\begin{array}{ccc} \mathbb{N}^+ & \to & \mathbb{R} \\ n & \mapsto & a_n \end{array} \tag{29}$$

ist offensichtlich eine zahlentheoretisch multiplikative Funktion

Die Funktion f_E wird für uns von großer Bedeutung sein. Sie fällt hier vom Himmel, daher werde ich im folgenden Unterkapitel einen möglichen Weg aufzeigen, wie man auf f_E kommt.

2.2 Galoisdarstellungen

Eine Möglichkeit, die Funktion f_E zu motivieren geht über die Galoisdarstellungen. Zudem sind diese Darstellungen ein wichtiger Bestandteil des Beweises von Wiles für den Modularitätssatz. Daher beschäftigen wir uns im folgenden Abschnitt damit.

Sei E eine elliptische Kurve über $\mathbb{Q}$, dann gilt (vgl. [Kle])

$$E[m] \cong {}^{\mathbb{Z}}/_{m\mathbb{Z}} \oplus {}^{\mathbb{Z}}/_{m\mathbb{Z}} \tag{30}$$

Sei nun $\{\beta_1, \beta_2\}$ eine Basis von $E[m]$ und sei $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, dann ist auch $\sigma\beta_i \in E[m]$ und es gilt

$$\begin{aligned} \sigma\beta_1 &= a\beta_1 + c\beta_2 \\ \sigma\beta_2 &= b\beta_1 + d\beta_2 \end{aligned}$$

wobei $a, b, c, d \in {}^{\mathbb{Z}}/_{m\mathbb{Z}}$. Somit erhält man den Isomorphismus

$$\rho_m : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2({}^{\mathbb{Z}}/_{m\mathbb{Z}}) \ : \ \sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Definition 2.11. ***Galoisdarstellung***
Ist $m = p \in \mathbb{P}$, so nennen wir ρ_p die mod p ***Galoisdarstellung*** *von E*

Bemerkung 2.12. *Die Galoisdarstellungen lässt sich auf $m = p^n$ mit $n \in \mathbb{N}^+$ verallgemeinern, wobei dann $\rho_{p^n} \equiv \rho_{p^{n+1}} \pmod{p^n}$ gilt. Ferner erhält man auf diese Weise*

auch

$$\rho_{p^\infty} \ : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_p)$$

wobei $\mathcal{O}_p$ ein Ring ist, der die p-adischen Zahlen enthält und Charakteristik 0 besitzt.

Durch die Betrachtung geeigneter Elemente (vgl. [Wa], S.449) $\mathrm{Frob_r} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ für eine Primzahl r, deren Anwendung auf $E(\overline{\mathbb{Q}})$ der Anwendung von ϕ_r auf $E(\overline{\mathbb{F}}_r)$ entspricht, erhält man unter gewissen Voraussetzungen[3] für die Darstellung

$$\rho : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_p)$$

dass $a_r = \mathrm{Spur}(\rho(\mathrm{Frob_r}))$. Hierbei erhält man, dass a_r das a_p aus Definition 2.9 ist.

Dies motiviert und liefert uns in letzter Konsequenz die Definition von f_E.

Bemerkung 2.13. *In der Tat kann man mit sehr viel mathematischem Aufwand zeigen, dass nicht nur die elliptische Kurve die Funktion f_E eindeutig festlegt, sondern auch, dass f_E eine (eindeutige) elliptische Kurve definiert. Man kann folglich f_E als eine Repräsentation von E auffassen.*

2.3 Der Modularitätssatz

Wir kommen nun zu der zentralen Aussage, dem Modularitätssatz für elliptische Kurven. Um die Aussage zu verstehen benötigt man ein paar Grundkenntnisse aus der Funktionentheorie. Leser, welche noch keine Vorlesung aus diesem Gebiet gehört haben, oder deren Wissen nicht mehr ganz frisch ist, können die benötigten Definitionen im Anhang nachlesen.

Lemma 2.14. *Sei $N \in \mathbb{N}$,dann ist*

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\} \tag{31}$$

eine Untergruppe der $SL_2(\mathbb{Z})$

Beweis:

- $\Gamma_0(N) \subseteq SL_2(\mathbb{Z})$
- $\mathbb{1} \in \Gamma_0(N) \ \Rightarrow \ \Gamma_0(N) \neq \emptyset$

[3] im Wesentlichen nur eine Bedingung: ρ muss unverzweigt (siehe Definition 3.2) bei allen bis auf endlich vielen Primzahlen sein

- $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(N) \Rightarrow AB = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}$ nun gilt $c \equiv 0 \equiv \gamma \bmod N \Rightarrow AB \in \Gamma_0(N)$
- Die Inverse zu $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ ist gegeben durch $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
  Wegen $c \equiv 0 \bmod N$ gilt $-c \equiv 0 \bmod N$ und auch
  $\det(A^{-1}) = ad - bc = det(A) = 1 \Rightarrow A^{-1} \in \Gamma_0(N)$

□

Definition 2.15. *Modulform*
*Sei $k \in \mathbb{Z}$. Eine komplexwertige Abbildung f auf $\mathcal{H}$ heißt **Modulform** oder **modular** vom **Gewicht** k, falls f meromorph ist und*

1. $\forall z \in \mathcal{H} \; \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *gilt:*

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \tag{32}$$

2. *f eine Lagrangeentwicklung der Form*

$$f(z) = \sum_{n=0}^{\infty} a_n \mathrm{e}^{2\pi i n z} \tag{33}$$

besitzt

*f heißt **Spitzenform**, falls zusätzlich noch $a_0 = 0$ gilt*

Da $|SL_2(\mathbb{Z})| = \infty$ lässt sich mit dieser Definition nur schwer nachprüfen, ob eine gegebene Abbildung f eine Modulform ist oder nicht. Man kann jedoch die Definition so abändern, dass diese Probleme nicht auftreten.

Bemerkung 2.16. *Man kann die erste Bedingung ersetzen durch die Bedingungen*

$$f(z+1) = f(z) \tag{34}$$

und

$$f\left(-\frac{1}{z}\right) = z^k f(z) \tag{35}$$

Oftmals möchte man jedoch nicht die gesamte $SL_2(\mathbb{Z})$ betrachten, sondern sich auf $\Gamma_0(N)$ für ein $N \in \mathbb{N}$ einschränken. Dies liefert:

Definition 2.17. *(Modulformen der Stufe N)*
Ersetzt man in Definition 2.15 die Gruppe $SL_2(\mathbb{Z})$ durch $\Gamma_0(N)$, so nennt man eine komplexwertige Abbildung f auf $\mathcal{H}$, welche die dadurch modifizierten Bedingungen erfüllt, ***Modulform*** *oder* ***modular*** *vom* ***Gewicht*** *k und* ***Stufe*** *N. Analoges gilt auch für die Spitzenformen.*

Bemerkung 2.18. *(Modulformen und Spitzenformen)*

a) Die Menge

$$S(N) := \{\text{Spitzenformen vom Gewicht 2 und Stufe N}\}$$

ist ein endlich-dimensionaler Vektorraum

b) Falls $M|N$, dann gilt $\Gamma_0(N) \subseteq \Gamma_0(M)$, d.h. eine Modulform der Stufe M kann als Modulform der Stufe N aufgefasst werden, da die Anforderungen für Modulformen der Stufe M größer sind als die Anforderungen für Modulformen der Stufe N.
Es gilt sogar: Wenn $d|\frac{N}{M}$ und $f(\tau)$ Spitzenform vom Grad M, dann ist $f(d\tau)$ eine Spitzenform vom Grad N

Damit kommen wir nun endlich zu dem zentralen Satz dieses Vortrags, dem Modularitätssatz. Er wird hier nicht bewiesen, da der Beweis den Rahmen des Seminarvortrags sprengen würde.

Satz 2.19. ***Modularitätssatz***
Sei E eine elliptische Kurve über $\mathbb{Q}$. Dann gibt es eine Zahl $N \in \mathbb{Z}$, so dass für alle $\tau \in \mathcal{H}$ gilt:

1.

$$f_E\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 f_E(\tau) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \tag{36}$$

2.

$$f_E\left(-\frac{1}{N\tau}\right) = \pm N\tau^2 f_E(\tau) \tag{37}$$

□

In den 50er Jahren des letzten Jahrhunderts stellte Taniyama diese Vermutung auf. Eichler und Shimura zeigten die Umkehrung des Satzes und seit 1967 arbeitete Wiles an

dem Beweis. 1990 zeigte WILES, dass es unendlich viele Äquivalenzklassen (im Sinne der Äquvalenzrelation, welche im Vortag am 20.06.2011 [Hof] definiert wurde) gibt, welche die Bedingungen des Satz erfüllen. 1994 zeigten er und TAYLOR, dass der Satz für alle semistabilen Kurven gilt. Der Endgültige Beweis folgte 2001 von BREUIL, CONRAD, DIAMOND und TAYLOR.

Bemerkung 2.20. *Der Modularitätssatz sagt nicht anderes als: f_E ist modular vom Gewicht k und Stufe N.*

Es stellt sich jedoch die Frage, welcher Wert N bei elliptischen Kurven ist. Daher werfen wir auf diese Fragestellung einen kurzen Blick.

Definition 2.21. *Ist E eine elliptische Kurve, so heißt das kleinst mögliche N* ***Konduktor*** *von E.*

Der Konduktor ist wichtig, da wir uns für die folgende Betrachtung auf ihn beschränken können.

Ist E eine elliptische Kurve, so sind die Primzahlen, welche den Konduktor N teilen genau die Primzahlen mit schlechter Reduktion. Es gilt sogar

$$p|N \text{ und } p^2 \not| N \;\Leftrightarrow\; E \text{ hat multiplikative Reduktion mod } p \tag{38}$$

damit ergibt sich:

$$N = \prod_{p|\Delta} p \tag{39}$$

d.h. N ist das Produkt der Primzahlen, welche die Minimaldiskriminante Δ teilen.

Bemerkung 2.22. *Man kann zeigen: N quadratfrei $\Leftrightarrow$ E ist semistabil.*

3 Anwendung auf $\mathbf{E_{Frey}}$

Wir wenden nun die gesammelten Ergebnisse auf die Kurve E_{Frey} an, um so Fermats letzten Satz zu beweisen. Zunächst ein einfaches Korollar

Korollar 3.1. ***Modularität von*** E_{Frey}
Existiert die Kurve $y^2 = x(x - a^p)(x - b^p)$*, so ist sie modular.*

Beweis:
Existiert die Kurve, so ist sie nach Lemma 2.8 semistabil. WILES zeigte, dass alle semistabilen Kurven modular sind.

□

Im folgenden benötigen wir noch eine wichtige Aussage, den Satz von Ribet. Hierfür ist jedoch etwas mehr Theorie notwendig.

Da $\mathbb{Q} \subset \mathbb{Q}_p$ gilt:

$$G_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

ferner gibt es eine natürliche (kanonische) Abbildung η_p von G_p nach $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Sei im folgenden $I_p := \mathrm{Ker}(\eta_p)$, dann gilt:

$$G_p/I_p \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$$

Definition 3.2. *(Trägheitsuntergruppe, unverzweigte und endliche Repräsentationen)*
Seien $l, p \in \mathbb{P}$*. Der Kern* I_p *der Abbildung* η_p *heißt* ***Trägheitsuntergruppe*** *von* G_p*.*
Eine Repräsentation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_l)$ *nennen wir* ***unverzweigt*** *bei* p*, falls* $\rho(I_p) = 1$*, d.h.* $I_p \subseteq \mathrm{Ker}(\rho)$*. Gilt zudem noch* $p \neq l$ *und* ρ *ist unverzweigt, so nennt man* ρ ***endlich*** *bei* p*.*

Damit kommen wir zu einem wichtigen Satz, dem Satz von Ribet.

Satz 3.3. *(Satz von Ribet)*
Sei $p \in \mathbb{P}$ *mit* $p \geq 3$ *und sei* $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_p)$ *eine irreduzible Darstellung. Ferner sei* ρ *modular der Stufe* N *und existiert eine Primzahl* $q|N$ *mit* $q \neq p$*, bei der* ρ *nicht endlich ist. Gibt es eine Primzahl* s *mit* $s|N$ *und* ρ *endlich bei* s*, dann ist* ρ *modular der Stufe* $\frac{N}{p}$*.*□

Diese Aussage beweisen wir hier nicht, sie wird auch in [Wa] nicht bewiesen.

Bemerkung 3.4. *Die Aussage des Satzes bedeutet vereinfacht: wenn ρ von einer Modulform der Stufe N kommt, dann kommt ρ unter gewissen Annahmen auch von einer Modulform der Stufe $\frac{N}{p}$.*

Die nun folgende Aussage mag daher überraschen, sie liefert uns jedoch Fermats letzten Satz als Korollar.

Satz 3.5. *E_{Frey} kann für $p \in \mathbb{P}$ mit $p \geq 5$ nicht modular sein*

Beweis:
Angenommen E_{Frey} wäre modular, dann ist die zugehörige Galoisdarstellung ρ_p modular der Stufe N. Da E_{Frey} semistabil ist, folgt aus (39), dass $N = \prod_{p|abc} p$. Man kann zeigen, dass ρ_p für $p \geq 5$ irreduzibel ist. Setze nun $q = 2$ in Ribet's Satz, dann ist ρ_p nicht endlich bei 2, aber endlich bei allen anderen Primzahlen (siehe [Wa], section 13.2). Nach dem Satz von Ribet können wir daher alle ungeraden Primzahlen von N entfernen, d.h. ρ_p kann höchstens modular der Stufe $N = 2$ sein. Dies würde jedoch bedeuten, dass es eine Spitzenform von Gewicht 2 bzgl. $\Gamma_0(2)$ gibt, so dass ρ_p die zugehörige Galoisdarstellung ist. Es gibt jedoch keine Spitzenformen von Gewicht 2 bzgl. $\Gamma_0(2)$, welche nicht identisch gleich 0 sind. $\lightning$ Widerspruch

□

Somit erhalten wir:

Korollar 3.6. ***Fermats letzter Satz***
Für $n \in \mathbb{N}$ mit $n \geq 3$ existiert kein Tripel $(x, y, z) \in \mathbb{Z}^3$ mit $xyz \neq 0$ und $x^n + y^n = z^n$

Beweis:
In Lemma 1.7 haben wir gesehen, dass wir das Problem auf $n = 4$ und $p \in \mathbb{P}\backslash\{2\}$ zurückführen können. Für $n \in \{3, 4\}$ gibt es keine nicht-triviale Lösung (siehe Sätze 1.5 und 1.6) und im Falle $p \in \mathbb{P}$ mit $p \geq 5$ gibt es eine Lösung, falls die zugehörige Kurve E_{Frey} existiert. Aus Korollar 3.1 und Satz 3.5 folgt jedoch, dass die Kurve in diesem Fall nicht existieren kann. Folglich existiert für den Fall $p \in \mathbb{P}\backslash\{2\}$ keine nicht-triviale Lösung.

□

A etwas Funktionentheorie

Die folgenden Definitionen stammen größtenteils aus [Ga] und sind wichtig für die Definition von modularen Funktionen.

Definition A.1. *Es sei $D \subset \mathbb{C}$, $f : D \to \mathbb{C}$ eine Abbildung und $a \in \overline{D}$ ein Punkt im Abschluss von D, dann heißt eine Zahl $c \in \mathbb{C}$ Grenzwert von $f(z)$ für $z \to a$, wenn*

$$\forall \varepsilon > 0 \exists \delta > 0 \forall z \in D : |z - a| < \delta \Rightarrow |f(z) - c| < \varepsilon \tag{40}$$

gilt. Wie üblich schreibt man diese Bedingung auch als $\lim_{z \to a} f(z) = c$ und sagt, dass $f(z)$ mit $z \to a$ gegen c konvergiert.

Mit dieser Definition des Grenzwertes kann man sich die komplexe Differenzierbarkeit definieren:

Definition A.2. ***holomorphe Abbildungen***
Sei $D \subset \mathbb{C}$ offen, $f : D \to \mathbb{C}$ eine Abbildung und $a \in D$, dann heißt f ***komplex differenzierbar*** *in a, wenn der Grenzwert*

$$f'(a) := \lim_{\substack{z \in D \setminus \{a\} \\ z \to a}} \frac{f(z) - f(a)}{z - a} \tag{41}$$

existiert. Diese Zahl heißt dann auch die ***Ableitung*** *von f in a. Ist f in jedem Punkt von D komplex differenzierbar, so heißt f auf D* ***holomorph****.*

Definition A.3. ***diskrete Mengen***
Sei $M \subset \mathbb{C}$, dann heißt M diskret, falls gilt

$$\forall c \in \mathbb{C} \; \exists U \subset \mathbb{C}, \; U \text{ Umgebung von } c : |M \cap U| < \infty \tag{42}$$

Definition A.4. ***meromorphe Abbildungen***
Sei $D \subset \mathbb{C}$, $f : D \to \mathbb{C}$ eine Abbildung und $P_f \subset D$ eine diskrete Teilmenge. Dann heißt f ***meromorph****, falls f auf $D \setminus P_f$ holomorph ist und in den Punkten von P_f Polstellen besitzt.*

B p-adische Zahlen

Dieses Kapitel dient der kurzen Definition und Einführung der p-adischen Zahlen, welche im Abschnitt über Glaoisdarstellungen erwähnt wurden. Es stellt einen winzigen Bruchteil der Theorie zu diesen, für einige mathematische Gebiete wichtigen Zahlen, dar und lehnt sich stark an [Ot] an.

Zur Motivation der p-adischen Zahlen, betrachten wir das folgende Beispiel.

Beispiel B.1. *Die Zahl $n = 137$ lässt sich schreiben als:*

$$137 = 2 \cdot 3^0 + 0 \cdot 3^1 + 0 \cdot 3^2 + 2 \cdot 3^3 + 1 \cdot 3^4 \tag{43}$$

oder etwas formaler:

$$137 = \sum_{n=0}^{\infty} a_i 3^i \tag{44}$$

wobei

$$a_i = \begin{cases} 0 & i \in \{1,2\} \cup \{n \in \mathbb{N} \mid n \geq 5\} \\ 1 & i = 4 \\ 2 & i \in \{0,3\} \end{cases}$$

Diese Ergebnis lässt sich verallgemeinern. Man erhält

Proposition B.2. *Sei $p \in \mathbb{P}$ beliebig, dann gilt für alle $n \in \mathbb{N}$:*

$$n = \sum_{i=0}^{\infty} a_i p^i \tag{45}$$

mit $a_i \in \{0, 1, 2, \ldots, p-1\}$

Beweis: Den Beweis findet man in [Ot] S.19 □

Definition B.3. *Sei $p \in \mathbb{P}$, dann heißt*

a) $\sum_{i=0}^{\infty} a_i p^i$ *mit* $a_i \in \{0, 1, 2, \ldots, p-1\}$ ***ganze p-adische Zahl***

b) $\sum_{i=-k}^{\infty} a_i p^i$ *mit* $a_i \in \{0, 1, 2, \ldots, p-1\}$ ***p-adische Zahl***

c) $\mathbb{Z}_p := \left\{ \sum_{i=0}^{\infty} a_i p^i \;\middle|\; a_i \in \{0,1,2,\ldots,p-1\} \right\}$ *die Menge der ganzen p-adischen Zahlen*

d) $\mathbb{Q}_p := \left\{ \sum_{i=-k}^{\infty} a_i p^i \;\middle|\; a_i \in \{0,1,2,\ldots,p-1\} \right\}$ *die Menge der p-adischen Zahlen*

Bemerkung B.4. *(Basis und alternative Darstellung)*

a) Die Primzahl p bezeichnet man manchmal auch als Basis.

b) Ist offensichtlich, welche Primzahl p als Basis gewählt wurde, so repräsentiert man die p-adische Zahl $\sum_{i=-k}^{\infty} a_i p^i$ *durch die Folge* $a_{-k}a_{-k+1}\ldots a_{-1}a_0a_1\ldots$

Veranschaulichen wir uns das alles einmal an einem Beispiel.

Beispiel B.5. *(binäre Zahlen)*
Wählen wir $p = 2$*, so erhalten wir die 2-adischen Zahlen, welche wir auch als binäre Zahlen kennen und in der Informatik eine besondere Rolle spielen. Bei der Notation in Form der Folge der* a_i *muss man jedoch beachten, dass die Aufschreibrichtung umgekehrt ist. Betrachten wir als Beispiel die folgenden Zahlen:*

n	*2-adische Entwicklung*	*2-adisch als Folge*	*binär*
18	$0\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2 + 0\cdot 2^3 + 1\cdot 2^4$	*01001*	*10010*
26	$0\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2 + 1\cdot 2^3 + 1\cdot 2^4$	*01011*	*11010*
44	$0\cdot 2^0 + 0\cdot 2^1 + 1\cdot 2^2 + 1\cdot 2^3 + 0\cdot 2^4 + 1\cdot 2^5$	*001101*	*101100*

Auf den p-adsichen Zahlen lässt sich auch ein Betrag definieren. Dazu schreiben wir jede rationale Zahl[4] wie folgt: $x = p^r \frac{a}{b}$ wobei $p \nmid ab$

Definition B.6. *(p-adischer Betrag)*
Für x definieren wir den ***p-adischen Betrag*** *als*

$$|x|_p := \frac{1}{p^r} \tag{46}$$

und setzen $|0|_p := 0$

Es ist nicht sichergestellt, dass die Darstellung der p-adsichen Zahlen aus Definition B.3 in $\mathbb{R}$ konvergiert, jedoch gilt mit dem p-adischen Betrag

$$\lim_{i\to\infty} |a_i p^i|_p \to 0 \tag{47}$$

[4] Wir werden gleich noch sehen, dass $\mathbb{Q} \subset \mathbb{Q}_p$ gilt.

so dass die Definition der p-adischen Zahlen Sinn macht.

Das schöne an den p-adischen Zahlen sind ihre Eigenschaften, so unter anderem die folgende Proposition:

Proposition B.7. *Es gilt für alle $p \in \mathbb{P}$:*

a) $\mathbb{Z}_p$ ist ein Integritätsbereich

b) $\mathbb{Q}_p$ ist ein Körper

Beweis:
Der Beweis von a) ist analog zu dem für formale Potenzreihen aus AGS.
Für b) geben wir hier nur die Verknüpfungen an. Es ist

$$+ : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p \ : \ \sum_{i=-n}^{\infty} a_i p^i + \sum_{i=-m}^{\infty} b_i p^i := \sum_{i=\min\{-n,-m\}}^{\infty} (a_i + b_i) p^i \tag{48}$$

$$\cdot : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p \ : \ \left(\sum_{i=-n}^{\infty} a_i p^i \right) \cdot \left(\sum_{i=-m}^{\infty} b_i p^i \right) := \sum_{i=-n-m}^{\infty} \sum_{k=-n}^{i+m} (a_k \cdot b_{i-k}) p^i \tag{49}$$

Der Rest des Beweises ist langwieriges nachrechnen, welches wir hier an dieser Stelle nichtausführen. Die Details des gesamten Beweises von a) und b) kann man in [Ot] auf S. 19 ff. nachlesen.

□

Bemerkung B.8. *(Rechnen mit p-adischen Zahlen und Charakteristik von $\mathbb{Q}_p$)*

a) Bei der Rechnung von $+$ und $\cdot$ muss man vorsichtig sein. Man kann zwar wie man es in $\mathbb{R}$ kennt rechnen, es kann jedoch zu Überträgen kommen, welche dann nach rechts und nicht wie gewohnt nach links erfolgen. Dies wurde in der Darstellung von $+$ und $\cdot$ im Beweis nicht deutlich, ist aber anschaulich klar, da für $a_i + b_i = p + x$ mit $0 \leq x < p$ natürlich $(a_i + b_i)p^i = (p + x)p^i = p^{i+1} + xp^i$ gilt. Analoges gilt für $a_i \cdot b_{i-k}$.

b) Die Darstellung negativer Zahlen ist nicht offensichtlich, aber sehr einfach. Sei $z \in \mathbb{Z}_{>0}$, dann ist $-z = (-1) \cdot z$ und

$$-1 = \frac{p-1}{1-p} = \frac{p}{1-p} - \frac{1}{1-p} = p \cdot \sum_{i=0}^{\infty} p^i - \sum_{i=0}^{\infty} p^i \tag{50}$$

Insbesondere gilt $\mathbb{Z} \subset \mathbb{Z}_p$

c) Auch die rationalen Zahlen lassen sich p-adisch darstellen. Da man für jede ganze Zahl nur die a_i mit $i \geq 0$ benötigt liefern die a_i mit $-k \leq i < 0$ die Nachkommastellen der Darstellung als Dezimalbruch. Hierbei ist ebenfalls wieder a) zu beachten.

d) Nach c) gilt $\mathbb{Q} \subset \mathbb{Q}_p$, d.h. $\mathbb{Q}_p$ ist ein Erweiterungskörper von $\mathbb{Q}$. Insbesondere gilt also $\mathrm{char}(\mathbb{Q}_p) = 0$

Die p-adischen Zahlen lassen sich auch auf $n \in \mathbb{N}$ verallgemeinern, man verliert dadurch jedoch einige gute Eigenschaften:

Bemerkung B.9. *(Verallgemeinerung der p-adischen Zahlen)*
Die Definition der p-adischen Zahlen lässt sich direkt auf Primzahlpotenzen erweitern. Die Erweiterung auf $n \in \mathbb{N}$ erfolgt dann, wie man es von zahlentheoritsch-multiplikativen Funktionen kennt:
Sei $n \in \mathbb{N}$ und $n = \prod_i p_i^{\alpha_i(n)}$ die zugehörige PFZ, dann gilt:

$$\mathbb{Q}_n = \bigotimes_i \mathbb{Q}_{p_i^{\alpha_i(n)}} \tag{51}$$

beispielsweise gilt:

$$\mathbb{Q}_{10} = \mathbb{Q}_2 \times \mathbb{Q}_5$$

aber $\mathbb{Q}_{10}$ ist kein Körper, ja sogar kein Integritätsbereich mehr, denn multipliziert man in $\mathbb{Q}_{10}$ die Eins aus $\mathbb{Q}_2$ mit der Eins aus $\mathbb{Q}_5$, so erhält man:

$$(1,0) \cdot (0,1) = (0,0) \tag{52}$$

Literatur

[Ba] M. Barakat: “Cryptography“, Lecture notes, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~barakat/Lehre/WS10/Cryptography/lecture_notes/Cryptography.pdf

[Coa] J. Coates (Hrsg.): „Elliptic curves, modular form & Fermats last theorem“, International Press 1997

[Cor] G. Cornell (Hrsg.): „Modular forms and Fermat’s last theorem“, Springer 1998

[Eie] M. Eie: „Topics in number theory“, World Scientific, 2009

[Fr] G. Frey: „Galois Representations Attached to Elliptic Curves and Diophantine Problems “
http://www.iem.uni-due.de/zahlentheorie/preprints/turku.ps

[Ga] A. Gathmann: “Einführung in die Funktionentheorie“, Vorlesungsskript, TU Kaiserslautern, 2008/2009 2011
http://www.mathematik.uni-kl.de/~gathmann/class/futheo-2008/main.pdf

[Her] N. Herzog: „Elliptische Kurven und Fermats letzter Satz“, Maturaarbeit im Fach Mathematik, Kantonsschule Frauenfeld, 2007
http://nicolash.cwsurf.de/schule/matura/matura.pdf

[Hof] S. Hofmann: „Die j-Invariante und Endomorphismen einer elliptischen Kurve“, Ausarbeitung zum Vortrag im Rahmen des Seminars „Kryptographie“, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~barakat/Lehre/SS11/KryptoSeminar/Vortraege/Stephan%20Hofmann:%20Die%20j-Invariante%20und%20Endomorphismen%20einer%20elliptischen%20Kurve.pdf

[Kle] B. Klein „Torsinospunkte und Divisionspolynome“, Ausarbeitung zum Vortrag im Rahmen des Seminars „Kryptographie“, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~barakat/Lehre/SS11/KryptoSeminar/Vortraege/Benjamin%20Klein:Torsionspunkte%20und%20Divisionspolynome.pdf

[Ma] T. Markwig: “Elementare Zahlentheorie“, Vorlesungsskript, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~keilen/download/LectureNotes/zahlentheorie.pdf

[Ot] D. Otten: „Die p-adischen Zahlen“, Seminararbeit, Universität Bielefeld, 2006
http://www.math.uni-bielefeld.de/~dotten/files/sonstiges/Diep-adischenZahlen.pdf

[St] W. Stein: “Computing With Modular Forms“, 2005
http://www.wstein.org/edu/fall05/168/notes/modular_forms_book/current.pdf

[Wa] L. Washington: “Elliptic curves: number theory and cryptography“, Chapman & Hall/CRC, 2008

[Wi] A. Wiles: „Modular elliptic curves an Fermat’s Last Theorem“, Annals of Mathematics, 142 (1995), 443-551
http://math.stanford.edu/~lekheng/flt/wiles.pdf