Universität des Saarlandes,
Saarbrücken

p-adische Betrachtung von Bernoulli Zahlen

Diplomarbeit

vorgelegt von
Kathrin Engstler

angefertigt
an der Mathematischen Fakultät
der Universität des Saarlandes
2005

Ich erkläre hiermit an Eides statt, diese Arbeit selbständig geschrieben und keine weiteren Hilfsmittel ausser den angegebenen verwendet zu haben.

Danksagung

Herrn Prof. Dr. Ernst-Ulrich Gekeler gilt mein besonderer Dank für das interessante Thema und die sehr intensive und wertvolle Betreuung.
Ich möchte mich auch bei Frau Dr. Alice Keller danken, die mir jederzeit für Fragen zur Verfügung stand.
Herrn Johannes Lengler danke ich für sein offenes Ohr und für das Korrektur Lesen dieser Arbeit.
Des weiteren danke ich Herrn Bernd Christian Kellner für das Zusenden seiner Ergebnisse und Arbeiten.
Ansonsten bedanke ich mich bei allen, die mich beim Erstellen dieser Arbeit unterstützt haben.

Inhaltsverzeichnis

Vorwort

Diese Diplomarbeit richtet sich hauptsächlich an Mathematiker und Mathematikstudenten, die sich mit Bernoulli Zahlen oder auch Eisensteinreihen beschäftigen wollen. Gerade das letzte Kapitel kann für Mathematiker interessant sein, da dort auch neue Kongruenzen aufgestellt werden. Die vorliegende Diplomarbeit beruht hauptsächlich auf einer Arbeit von Herrn Prof. Dr. Gekeler, die er 2002 verfasste (siehe [Gek]). In dieser Arbeit stellte er Kongruenzvermutungen für Bernoulli Zahlen auf.
Das Ziel meiner Arbeit ist es diese Kongruenzen zu überprüfen. Um dies effizient durchführen zu können, wurden die *p*-adischen Zahlen herangezogen.
In der *p*-adischen Darstellung von Bernoulli Zahlen können direkt Kongruenzen für mehrere Primzahlpotenzen abgelesen werden. Aus diesem Grund beschäftigt sich das erste Kapitel mit den *p*-adischen Zahlen. Dabei ist es so aufgebaut, dass auch ein Mathematikstudent, der sich noch nicht mit diesem Thema beschäftigt hat, danach so viel über die *p*-adischen Zahlen wissen müsste, um das Folgende gut nachvollziehen zu verstehen.
Das zweite Kapitel betrachtet die Bernoulli Zahlen genauer. Der Sinn dieses Kapitels ist es, ein Überblick über die bereits bekannten Eigenschaften dieser Zahlen zu liefern. Es sollte Neulingen auf dem Gebiet der Bernoulli Zahlen auch ein Gefühl für diese besonderen Zahlen vermitteln.
Kapitel 3 ist etwas anspruchsvoller, wenn auch komprimierter. In diesem Kapitel gibt es viele Bemerkungen und weniger bewiesene Sätze. Ein Beweis jeder Bemerkung würde den Rahmen sprengen und nichts zum Verständnis beitragen. Kapitel 3 steuert nur auf den letzten und entscheidenden Satz dieses Kapitels zu. Ohne diesen Satz hätte es diese Diplomarbeit so wahrscheinlich nie gegeben. Dieser Satz 3.5.2 liefert ein Beweisschema, dass auf die Kongruenzen in Kapitel 5 anwendbar ist. Das Beweisschema wird in Kapitel 4 näher betrachtet und mit Beispielen verdeutlicht.
Dieses vorletzte Kapitel hat allerdings nicht nur den Zweck, dass Beweisprinzip zu erläutern, sondern dem Leser auch die Probleme die im Laufe meiner Arbeit auftraten auf zu zeigen. Diese Probleme haben ausschließlich mit dem Weiterverarbeiten der berechneten Bernoulli Zahlen und dem Implementieren der benötigten Programme zu tun. Denn diese beiden Punkte und das Berechnen möglichst großer und möglichst vieler Bernoulli Zahlen haben auch die meiste Zeit vereinnahmt. Dabei war es besonders ärgerlich, dass es mir, aus den in Kapitel 4 dargelegten Gründen, nicht möglich war, die 60.000 mit Calcbin[1] berechneten Bernoulli Zahlen weiter zu verarbeiten.
In Kapitel 5 werden nun die von Herrn Prof. Dr. Gekeler aufgestellten Kongruenzen vorgestellt. Leider konnte ich diese Kongruenzen nicht allgemein beweisen, sondern lediglich im Rahmen von 20.000 Bernoulli Zahlen. Bei meinen Untersuchungen bin ich auch noch auf einige neue Kongruenzen gestossen, die ebenfalls in diesem letzten Kapitel vorgestellt werden. Auch diese Kongruenzen konnten lediglich für die ersten 20.000 Bernoulli Zahlen beweisen werden.

[1] Siehe hierzu [Kel3].

Die Geschichte der Bernoulli Zahlen

Die Bernoulli Zahlen wurden von Abraham de Moivre nach ihrem Entdecker Jakob Bernoulli benannt.
Jakob Bernoulli stammt aus einer Gelehrtenfamilie, er studierte Philosophie, Theologie und gegen den Willen seines Vaters auch Mathematik und Astronomie. Er wurde 1654 in Basel geboren, hielt ab 1683 mathematische Vorlesungen in Basel, verfasste von 1689 bis 1704 fünf Abhandlungen über die Reihenlehre, gab die „Geometrica“ von Rene Descartes neu heraus und schrieb zahlreiche Beiträge für die „Acta Eroditorum“ (die erste wissenschaftliche Zeitung Deutschlands). Erst nach seinem Tod 1705 wurde 1713 sein Werk „Ars Conjectandi“ veröffentlicht, in diesem Werk tauchten die Bernoulli Zahlen zum ersten Mal auf.
Jakob Bernoulli berechnete Potenzsummen mit Hilfe der Bernoulli Zahlen und ist Mitbegründer der Wahrscheinlichkeitslehre.

Seit dieser Zeit spielen die Bernoulli Zahlen in fast jedem Gebiet der Mathematik eine wichtige Rolle. In der Iwasawa Theorie werden sie bei den Eisensteinreihen benötigt, auch bei der Betrachtung der Riemannschen Zetafunktion und Fermat´s letztem Theorem können Bernoulli Zahlen hilfreich sein. Weitere Anwendungen findet man in der Kombinatorik und bei den diophantischen Gleichung, der Potenzreihen Berechnung und zahlreichen weiteren Gebieten der Zahlentheorie.
Inzwischen gibt es für die Bernoulli Zahlen etliche Definitionen, schon bewiesene Kongruenzen und auch Vermutungen.

1. Die p-adischen Zahlen

Es gibt mehrere Möglichkeiten eine Zahl auszudrücken: als reelle Zahl, als rationale Zahl... Eine weitere Möglichkeit besteht in der Darstellung als *p*-adische Zahl. Hierfür sei im Folgenden *p* eine beliebige aber feste Primzahl. Siehe auch [Kob] und [Mur].

1.1 Definition

Eine ganze *p*-adische Zahl ist eine formale unendliche Potenzreihe der Form

$$a_0 + a_1 p + a_2 p^2 + \ldots$$

mit $0 \le a_i < p$ für $i = 0,1,2,\ldots.$

1.2 Bemerkung

Mit $\mathbf{à}_p$ bezeichnet man die Gesamtheit der *p*-adischen Zahlen.

Will man nun die Restklasse einer großen Zahl modulo mehrerer Potenz einer festen Primzahl berechnen, kann es sehr hilfreich sein, diese Zahl als *p*-adische Zahl auszudrücken. Denn wie folgender Satz zeigt, kann man an Hand dieser Darstellung die Restklasse direkt ablesen.

1.3 Satz

Sei *a* durch die *p*-adische Zahl

$$a = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \ldots. \in \mathbf{à}_p$$

mit $0 \le a_i < p$ für $i = 0,\ldots,$ gegeben. Dann erhält man die Restklasse $a \bmod p^n \in \mathbf{à} / p^n\mathbf{à}$ durch

$$a \equiv a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1} \mod p^n,$$

wobei $0 \le a_i < p$ für $i = 0,1,\ldots,n-1.$

Beweis mittels vollständiger Induktion über *n* (siehe [Neu])

Induktionsanfang:	die Behauptung ist klar für *n=1*.
Induktionsbehauptung:	die Behauptung sei für *n-1* bewiesen.
Induktionsschritt:	mit der Induktionsbehauptung , gibt es eine eindeutige Darstellung

$$a = a_0 + a_1 p + a_2 p^2 + ... + a_{n-2} p^{n-2} + g p^{n-1}$$

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

t

1.4 Definition

Jede rationale Zahl $f = \frac{b}{d}$, mit $p \nmid d$, definiert eine Folge von Restklassen

$$\overline{s_n} = f \bmod p^n,$$

mit $n = 1, 2, ...$ Für diese gilt nach Satz 1.3

$$\begin{aligned}
&\overline{s_1} = a_0 \bmod p, \\
&\overline{s_2} = a_0 + a_1 p \bmod p^2, \\
&\overline{s_3} = a_0 + a_1 p + a_2 p^2 \bmod p^3, \\
&. \\
&. \\
&.
\end{aligned}$$

mit eindeutig bestimmten und gleichbleibenden Koeffizienten $a_i \in \{0, 1, 2, ..., p-1\}$, wobei $i = 0, 1, 2, ...$ Die Zahlenfolge

$$s_n = a_0 + a_1 p + a_2 p^2 + ... + a_{n-1} p^{n-1},$$

mit $n = 1, 2, ...$ definiert eine *p*-adische Zahl $\sum_{k=0}^{\infty} a_k p^k \in$ **à**$_p$.
Dies wird die *p*-adische Entwicklung von *f* genannt.

Definition

Der Bereich der ganzen *p*-adischen Zahlen kann durch die formalen Reihen

$$\sum_{k=-m}^{\infty} a_k p^k = a_{-m} p^{-m} + ... + a_{-1} p^{-1} + a_0 + a_1 p + ...,$$

wobei $m \in \mathbb{Z}$ und $0 \le a_k < p$ ist, erweitert werden. Die Gesamtheit dieser Reihen wird mit $\mathbb{Q}_p$ bezeichnet. Ist $f = \frac{g}{h} p^{-m} \in \mathbb{Q}$ mit $g, h \in \mathbb{Z}$ und $(gh, p) = 1$, und ist $a_0 + a_1 p + a_2 p^2 + \ldots$ die *p*-adische Entwicklung von $\frac{g}{h}$. So wird *f* die *p*-adische Zahl

$$a_0 p^{-m} + a_1 p^{-m+1} + \ldots + a_m + a_{m+1} p + \ldots \in \mathbb{Q}_p$$

zugeordnet.

Die Addition und Subtraktion von *p*-adischen Zahlen geschieht ähnlich wie bei den Dezimalzahlen, nur dass man anstatt von rechts nach links genau umgekehrt vorgeht.
Dazu hier nun eine Beispiel:

Addition in $\mathbb{Q}_5$:

$$\begin{array}{rl} & (3 + 4 \cdot 5 + 2 \cdot 5^2 + \ldots) \\ + & (1 + 3 \cdot 5 + 1 \cdot 5^2 + \ldots) \\ \hline & 4 + 2 \cdot 5 + 4 \cdot 5^2 + \ldots \end{array}$$

Auch eine *p*-adische Norm kann definiert werden:

1.6 Definition

Sei *a* eine ganze Zahl, dann bezeichne $ord_p a$ die höchste Potenz von *p* die *a* teilt (d.h. das grösste *n*, so dass $a \equiv 0 \pmod{p^n}$). Es gilt $ord_p 0 = \infty$.

Rechenregeln

Für $a = a_1 a_2$ gilt $ord_p a = ord_p a_1 + ord_p a_2$, und für $b = \frac{c}{d}$ sei $ord_p b = ord_p c - ord_p d$.

Beweis

Dies ist klar nach Definition.

t

Definition

Es sei

$$|x|_p = \begin{cases} p^{-ord_p x}, & x \neq 0 \\ 0 \quad , & x = 0 \end{cases}.$$

Für $x = p^n \left(\frac{a}{b} \right)$ gilt also $|x|_p = p^{-n}$.

1.9 Proposition

Durch $|x|_p$ wird eine Norm definiert.

Beweis

Zu zeigen ist: 1.) Es gilt $|x|_p = 0$ genau dann wenn $x = 0$.
2.) Es gilt $|xy|_p = |x|_p |y|_p$.
3.) Es gilt $|x+y|_p \leq |x|_p + |y|_p$.

Zu 1: Dies ist mit der Definition von $|x|_p$ direkt ersichtlich.

Zu 2: Hierzu muss eine Fallunterscheidung betrachtet werden.

Fall 1: Sei $x = 0$ oder $y = 0$ (also auch $|x|_p = 0$ oder $|y|_p = 0$).
In diesem Fall gilt $xy = 0$, also per Definition $|xy|_p = 0$.

Fall 2: Sei $x = \frac{a}{b}$ und $y = \frac{c}{d}$, also $ord_p(x) = ord_p(a) - ord_p(b)$ und $ord_p(y) = ord_p(c) - ord_p(d)$.
In diesem Fall ist $xy = \frac{ac}{bd}$, also

$$ord_p(xy) = ord_p(ac) - ord_p(bd) = ord_p a + ord_p c - ord_p b - ord_p d.$$

Somit ist die Aussage klar.

Zu 3: Auch hierzu wird eine Fallunterscheidung benötigt:

Fall 1: Sei $x = 0$ oder $y = 0$ oder $x + y = 0$ (also auch $|x|_p = 0$ oder $|y|_p = 0$ oder $|x+y|_p = 0$).
Dann ist dies klar nach Definition.

Fall 2: Sei nun $x = \frac{a}{b}$ und $y = \frac{c}{d}$, also $ord_p(x) = ord_p(a) - ord_p(b)$ und $ord_p(y) = ord_p(c) - ord_p(d)$.

Es gilt $x + y = \frac{ad + bc}{bd}$, somit ist

$$ord_p(x+y) = ord_p(ad+bc) - ord_p(b) - ord_p(d).$$

Es gilt

$$\begin{aligned} ord_p(x+y) &\geq \min(ord_p ad, ord_p bc) - ord_p(b) - ord_p(d) \\ &= \min(ord_p a + ord_p d, ord_p b + ord_p c) - ord_p b - ord_p d \\ &= \min(ord_p a - ord_p b, ord_p c - ord_p d) \\ &= \min(ord_p x, ord_p y). \end{aligned}$$

Also $|x+y|_p = p^{-ord_p(x+y)} \leq \max\left(p^{-ord_p x - ord_p y}\right) = \max\left(|x|_p, |y|_p\right) \leq |x|_p + |y|_p$.

t

Im letzten Beweis wurde in 3.) eine weit strengere Ungleichung bewiesen, als eigentlich für die Definition einer Norm nötig gewesen wäre. Dies führt zu:

1.10 Satz und Definition

Für die *p*-adische Norm gilt

$$|x+y|_p \leq \max\left(|x|_p, |y|_p\right).$$

Eine Norm die obige Ungleichung erfüllt, wird nichtarchimedisch genannt.

Beweis

Siehe hierzu Teil 3 des Beweises zu 1.9.

t

Man kann $\hat{\mathbf{a}}_p$ auch anders einführen als es in 1.2 geschah:

1.11 Bemerkung

Es gilt $\hat{\mathbf{a}}_p = \left\{a \in \hat{\mathbf{a}}_p \mid |a|_p \leq 1\right\}$.

1.12 Bemerkung

Für $a,b \in \hat{\mathbf{a}}_p$ gilt die Kongruenz $a \equiv b (\mathrm{mod}\, p^n)$ genau dann wenn $|a-b|_p \leq p^n$ oder äquivalent $\frac{(a-b)}{p^n} \in \mathbf{à}_p$.

1.13 Definitionen

Man definiert $\mathbf{à}_p^* = \left\{ a \mid \frac{1}{a} \in \mathbf{à}_p \right\}$.

Weiter wird eine *p*-adische Zahl, deren erste Ziffer ungleich *0* ist, mit *p*-adischer Einheit bezeichnet.

2. Bernoulli Zahlen

Da es verschiedenen Möglichkeiten bei der Einführung der Bernoulli Zahlen gibt, die eventuell zu verschiedenen Vorzeichen führt, hier nun die in dieser Arbeit verwendetet Definition:

2.1 Definition

Die Bernoulli Zahlen, in Zeichen B_n mit $n \in$ **ã**, werden durch die Potenzreihe

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} z^k, \quad |z| < 2\pi$$

definiert.

2.2 Satz

Da $\frac{z}{e^z - 1} + \frac{z}{2}$ eine gerade Funktion ist und $B_1 = -\frac{1}{2}$ lässt sich die Formel aus Definition 1.1 folgendermaßen umformen:

$$\frac{z}{e^z - 1} + \frac{z}{2} = \sum_{k=0}^{\infty} \frac{B_{2k}}{(2k)!} z^{2k}.$$

Beweis

Da $\frac{t}{e^t - 1} + \frac{t}{2}$ das selbe ist wie $\frac{t}{2}\left(\frac{e^t + 1}{e^t - 1}\right)$ und da man nun hier t durch $-t$ ersetzen kann, bleibt der Wert in beiden Formeln gleich.

t

Mit dieser Definition haben die Bernoulli Zahlen mit geradem Index wechselnde Vorzeichen und sind für ungerade $n>1$ identisch Null. Siehe hierzu Satz 2.12.

2.3 Theorem

Für jede ganze Zahl $n \geq 2$ gilt

$$\sum_{k=1}^{n-1} \binom{2n}{2k} B_{2k} B_{2n-2k} = -(2n+1) B_{2n}.$$

Beweis

Diese Rekursionsformel folgt direkt aus der Definition der Bernoulli Zahlen, es gilt nämlich

$$\left(\frac{x}{e^x-1}\right)^2=(1-x)\frac{x}{e^x-1}-x\left(\frac{x}{e^x-1}\right)'.$$

Dann folgt die Formel indem man beide Seiten von

$$\coth^2 x=1-(\coth x)'$$

vergleicht.

t

2.4 Lemma

Es gilt

$$(m+1)B_m=-\sum_{k=0}^{m-1}\binom{m+1}{k}B_k.$$

Beweis (vgl. [Ir.&Ro.], S. 229f)

Laut Definition gilt $\frac{z}{e^z-1}=\sum_{k=0}^{\infty}\frac{B_k}{k!}z^k,\quad |z|<2\pi$. Multipliziert man nun beide Seiten mit e^z-1, so erhält man $z=\sum_{n=1}^{\infty}\frac{z^n}{n!}\sum_{m=0}^{\infty}B_m\frac{z^m}{m!}$. Setzt man weiter beide Exponenten auf $m+1$, so erhält man für $m=0$, dass $B_0=1$ sein muß und dass sonst $\sum_{k=0}^{m}\binom{m+1}{k}B_k=0$ gelten muss. Also folgt, dass $(m+1)B_m=-\sum_{k=0}^{m-1}\binom{m+1}{k}B_k$ sein muss.

t

2.5 Definition

Analog zur Definition 2.1 werden mit $|z|<2\pi$ die Bernoulli Polynome, in Zeichen $B_k(x)$, definiert durch

$$\frac{ze^{zx}}{e^z-1}=\sum_{k=0}^{\infty}B_k(x)\frac{z^k}{k!}.$$

2.6 Bemerkung

Wie man durch leichtes Nachrechnen direkt sieht, gilt:

$$B_n(0) = B_n,$$
$$\frac{d}{dx} B_n(x) = nB_{n-1}(x).$$

2.7 Theorem

Es gibt auch einen Zusammenhang der Bernoulli Zahlen mit der Summationsformel $S_n(m) = \sum_{k=0}^{m-1} k^n$:

$$(m+1)S_n(m) = \sum_{k=0}^{n} \binom{n+1}{k} B_k m^{n+1-k}.$$

Beweis (siehe [Ir.&Ro.])

Setzt man $k = 0,1,2,...,m-1$ in $e^{kt} = \sum_{m=0}^{\infty} k^m \left(\frac{t^m}{m!} \right)$ und addiert dies dann auf, so erhält man

$$1 + e^t + e^{2t} + ... + e^{(n-1)t} = \sum_{m=0}^{\infty} S_m(n) \frac{t^m}{m!}.$$

Für die linke Seite gilt

$$\frac{e^{nt}-1}{e^t-1} = \frac{e^{nt}-1}{t} \frac{t}{e^t-1} = \sum_{k=1}^{\infty} n^k \frac{t^{k-1}}{k!} \sum_{j=0}^{\infty} B_j \frac{t^j}{j!}.$$

Koeffizientenvergleich und Multiplikation mit $(m+1)!$ liefert das gesuchte Ergebnis.

t

2.8 Bemerkung

Aus Theorem 2.7 folgt für $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$, dass

$$S_m(n) = \frac{1}{m+1} \left(B_{m+1}(n) - B_{m+1} \right)$$

[vergleiche [Ir.&Ro.], S.230].

2.9 Satz

Für $n \in \mathbb{N}$, mit $\left\langle {n \atop k} \right\rangle := \sum_{\nu=1}^{k} \binom{k}{\nu} (-1)^{k-\nu} \nu^n$ und $S_n(x) = \sum_{k=1}^{n} \left\langle {n \atop k} \right\rangle \binom{x}{k+1}$ [siehe hierzu [Kel 1]. S.23] gilt

i) $\left\langle {n \atop k-1} \right\rangle \equiv \begin{cases} -1, & k = p, p-1 \mid n \\ 0, & sonst \end{cases} \pmod{k}$,

ii) $B_n = \sum_{k=1}^{n} \left\langle {n \atop k} \right\rangle \frac{(-1)^k}{k+1}$.

Beweis (vgl. auch [Kel 2.])

Zu i):

Die Fälle $k = 1, 2$ sind klar. Da $(k-1)! \equiv \begin{cases} -1, & k = p \\ 2, & k = p \\ 0, & sonst \end{cases} \pmod{k}$ und $(k-1)! \mid \left\langle {n \atop k-1} \right\rangle$ bleiben nur noch die Fälle $k = 4$ und $k = p > 2$ zu überprüfen. Sei nun $n \geq 2$ eine gerade Zahl.
Im Fall $k = 4$ gilt:

$$\left\langle {n \atop 3} \right\rangle = \binom{3}{1} 1^n - \binom{3}{2} 2^n + \binom{3}{3} 3^n = 3 - 3 \cdot 2^n + 3^n \equiv -1 + (-1)^n \equiv 0 \pmod{4}.$$

Nun zum Fall $k = p > 2$:
Es gilt

$$\left\langle {n \atop p-1} \right\rangle \equiv \sum_{l=1}^{p-1} \binom{p-1}{l} (-1)^l l^n \equiv \sum_{l=1}^{p-1} l^n \equiv S_n(p) \equiv \begin{cases} -1, & p-1 \mid n \\ 0, & sonst \end{cases} \pmod{p}.$$

Siehe hierzu [Ir&Ro], Lemma 2, Seite 235].

Zu ii):

Betrachte hierzu $\frac{S_n(x)}{x}$ an der Stelle 0. Da $\binom{x}{k+1} = \frac{x}{k+1} \binom{x-1}{k}$, folgt

$$\frac{S_n(x)}{x} = \sum_{k=1}^{n} \left\langle {n \atop k} \right\rangle \frac{1}{k+1} \binom{x-1}{k}.$$

Da $S_n(0) = 0$ und $\binom{-1}{k} = (-1)^k$ ist, folgt

$$\lim_{x\to 0}\frac{S_n(x)}{x}=\sum_{k=1}^{n}\left\langle {n \atop k}\right\rangle\frac{(-1)^k}{k+1}.$$

Mit 2.8 und l´Hospital gilt schließlich

$$\lim_{x\to 0}\frac{S_n(x)}{x}=\lim_{x\to 0}\frac{\frac{1}{n+1}\left(B_{n+1}(x)-B_{n+1}\right)}{x}=B_n(0)=B_n.$$

t

2.10 Satz

Sei *n* eine gerade natürliche Zahl und *m* eine natürliche Zahl grösser 1. Dann gilt

$$S_n(m)\equiv mB_n\equiv-\sum_{\substack{p|m\\(p-1)|n}}\frac{m}{p}\qquad(\mathrm{mod}\,m).$$

Beweis (siehe [Kel 2])

Es gilt $S_n(m)=\sum_{k=1}^{n}\left\langle {n \atop k}\right\rangle\binom{m}{k+1}=\sum_{k=2}^{n+1}\left\langle {n \atop k-1}\right\rangle\frac{m}{k}\binom{m-1}{k-1}$ Falls $(k,m)=1$ dann gilt $\frac{m}{k}\equiv 0\pmod m$. Satz 2.9 besagt, dass $k\,|\left\langle {n \atop k-1}\right\rangle$ für alle *k* ausser $k=p$ mit $p-1\,|\,n$. Also folgt für alle *k*, ausser eben $k=p$ mit $p-1\,|\,n$, dass

$$\left\langle {n \atop k-1}\right\rangle\frac{m}{k}\binom{m-1}{p-1}\equiv 0\pmod m.$$

Somit bleibt nur $S_n(m)\equiv\sum_{\substack{p|m\\p-1|n}}\left\langle {n \atop p-1}\right\rangle\frac{m}{p}\binom{m-1}{p-1}\pmod m$ übrig. Da nun *m* ein Vielfaches von *p* und *n* ein Vielfaches von *p*-1 ist, ist mit Satz 2.9 die Gleichheit für *p*=2 gegeben:

$$\left\langle {n \atop p-1}\right\rangle\binom{m-1}{p-1}\equiv(-1)\cdot(-1)^{p-1}\equiv-1\pmod p.$$

Letztendlich erhält man also

$$S_n(m) \equiv \sum_{\substack{p|m \\ p-1|n}} \left\langle {n \atop p-1} \right\rangle \frac{m}{p}\binom{m-1}{p-1} \equiv -\sum_{\substack{p|m \\ p-1|n}} \frac{m}{p} \pmod{m}.$$

Betrachtet man nun mB_n und benutzt man die gleichen Argumente wie oben, so erhält man:

$$mB_n \equiv \sum_{k=2}^{n+1} \left\langle {n \atop k-1} \right\rangle \frac{m}{k}(-1)^{k-1} \equiv \sum_{\substack{p|m \\ p-1|n}} \left\langle {n \atop p-1} \right\rangle \frac{m}{p}(-1)^{p-1} \equiv -\sum_{\substack{p|m \\ p-1|n}} \frac{m}{p} \pmod{m}.$$

Also gilt die gesuchte Gleichheit.

t

2.11 Theorem

Es gibt auch für gerade *n* eine Beziehung zwischen der Riemannschen Zetafunktion ($\zeta(s) = \sum_{k=1}^{\infty} k^{-s}, \quad s \in \mathbf{á}, \quad \mathrm{Re}\, s > 1$) und den Bernoulli Zahlen, die schon seit Euler bekannt ist:

$$2\zeta(2m) = (-1)^{m+1} \frac{(2\pi)^{2m}}{(2m)!} B_{2m}.$$

Beweis (vgl. [Ir.&Ro.])

Für den Beweis dieses Theorems benötigt man folgende Tatsache aus der Analysis:

$$\cot x = \frac{1}{x} - 2\sum_{n=1}^{\infty} \frac{x}{n^2\pi^2 - x^2}.$$

Dies kann in eine Potenzreihe um 0 entwickelt werden. Somit erhält man

$$x \cot x = 1 - 2\sum_{m=1}^{\infty} \zeta(2m) \frac{x^{2m}}{\pi^{2m}}.$$

Weiterhin gilt $\cos x = \frac{e^{ix} + e^{-ix}}{2}$ und $\sin x = \frac{e^{ix} - e^{-ix}}{2}$. Damit gilt

$$x \cot x = ix + \frac{2ix}{e^{2ix} - 1} = 1 + \sum_{n=2}^{\infty} B_n \frac{(2ix)^n}{n!}.$$

Koeffizientenvergleich liefert nun

$$-\frac{2}{\pi^{2m}}\zeta(2m)=(-1)^m\frac{2^{2m}}{(2m)!}B_{2m}.$$

t

2.12 Satz

Für die Vorzeichen der Bernoulli Zahlen gilt

$$\operatorname{sgn}(B_n)=(-1)^{\frac{n}{2}+1}.$$

Beweis (vgl. [Iwa], S.13)

Dies folgt direkt aus Theorem 2.11.

t

2.13 Theorem

Mit Hilfe der Funktionalgleichung von $\zeta(s)$ wird die Riemannsche Zetafunktion auf der gesamten komplexen Ebene analytisch fortgesetzt, ausser einer einfachen Polstelle mit Residuum 1 bei $s=1$:

$$\zeta(1-s)=2(2\pi)^s\cos\left(\frac{\pi s}{2}\right)\Gamma(s)\zeta(s),\quad s\in\mathbb{C}\setminus\{0,1\}.$$

Dann kann (2.11) umgeformt werden zu

$$\zeta(1-n)=-\frac{B_n}{n},\quad n\in\mathbb{N},\ n\geq 2.$$

Beweis (vgl [Ir.&Ro.] S. 240)

Für eine ganze Zahl m gilt $\Gamma(m)=(m-1)!$. Ist nun $m\geq 2$ eine gerade ganze Zahl folgt die Behauptung direkt aus 2.11.

t

Da $\zeta(n)$ gegen 1 konvergiert, sieht man an Hand dieser Formeln, wie schnell die Bernoulli Zahlen wachsen. Um dieses Wachstum zu verdeutlichen, hier eine einige Bernoulli Zahlen:

2.14 Beispiele

$B_0 = 1,$

$B_1 = -\frac{1}{2},$

$B_2 = \frac{1}{6},$

$B_4 = -\frac{1}{30},$

$B_6 = \frac{1}{42},$

$B_8 = -\frac{1}{30},$

$B_{10} = \frac{5}{66},$

$B_{12} = -\frac{691}{2730},$

$B_{14} = \frac{7}{6},$

.

.

.

Die größte bisher berechnete Bernoulli Zahl ist die 2000000ste (siehe [Kel3]):

$$B_{2000000} = -\frac{1329775613657311363237415859...3131145227911472514209002960697}{960148018301652497088402022491 0}$$

Wobei hier in der Mitte des Zähler mehr als 10 Millionen Ziffern fehlen!

Nun zu einigen wichtigen Eigenschaften der Bernoulli Zahlen:

2.15 Theorem (Clausen-von Staudt)

Sei *n* eine gerade ganze Zahl. Dann gilt

$$B_n + \sum_{p-1|n} \frac{1}{p} \in \mathbf{à}$$

und es gilt

$$denom(B_n) = \prod_{p-1|n} p.$$

Beweis (siehe [Kel. 2])

Da Satz 2.9 für alle $m>1$ gilt, gilt dieser Satz auch für $m=p$ mit *p* prim. Somit gilt

$$pB_n \equiv \left\{ \begin{array}{l} -1, \quad p-1 \mid n \\ \\ 0, \quad sonst \end{array} \right\} \pmod{p}.$$

Also muss der Nenner quadratfrei sein und die gesuchte Form haben. Setzt man nun $m = denom(B_n)$ und benutzt wieder Satz 2.9 so erhält man:

$$mB_n \equiv -\sum_{p-1|n} \frac{m}{p} \pmod{m}.$$

Durch *m* geteilt hat man also:

$$B_n \equiv -\sum_{p-1|n} \frac{1}{p} \pmod{\mathbf{à}}.$$

t

Theorem 2.15 zeigt, wie man den Nenner einer Bernoulli Zahl leicht berechnen kann.

2.16 Satz

Sei *k* eine gerade natürliche Zahl, für die $k \equiv 0 (\mathrm{mod}\ p-1)$ gilt. Dann ist $(B_k + 1/p) \in \mathbf{à}_p \subset \mathbf{â}_p$.

Beweis

Dies ist eine direkte Folgerung aus Theorem 2.15.

t

2.17 Theorem (Kummer)

Sei φ die Eulersche φ-Funktion. Seien weiter $n, m, p, e \in \mathbf{ã}$ mit *n*, *m* gerade, *p* prim und $p-1 \nmid n$. Dann gilt folgende Kummer-Kongruenz

$$\left(1-p^{n-1}\right)\frac{B_n}{n} \equiv \left(1-p^{m-1}\right)\frac{B_m}{m} \pmod{p^e}$$

mit $n \equiv m \pmod{\varphi(p^e)}$.

Beweis (vgl. [Ir.&Ro.], S. 239)

Sei im folgenden $t = ord_p m$, $B_m = \frac{U_m}{V_m}$ und $n = p^{e+t}$. Sei weiter *a* eine positive ganze Zahl mit $(a,n) = 1$. Wegen Theorem 2.15 gilt $p^t \mid U_m$. Da p^t sowohl *m* als auch U_m teilt, erhält man mit Hilfe von Satz 2.10 (für genaueres siehe [Ir.&Ro.], S. 237ff), dass

$$\frac{\left(a^m - 1\right)B_m}{m} \equiv a^{m-1} \sum_{j=1}^{p^{e-t}-1} j^{m-1} \left[\frac{ja}{p^{e+t}}\right] \qquad \left(p^e\right). \qquad (*)$$

Zu erst sei $e = 1$.
Nun lässt man auf der rechten Seite diejenigen j weg, die durch *p* teilbar sind. Gilt also $p \nmid j$ so ist $j^{p-1} \equiv 1 \quad (p)$. Ebenso ergibt sich aus $p \nmid a$, dass $a^{p-1} \equiv 1 \quad (p)$. Also verändert sich die rechte Seite nicht, wenn man m durch m', mit $m' \equiv m \quad (p-1)$, ersetzt. Somit ergibt sich

$$\frac{\left(a^{m'} - 1\right)B_{m'}}{m'} \equiv \frac{\left(a^m - 1\right)B_m}{m} \quad (p).$$

Wählt man nun für a eine primitive Wurzel modulo *p*, und da $p-1 \nmid m$ erhält man $a^{m'} - 1 \equiv a^m - 1 \not\equiv 0 \quad (p)$. Somit folgt, dass

$$\frac{B_{m'}}{m'} \equiv \frac{B_m}{m} \quad (p).$$

Ist nun $e > 1$ dann ist es nicht ganz so einfach, da man diejenigen Terme die j enthalten die durch *p* teilbar sind nicht so einfach beseitigt werden können. Man versucht also diese Terme zu separieren und die so erhaltene Summe um zu schreiben:

$$\sum_{j=1}^{p^{e-t}-1} j^{m-1} \left[\frac{ja}{p^{e+t}}\right] = \sum_{\substack{j=1 \\ (p,j)=1}}^{p^{e-t}-1} j^{m-1} \left[\frac{ja}{p^{e+t}}\right] \left(p^e\right) + p^{m-1} \sum_{i=1}^{p^{e-t-1}-1} i^{m-1} \left[\frac{ia}{p^{e+t-1}}\right].$$

Betrachtet man nun (*) und ersetzt *e* durch $e-1$, so erhält man,

$$\frac{p^{m-1}\left(a^m - 1\right)B_m}{m} \equiv p^{m-1} a^{m-1} \sum_{i=1}^{p^{e-t-1}-1} i^{m-1} \left[\frac{ia}{p^{e+t-1}}\right] \qquad \left(p^e\right).$$

Setzt man dies zusammen, so erhält man

$$\frac{\left(1 - p^{m-1}\right)\left(a^m - 1\right)B_m}{m} \equiv a^{m-1} \sum_{j=1}^{p^{e-t}-1} j^{m-1} \left[\frac{ja}{p^{e+t-1}}\right] \qquad \left(p^e\right). \qquad (**)$$

Gilt $m' \equiv m \quad \left(\varphi\left(p^e\right)\right)$ und $p \nmid j$, so ist $j^{m'-1} \equiv j^{m-1} \quad \left(p^e\right)$. Nun bleibt also die rechte Seite von $(**)$ unverändert modulo p^e, wenn man m durch m', mit $m' \equiv m \quad \left(\varphi\left(p^e\right)\right)$, ersetzt. Macht man genauso weiter wie im Fall $e = 1$ so erhält man das gesuchte Resultat.

t

2.18 Bemerkung (andere Version von Theorem 2.17)

Ist $n \not\equiv 0,1 \mod(p-1)$ und $n > a$ so gilt:

$$\frac{B_n}{n} \equiv \frac{B_{n+p^{a-1}(p-1)}}{n+p^{a-1}(p-1)} \qquad (\text{mod } p^a).$$

2.19 Bemerkung

Diese wichtige Kongruenz aus 2.18 bzw. 2.19 zeigt , dass

$$p^r \mid \frac{B_n}{n} \quad \Leftrightarrow \quad p^r \mid \frac{B_{n+k\varphi\left(p^r\right)}}{n+k\varphi\left(p^r\right)} \qquad \forall k \geq 0$$

für $2 \leq n < \varphi\left(p^r\right) = p^{r-1}(p-1)$ gilt.

Bernoulli Zahlen tauchen auch in der Definition der Eisenstein-Reihen ($E_k = 1 - \frac{2k}{B_k}\sum \sigma_{k-1}(n) q^n$, mit $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ und $q = e^{2\pi i}$) auf. Somit erhält man mit Aussagen über die Eisenstein-Reihen automatisch auch Aussagen über die Bernoulli Zahlen. In den folgenden Kapiteln wird hauptsächlich folgende, sich aus den Eisenstein-Reihen ergebende, „Variante“ der Bernoulli Zahlen benutzt.

2.20 Definition

Man definiere die Inversen Bernoulli Zahlen als $C_k := \frac{2k}{B_k}$.

3. Iwasawa Algebra

Dieses Kapitel wird zu einem für den weiteren Verlauf grundlegenden Satz führen. Und hat daher eine Schlüsselrolle. Da es nicht zum Verständnis beitragen würde wurde hier auf einige Beweise verzichtet und es wurden deshalb relativ viele Bemerkungen formuliert.
Zu diesem Kapitel vergleiche [Ser] und [Gek].

3.1. Die Iwasawa-Algebra für p ≠ 2

3.1.1 Bezeichnung

Ist n ≥1, so bezeichnet U_n die Untergruppe von $\mathbb{Z}_p^*$, die von den p-adischen Zahlen u mit $u \equiv 1 (\mathrm{mod}\ p^n)$ gebildet wird.

3.1.2 Bemerkung

Ist $s = s_0 + s_1 p + s_2 p^2 + \ldots \in \mathbb{Z}_p$ und $u \in U_1$ so setzt man

$$u^s = ((u-1)+1)^s = \sum_{k=0}^{s} \binom{s}{k}$$

3.1.3 Definitionen und Bemerkung

Man bezeichnet mit F die Algebra der Funktionen von $\mathbb{Z}_p$ mit Werten in $\mathbb{Z}_p$.
Ist $u \in U_1$, so bezeichnet f_u die Funktion $s \to u^s$. Die f_u ($u \in U_1$) erzeugen einen $\mathbb{Z}_p$-Untermodul L von F, der für sich betrachtet eine Unteralgebra ist. Die f_u formen nach dem Satz von Dedekind über die Unabhängigkeit der Charaktere eine Basis von L, deshalb ist es möglich, L mit der Algebra $\mathbb{Z}_p[U_1]$ der Gruppe U_1 zu identifizieren. Also schreibt sich ein Element von L eindeutig in der Form

$$s \sim f(s) = \sum_{u \in U_1} \lambda_u u^s$$

mit $\lambda_u \in \mathbb{Z}_p$ wobei die λ_u fast alle Null sind.

3.1.4 Definition

Man definiert $\overline{L}$ als den Abschluß von L in F versehen mit der Topologie der gleichmäßigen Konvergenz.

3.1.5 Satz

Die Elemente von L sind gleichstetig. Sind nämlich $f \in F$ und $n \geq 0$ gegeben, so gilt:

$$s \equiv s' \pmod{p^n} \quad \Rightarrow \quad f(s) \equiv f(s') \pmod{p^{n+1}}.$$

Beweis:

Offensichtlich genügt es, die Eigenschaft für die Funktionen

$$f_u(s) = \sum_{k \geq 0} \binom{s}{k} (pv)^k$$

mit $v = u - 1$ zu zeigen. Denn mittels Linearität und Grenzübergang ergibt sich dann die Behauptung für alle $f \in \overline{L}$. Setze dazu $s' = s+h$ mit $h \in p^n \mathbb{Z}_p$. Man zeigt die Kongruenz koeffizientenweise, also unter der Benutzung der Implikation

$$\binom{s+h}{k} \equiv \binom{s}{k} \pmod{p^n} \qquad \forall (k \geq 0) \Rightarrow f_u(s) \equiv f_u(s+h) \pmod{p^{n+1}}$$

Für den Koeffizienten $k = 0$ gilt trivialerweise die linke Seite.
Setze für $k \neq 0$

$$\phi(s) := \binom{s}{k}$$

was mittels Betrachtung der Taylorentwicklung

$$\phi(s + h) = \phi(s) + h\phi'(s) + O(h^2)$$

sofort die Behauptung für alle Koeffizienten k impliziert.

t

3.1.6 Bemerkung

Zusätzlich stimmt auf $\overline{L}$ die Topologie der gleichmäßigen Konvergenz mit jener der einfachen Konvergenz auf einem dichten Unterraum überein. Diese Topologie macht aus L einen kompakten Raum.

3.1.8 Definition und Bemerkung

Sei Λ definiert als die Algebra $\mathbb{Z}_p[[U_1]] = \varprojlim \mathbb{Z}_p[U_1/U_n]$. Diese ist isomorph zur Algebra $\mathbb{Z}_p[[T]]$ der formalen Potenzreihen in der Unbestimmten T. Der Isomorphismus ergibt sich durch Wahl eines topologischen Erzeugers $u = 1 + \pi$ von U_1, mit $v_p(\pi) = 1$ und durch Identifikation des Elementes f_u aus $\mathbb{Z}_p[U_1]$ mit dem Element $1 + T$ aus $\mathbb{Z}_p[[T]]$.

Λ ist kompakt in der Topologie, welche durch die Potenzen seines maximalen Ideals erzeugt wird, sofern man Λ mit $\mathbf{à}_p[[T]]$ identifiziert, da nur endlich viele Restklassen von U_1 existieren. Diese Topologie ist dann jene der einfachen Konvergenz der Koeffizienten. Die topologische Gruppe Λ ist deshalb isomorph zu einem abzählbaren Produkt über die Gruppen $\mathbf{à}_p$.
Die Algebren $\overline{L}$ und Λ enthalten beide $L = \mathbf{à}_p[U_1]$ als dichte Unteralgebra.

3.1.9 Lemma

Es existiert ein eindeutig bestimmter Isomorphismus $\varepsilon : \Lambda \to \overline{L}$ topologischer Algebren, dessen Einschränkung auf $\mathbf{à}_p[U_1]$ die Identität ist.

Beweis:

Die Eindeutigkeit von ε folgt aus der Tatsache, daß $\mathbf{à}_p[U_1]$ dicht in Λ liegt.
Um die Existenz zu zeigen, identifizieren man wie oben Λ mit $\mathbf{à}_p[[T]]$, indem man einen topologischen Erzeuger u aus U_1 wählen. Ist $f=\sum a_n T^n$ ein Element von Λ, so definiert man $\varepsilon(f)$ als die Funktion

$$s \to f(u^s-1)=\sum a_n(u^s-1)^n$$

Dies macht Sinn, da $u^s-1 \equiv 0 \pmod{p}$. Dann ist ε ein stetiger Homomorphismus von Λ nach F mit $\varepsilon(f_u) = f_u$. Daraus folgt, dass ε die Identität auf L ist. Mit der Stetigkeit erhälten man sogar $\varepsilon(\Lambda) = \overline{L}$.
Überdies ist ε injektiv und mit der Kompaktheit von Λ ein Homöomorphismus.

t

3.1.10 Zusätzliche Identitäten

Im Folgenden wird Λ mittels ε mit $\overline{L}$ identifiziert. Wie gesehen, geschieht dies durch Übergang einer Folge in der Unbestimmten T zu einer Funktion von s durch Variablentausch

$$T = u^s - 1 = vs + \ldots + v^n s^n/n! + \ldots, \quad \text{wobei } v = \log(u).$$

3.1.11 Satz

Jedes Element $f \neq 0$ von $\Lambda = \mathbf{à}_p[[T]]$ besitzt eine Weierstraßzerlegung:

$$f = p^\mu (T^\lambda + a_1 T^{\lambda-1} + \ldots + a_\lambda) u(T)$$

mit $\lambda, \mu \geq 0$, $v_p(a_i) \geq 1$ und u invertierbar in Λ.
Insbesondere ist die Anzahl der Nullstellen von $f(s)$ endlich und $\leq \lambda$.

Beweis

Sei o.B.d.A. $0 \neq f$ nicht durch p teilbar, dann hat man die übliche Darstellung von f als Potenzreihe $f=\sum_{i>0} a_i T^i$ mit Koeffizienten $a_i \in$ **à**$_p$. Setze nun $\lambda := \min\{i \mid p \text{ teilt nicht } a_i\}$. Man kann f anhand von λ zu

$$f = \sum_{i=0}^{\lambda} a_i T^i + \sum_{i>\lambda} a_i T^i$$

aufspalten. Setzt man zusätzlich

$$h = \sum_{i=0}^{\lambda} a_i T^i ,$$

so sucht man für die Weierstraßzerlegung eine Funktion $g \in \Lambda$, die der Gleichung $f = gh$ als Potenzreihe genügt. Dadurch erhält man folgende Identitäten für die Koeffizienten:
$a_0 = a_0 b_0$ also ist $b_0 = 1$.
Folglich ist g eine Einheit. Somit ist $b_i = 0$ für $1 \leq i \leq \lambda$. Dann ergibt sich
$b_{\lambda+1} = a_{\lambda+1}\, a_0^{-1}$, $b_{\lambda+2} = (a_{\lambda+2} - a_1\, b_{\lambda+1})\, a_0^{-1}$, u.s.w.
Die Koeffizienten b_i sind induktiv eindeutig durch die Koeffizienten a_i bestimmt. Also ist g eindeutig bestimmt. Da $f \in \Lambda$ und die Koeffizienten b_i durch Linearkombinationen von Koeffizienten von f von gleicher Ordnung bestimmt sind, und diese die entsprechenden Kongruenzbedingungen für Iwasawa-Funktionen erfüllen, folgt $g \in \Lambda$.
Zusammenfassend ist g damit eine der Potenzreihe f eindeutig zuzuordnende Einheit in Λ, die $f = gh$ erfüllt. Mit der Identifizierung $u(T) = g$ ist der Beweis abgeschlossen.

t

3.1.12 Lemma

Seien $f_1, \ldots f_n, \ldots$ eine Folge von Elementen von Λ. Wir nehmen an, daß lim $f_n(s)$ für jedes Element s einer unendlichen Teilmenge S von **à**$_p$ existiert. Dann konvergieren die f_n gleichmäßig auf **à**$_p$ gegen eine Funktion f, die wiederum zu Λ gehört.

Beweis

Angenommen, die Aussage des Lemmas wäre falsch. Dann existieren wegen der Kompaktheit von Λ zwei Teilfolgen von f_n, die gegen voneinander verschiedene Elemente f' und f'' von Λ konvergierten. Daraus würde folgen, daß $f' - f'' = 0$ auf ganz S wäre und mit der Voraussetzung einer unendlichen Nullstellenmenge, ist dies ein Widerspruch zur Weierstraßzerlegung.

t

3.2 Die Iwasawa-Algebra für p = 2

3.2.1 Definition

Wie in 3.1 werden die U_n als Untergruppen von $\mathbb{Z}_p^*$, die durch die 2-adischen Zahlen $u \equiv 1(\mathrm{mod}.2^n)$ gebildet werden definiert.

3.2.2 Bemerkung

Wir haben dann

$$\mathbb{Z}_p^* = U_1 = \{\pm 1\} \times U_2,$$

und U_2 ist isomorph zu $\mathbb{Z}_2$.

3.2.3 Definition

Falls $u \in U_1$, so bezeichnet man mit $\omega(u)$ seine Restklasse in $\{\pm 1\}$ und mit $\langle u \rangle$ seine Restklasse bzgl. U_2. Man definiert die Algebren L und Λ unter Benutzung der Gruppe U_2. Genauer ist L jetzt eine Algebra erzeugt von den Funktionen $f_u: s \sim u^s$ mit $u \in U_2$.

3.2.4 Bemerkungen

Genau wie in Abschnitt (1) zeigt man, daß sich der Abschluß $\overline{L}$ von L mit der Iwasawa-Algebra

$$\Lambda = \mathbb{Z}_2[[U_2]] = \varprojlim \mathbb{Z}_2[U_2/U_n]$$

identifizieren lässt. Deshalb ist dann auch Λ isomorph zu $\mathbb{Z}_2[[T]]$. Dieser Isomorphismus ergibt sich wieder durch die Wahl eines topologischen Erzeugers u von U_2 und durch Assoziation des Element f_u von $\mathbb{Z}_2[U_2]$ mit $1+T \in \mathbb{Z}_2[[T]]$. Die übrigen Resultate aus Abschnitt (1) übertragen sich auf offensichtliche Weise auf den Fall $p = 2$.

3.3 Charakterisierung der Elemente aus Λ durch ihre Reihenentwicklung

Wie soeben gesehen, können die zu Λ gehörigen Funktionen *f* als konvergente Taylorreihen der Form $f(s) = \sum_{n=0}^{\infty} a_n s^n$ aufgefaßt werden, wobei die Koeffizienten a_n jeweils die ihnen entsprechenden Kongruenzbedingungen erfüllen müssen. Um diese Kongruenzen bequem aufzuschreiben, definieren wir die Stirlingzahlen erster Art:

3.3.1 Definition

Die Stirlingzahlen erster Art, in Zeichen c_{in} $(1 \leq i \leq n)$, werden durch die Identität

$$\sum_{i=1}^{n} c_{in} Y^i = Y(Y-1)(Y-2)\ldots(-n+1) = n! \binom{Y}{n}$$

definiert.

3.3.2 Satz

Damit eine Funktion $f \in F$ zu Λ gehört, ist es notwendig und hinreichend, die Existenz *p*-adisch ganzer Zahlen b_k, $k = 1 \ldots n$ mit den Eigenschaften

$$a) \qquad f(s) = \sum_{n=0}^{\infty} b_n p^n s^n / n! \qquad \forall s \in \mathbf{Z}$$

$$b) \qquad v_p\left(\sum_{i=1}^{n} c_{in} b_i\right) \geq v_p(n!) \qquad \forall n \geq 1$$

zu zeigen. Ist $p = 2$, so muß man in (a) p^n durch 4^n ersetzen.

3.3.3 Bemerkung

Da $c_{nn} = 1$, ist (b) gleichbedeutend damit, zu sagen, daß jedes der b_n kongruent (mod $n!\,\mathbf{Z}_p$) zu einer $\mathbf{Z}$-Linearkombination der b_j für $j < n$ ist. Es gilt:

$v_p(b_n pn/n!) \geq n - v_p(n!) \geq n((p-2)/(p-1))$, falls $p \neq 2$
$v_2(b_n 4n/n!) \geq 2n - v_2(n!) \geq n$, falls $p = 2$.

Es folgt daraus, dass die *f* definierende Reihe auf einer *p*-adischen Kreisscheibe mit echt größerem Radius als die Einheitsscheibe konvergiert. A posteriori gilt also damit, dass die Reihe auf ganz $\mathbf{à}_p$ konvergiert, was der Formulierung in (a) einen Sinn gibt.

Beweis (von Satz (3.3.2))

Nur der Fall $p \neq 2$ soll vorgeführt werden, da der Fall $p = 2$ analog abzuhandeln ist.

(i) Die Entwicklung aus Abschnitt (1) $T = vs + \ldots + v^n s^n /n! + \ldots$ mit $v_p(v) = 1$ zeigt, dass sowohl T als auch alle Potenzen von T eine Entwicklung in der Form von (a) besitzt. Mit der Linearität und mittels Grenzübergang folgt, dass dies für jede Funktion f aus Λ so ist. Außerdem hängen die Koeffizienten $b_n = b_n(f)$ stetig von f ab. Hieraus läßt sich schließen, dass die Abbildung $f \sim (b_n(f))$ ein Isomorphismus des kompakten $\mathbf{à}_p$-Moduls Λ auf einen abgeschlossenen kompakten Untermodul S_Λ des Moduls $S = \left(\mathbf{à}_p\right)^{\tilde{a}}$ der Folgen (b_n) $n \geq 0$ ist. Zu zeigen ist, dass S_Λ mit dem Untermodul S_b von S, der durch die Kongruenzen in (b) bestimmt wird, übereinstimmt.

(ii) Jedes Element u aus U_1 läßt sich als $\exp(py)$ mit $y \in \mathbf{à}_p$ schreiben. Daraus folgt

$$u^s = \exp(pys) = \sum_{n=0}^{\infty} y^n p^n s^n / n!$$

also gilt $b_n(f_u) = y^n$. Daher gehört die Folge der (y^n) zu S_b. Somit ist

$$\sum_{i=0}^{n} c_{in} y^n = y(y-1)...(y-n+1) = n!\binom{y}{n}$$

eine p-adisch ganze Zahl. Dies zeigt, dass $\sum c_{in}\, y^n$ durch $n!$ in $\mathbf{à}_p$ teilbar ist. Wegen der Linearität und durch Grenzübergang folgt daher , dass S_Λ in S_b enthalten ist.
Es bleibt zu zeigen, dass $S_\Lambda = S_b$. Dazu reicht es zu zeigen, dass die Folgen der Form (y^n) mit $y \in \mathbf{à}_p$ einen dichten $\mathbf{à}_p$-Untermodul von S_b bilden.

(iii) Sei $m \geq 1$ und $b_o, \ldots, b_m \in \mathbf{à}_p$ genügen den Kongruenzen aus (b) für $n \leq m$. Zu zeigen ist, dass ein $f \in \Lambda$ existiert, so dass $b_i(f) = b_i$ für $0 \leq i \leq m$, was den Beweis vervollständigt.
Dazu wird eine Induktion über m benötigt. Der Fall $m = 0$ ist offensichtlich.
Mit der Induktionsannahme existiert dann ein $g \in \Lambda$, so dass $b_i(g) = b_i$ für $i \leq m - 1$. Es gilt nun, ein $h \in \Lambda$ zu finden, so dass $b_i(h) = 0$ für $i \leq m - 1$ und $b_m(h) = b_m - b_m(g)$. Damit sind sämtliche $b_i = 0$ für $i \leq m - 1$. Angesichts der Kongruenz aus Teil (b) folgt, dass b_m von der Form $m!z$ ist, mit $z \in \mathbf{à}_p$. Wir setzen daher $f = z(p/v)^m T^m$. Mit (i) folgt dann die Behauptung.

t

3.3.3 Korollar

Sei $f \in \Lambda$, und seien die b_n die entsprechenden Koeffizienten. Dann gilt:

$$b_n \equiv b_{n+p-1} \pmod{p} \qquad \forall\, n \geq 1.$$

Beweis:

Dies ist offensichtlich, falls die (b_n) alle von der Form (y^n) sind, mit $y \in \mathbf{à}_p$. Der allgemeine Fall folgt hieraus mittels Linearität und Grenzübergang.

t

3.3.4 Bemerkung

Eine andere Eigenschaft von Λ ist:
Ist $f \in \Lambda$, dann $(df/ds) \in p\Lambda$, falls $p \neq 2$ und $(df/ds) \in 4\Lambda$, falls $p = 2$.

Beweis:

Sei f vorgegeben durch die Form $f(s) = \sum_{n=0}^{\infty} b_n p^n \frac{s^n}{n!}$. Dann ist

$$\frac{df}{ds} = \sum_{n=0}^{\infty} b_n p^n \frac{s^{n-1}}{(n-1)!} = p \sum_{n=0}^{\infty} b_{n+1} p^n \frac{s^n}{n!} \quad \in \Lambda.$$

Der Fall ($p = 2$) verläuft analog.

t

3.3.5 Definition

Eine Funktion $f : X \to \mathbf{à}_p$ heißt Iwasawa in X, wenn $f \circ \alpha^{-1}$ eine Iwasawa-Funktion auf $\mathbf{à}_p$ ist.

Es sei daran erinnert, dass jede Funktion $f \in \Lambda$ eine eindeutige Mahler-Entwicklung (siehe hierzu Abschnitt (4)) besitzt. Diese ist von der Form

$$f(s) = \sum_{n \geq 0} \delta_n \binom{s}{n}$$

mit Koeffizienten $\delta_n \in \mathbf{à}_p$ mit $\delta_n \to 0$ für $n \to \infty$ und

$$\delta_n = \sum_{i=0}^{\infty} (-1)^i \binom{n}{i} f(n-i).$$

3.3.6 Bemerkung

Mit Induktion erhält man, dass für alle $f \in \Lambda$ die Kongruenz $\delta_n \equiv 0 (\mathrm{mod}\ p^n)$ erfüllt ist. Daraus wiederum erhält man die folgende Äquivalenz:

$$f(\mathbf{à}_p) \subset p^r \mathbf{à}_p \quad \Leftrightarrow \quad f(i) \equiv 0 (\mathrm{mod.}\ p^r),\ i = 0, 1, \ldots, r-1$$

für alle Iwasawa-Funktionen *f*.

Sei nun $X = a + p^t \mathbb{Z}_p$ eine Restklasse. Wähle einen affinen Isomorphismus $\alpha : \mathbb{Z}_p \to \mathbb{Z}_p$. Diese Definition ist sinnvoll und unabhängig von der Wahl von α, denn es gilt:

3.3.6 Bemerkung

Sei *f* eine Iwasawa-Funktion auf $\mathbb{Z}_p$, dann gilt:

(i) Für beliebige $a, b \in \mathbb{Z}_p$ ist $s \sim f(as + b)$ eine Iwasawa-Funktion auf $\mathbb{Z}_p$.

(ii) *f* eingeschränkt auf *X* ist eine Iwasawa-Funktion auf *X*.

Beweis

Zu (i): Die Behauptung gilt für die f_u. Mit dem Argument der Linearität und des Grenzüberganges folgt die Behauptung für alle Iwasawa-Funktionen.

Zu (ii): Nach Teil (i) ist die Definition der Iwasawa-Eigenschaft unabhängig von der Wahl eines Isomorphismus α. Deshalb ist die Zugehörigkeit zur Klasse der Iwasawa-Funktionen auch invariant gegenüber Inklusionsabbildungen und die Behauptung folgt.

t

3.3.7 Definition

Man definiere die arithmetische Progressionen modulo $(p - 1)p^t$ als:

$$C = \{k, k + (p - 1)\, p^t, k + 2(p - 1)\, p^t, \ldots\} \subset k = \{4, 6, 8, \ldots\}$$

3.3.8 Definition

Eine Funktion $f : C \to \mathbb{Z}_p$ heisst Iwasawa, falls sie eingeschränkt auf C eine Iwasawa-Funktion $f : X \to \mathbb{Z}_p$ bzgl. ihres topologischen Abschlusses $X = k + p^t \mathbb{Z}_p$ in $\mathbb{Z}_p$ ist.

3.3.9 Bemerkung

Sei *f* eine Iwasawa-Funktion auf C. Dann ist $f \equiv 0 (\mathrm{mod}\ p^r)$ genau dann, wenn *r* aufeinander folgende Elemente $k_1, k_2 = k_1 + (p - 1)\, p^t, \ldots, k_r = k_1 + (r - 1)(p - 1)\, p^t$ von C mit $f(k_1) \equiv f(k_2) \equiv \cdots f(k_r) \equiv 0 \pmod{p^r}$ existieren. (Für $p = 2$ erhalten wir ein entsprechendes Resultat durch Ersetzen von *p* durch 2 und von *r* durch $r' := [(r+1)/2]$.)

Beweis:

Dies ist eine direkte Folgerung aus Gleichung (1) und Bemerkung (3.2.1,(ii)).

t

3.4. Charakterisierung der Elemente Λ nach ihren Integrationseigenschaften

3.4.1 Definition

Seien $s_0, s_1 \in \mathbf{à}_p$ und $f \in F$. Setze $a_n = a_n(f) = f(s_0 + ns_1)$ und definiere $\delta_0, \delta_1, \ldots, \delta_n, \ldots$ als die fortgesetzten Differenzen der Folge (a_n) wie folgt:

$$\delta_0 = 0, \quad \delta_1 = a_1 - a_0, \quad \delta_2 = a_2 - 2a_1 + a_0, \quad \ldots \quad \delta_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_{n-i}.$$

3.4.2 Satz

Sei $h = 1 + v_p(s_1)$, falls $p \neq 2$ und $h = 2 + v_2(s_1)$, falls $p = 2$. Ist $f \in \Lambda$, so gilt:

$$(a) \quad \delta_n \equiv 0 \qquad (\mathrm{mod}.\, p^{nh}) \qquad \forall n \geq 0$$

$$(b) \quad v_p\Big(\sum_{i=1}^{n} c_{in}\delta_i p^{-ih}\Big) \geq v_p(n!) \quad \forall n \geq 1$$

Beweis:

Es genügt, Funktionen der Form $f(s) = u^s$ mit $u \in U_1$ zu betrachten (bzw. $u \in U_2$, falls p=2). Der allgemeine Fall ergibt sich dann mittels Linearität und Grenzübergang. Wir haben daher $a_n = u^{s_0} u^{ns_1}$ *sowie* $d_n = u^{s_0}\,(u^{s_1} - 1)^n$. Dabei ist $u^{s1} - 1$ ist von der Form $p^h y$, mit $y \in \mathbf{à}_p$. Also gilt $v_p(\delta_n) \geq nh$, und somit ist (a) gezeigt.
Die Behauptung in (b) folgt aus

$$\sum_{i=1}^{n} c_{in}\delta_i p^{-ih} = u^{s_0}\Big(\sum_{i=1}^{n} c_{in} y^i\Big) = u^{s_0} y(y-1)\ldots(y-n+1) = n!\,u^{s_0}\binom{y}{n} \equiv 0 \qquad (\mathrm{mod}.\, n!\mathbf{Z}_p).$$

t

3.4.3 Korollar

Sei $e_n = \delta_n p^{-nh}$, dann gilt: $e_n \equiv e_{n+p-1} \pmod{p}$ für alle $n \geq 1$.

Beweis:

Analog zum Beweis von 3.3.2.

t

3.4.4 Bemerkung

Es ist tatsächlich sogar so, dass Satz (3.4.2) die Elemente der Iwasawa-Algebra Λ charakterisiert. Genauer sei $s_0 = 0$ und $s_1 = 1$, so dass $a_n = f(n)$ und die δ_n die üblichen

Interpolationskoeffizienten sind. Nach dem Kriterium von Mahler gilt dann für stetige Funktionen f, daß $\delta_n \to 0$ für $n \to \infty$. Daraus läßt sich f dann in der Form

$$f(s) = \sum_{n=0}^{\infty} \delta_n \binom{s}{n} \qquad \forall s \in \mathbf{Z}_p$$

schreiben.

3.4.5 Satz

Sei f eine stetige Funktion in $\mathbf{à}_p$, mit Werten in $\mathbf{â}_p$, und seien $\delta_n = \sum_{i=1}^{n} (-1)^i \binom{n}{i} f(n-i)$ die Interpolationskoeffizienten. Damit f zu Λ gehört, ist es notwendig und hinreichend, dass:

$$(a) \quad \delta_n \equiv 0 \qquad \forall n \geq 0$$

$$(b) \quad v_p(\sum_{i=1}^{n} c_{in} \delta_i p^{-i}) \geq v_p(n!) \qquad \forall n \geq 1.$$

(Im Falle $p = 2$ ersetze man p^n durch 4^n in (a) sowie p^{-i} durch 4^{-i} in (b).)

Beweis:

Die Notwendigkeit folgt direkt aus Satz (3.4.2).
Für die andere Richtung sei $p \neq 2$. Es sei S_b die Menge der Folgen (b_n) von p-adischen Zahlen mit

$$v_p(\sum_{i=1}^{n} c_{in} b_i) \geq v_p(n!) \qquad \forall n \geq 1.$$

Wie in Abschnitt (2) gesehen, bilden die Folgen der Form (y^n) mit $y \in \mathbf{à}_p$ einen dichten Untermodul von S_b bzgl. der Produkttopologie. Nach Voraussetzung gehört so auch die Folge $(\delta_n p^{-n})$ zu S_b. Für jede Zahl m kann man deshalb endlich viele Elemente $\lambda_i, y_i \in \mathbf{à}_p$ wählen, so dass

$$\delta_n p^{-n} = \sum_{i=1}^{n} \lambda_i y_i^n \quad \forall n \leq m.$$

Setze $f_m(s) = \sum_{i=1}^{n} \lambda_i (1 + p y_i)^s$.

Es ist $f_m \in \Lambda$ (und auch $f_m \in L$). Außerdem zeigen die Definitionen von f_m und $\delta_n p^{-n}$, dass die n-ten Interpolationskoeffizienten von f_m für $n \leq m$ mit jenen von f übereinstimmen. Also gilt $f_m(n) = f(n)$ für $n \leq m$, und die Folge der f_m konvergiert punktweise gegen f $\mathbf{ã}$. Da nun $\mathbf{ã}$ dicht in $\mathbf{à}_p$ liegt, gilt schließlich mit Abschnitt (1) $f = \lim_{m \to \infty} f_m$. Es folgt $f \in \Lambda$, also die Behauptung.

t

3.5 Kongruenzen für Bernoulli-Zahlen

3.5.1 Definitionen

Setze $B_k/k := N_k/D_k$ mit ganzen Zahlen N_k, D_k, $D_k > 0$, für die ggT $(N_k, D_k) := (N_k, D_k) = 1$ ist. Dann ist auch N_k der Zähler von $B_k/2k$. Sei nun p eine feste aber frei wählbare Primzahl und sei

$$B_k^* := \left(1 - p^{k-1}\right) B_k,$$
$$C_k^* := \frac{-2k}{B_k^*}\left(1 - p^{k-1}\right)^{-1} C_k.$$

Unter der Regularitätsannahme gilt

$$C_k \equiv C_k^* \pmod{p^{k-1}}.$$

3.5.2 Satz

($p > 2$) Sei $p > 2$ eine Primzahl , $h \in \mathsf{k} = \{4, 6, 8, \ldots\}$, $\mathsf{C} \subset \mathsf{k}$ eine Restklasse modulo $(p - 1)p^t$, mit einer ganzen Zahl $t \geq 0$, und (h, p), (k, p) sowie $(k + h, p)$ seien regulär für alle $k \in \mathsf{C}$, was bedeutet, dass p kein Teiler der Zahlen B_k, B_h, B_{k+h} ist. Für gegebenes $r \geq 1$ und $1 \leq j \leq r$ sei

$$k_j = \min\{k \in \mathrm{C} \mid k \geq r + 1\} + (j - 1)(p - 1)\, p^t.$$

Setzen wir weiter $k_0 = k_r + h$ dann implizieren die Kongruenzen

$$C_{k+h} \equiv C_k + C_h \pmod{p^r}$$

für $k = k_1, k_2, \ldots, k_r$ dieselbe Kongruenz für alle $k \in \mathsf{C}$ mit $k \geq r + 1$.

($p = 2$) Sei $h \in \mathsf{k}$ und $\mathsf{C} \subset \mathsf{k}$ eine Restklasse modulo 2^t, mit einer ganzen Zahl $t \geq 0$. Für vorgegebenes $r \geq 1$ und $1 \leq j \leq r' := [(r+1)/2]$ sei

$$k_j = \min\{k \in \mathrm{C} \mid k \geq r + 1\} + (j - 1)2^t.$$

Setze weiter $k_0 = k_{r'} + h$. Dann implizieren die Kongruenzen

$$C_{k+h} \equiv C_k + C_h \pmod{2^r}$$

für $k = k_1, k_2, \ldots, k_{r'}$ dieselbe Kongruenz für alle $k \in \mathsf{C}$ mit $k \geq r + 1$.

Beweis:

Anstatt C_k zu betrachten kann man zu C_k^* übergehen. Denn C_k^* ist für jedes $k \in \mathbb{C}$ eine p-adische ganze Zahl, die gleich $2\zeta_p^{-1}(1-k)$ ist (mit ζ_p als p-adische Zeta-Funktion). Somit ist die Abbildung k ~ C_k^* eine Iwasawa-Funktion auf $\mathbb{C}$. Die Behauptung folgt daher aus Bemerkung (3.3.9) und aus der entsprechenden Version für $p = 2$.

t

4. Beweisprinzip und Probleme

Da man häufig nicht nur Kongruenz modulo p^r für ein bestimmtes *r* beweisen will, sondern für mehrere verschiedene *r*‘s, ist es sinnvoll, sich genügend Zahlenmaterial zu ermitteln. Dies ist auch die erste Hürde.
Zur Lösung des Problems benötigt man ein Programm, mit dem man schnellst möglich viele und große Bernoulli Zahlen berechnen kann. Ein solches Programm ist Calcbin[2] das von Bernd Kellner geschrieben wurde. Im Gegensatz zu anderen bekannten Programmen, die Bernoulli Zahlen berechnen können (z.Bsp. Pari), benutzt Calcbin nicht eine Rekursionsformel für Bernoulli Zahlen, siehe hierzu [Kel 3]. Dadurch ist es möglich, große Bernoulli Zahlen in verhältnismäßig kurzer Zeit zu berechnen.
Auf diese Weise wurde von mir ein Datenmaterial von 60.000 Bernoulli Zahlen erstellt.
Leider konnten die so erzeugten Zahlen nicht, in der von mir erwünschten Weise, in Calcbin weiter verarbeitet werden.
Zu dem war es mir nicht möglich, diese 60.000 Bernoulli Zahlen mit einem anderen Programm weiter zu verarbeiten. Die weiteren Berechnungen beruhten auf einer Datenbasis von 20.000 Inversen Bernoulli Zahlen. Diese wurden mit Pari erzeugt. Pari hat den großen Vorteil, dass mit diesem Programm alle weiteren Rechenschritte per Computer durchgeführt werden können. Um die recht unbequeme Ausgaberoutine von Pari einigermaßen beherrschen zu können, wurden die berechneten Inversen Bernoulli Zahlen jeweils in einer eigenen Datei abgespeichert. Für die weitere Verarbeitung wurden von mir geschriebene Unterprogramme von Pari zum Testen der Kongruenzen eingesetzt.
Der Nachteil von Pari ist, dass kein gutes Handbuch existiert. Zum Beispiel findet man nirgends eine Beschreibung, wie man eine Zahl als *p*-adische Zahl ausdrückt.
Die p-adischen Zahlen haben jedoch den Vorteil, dass die gesuchten Kongruenzen viel leichter zu erkennen sind.
Das nächste Problem, dass mit Hilfe des Pari Handbuches ungelöst bleibt, besteht in der Zuordnung der gespeicherten Inversen Bernoulli Zahlen. Es blieb einfach unklar, wie man sinnvoll auf die gespeicherten Daten zugreifen kann. Bei der Lösung dieser Probleme war mir der Pari Betreuer Karim Belabas behilflich (siehe hierzu [Pari]).

Mit Hilfe der oben erwähnten kleineren Programme, unter Verwendung von Satz 3.5.2 und im Rahmen der 20.000 Inversen Bernoulli Zahlen konnten die von Herrn Prof. Dr. Gekeler vermuteten Kongruenzen für einige Exponenten bewiesen werden (siehe hierzu 5.1). Sieht man sich diese Kongruenzen an, vermutet man, dass es vielleicht auch ähnliche Kongruenzen, die nicht schon durch die Kummer Kongruenzen abgedeckt werde, auch für andere Primzahlen größer als 7 gelten. Also wurden mit Hilfe der vorliegenden Daten und den geschriebenen Programmen solche Kongruenzen getestet. Diese Tests bewiesen für die ersten 20.000 Inversen Bernoulli Zahlen die neuen Kongruenzen, die in 5.2 dargestellt sind.

Um das angewendete Beweisprinzip, das auf Satz 3.5.2 beruht, zu verdeutlichen, hier einige Beispiele:

- $p = 2, \quad r = 11 \rightarrow r' = 6$
  Setzt man $t = 0$ so ergibt sich folgende Restklasse
  $C = \{0,2,4,6,8,10,12,14,16,18,20,22,24,.....\}$. Also erhält man folgende *k*’s:

[2] Siehe hierzu [Kel 3]

$$k_1 = 12 + 0 \cdot 2 = 12$$
$$k_2 = 12 + 1 \cdot 2 = 14$$
$$k_3 = 12 + 2 \cdot 2 = 16$$
$$k_4 = 12 + 3 \cdot 2 = 18$$
$$k_5 = 12 + 4 \cdot 2 = 20$$
$$k_6 = 12 + 5 \cdot 2 = 22$$

Diese Kongruenzen sind folglich zu testen:

$$C_{76=2^6+12} \equiv C_{64=2^6} + C_{12} \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{78=2^6+14} \equiv C_{64=2^6} + C_{14} \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{80=2^6+16} \equiv C_{64=2^6} + C_{16} \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{82=2^6+18} \equiv C_{64=2^6} + C_{18} \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{84=2^6+20} \equiv C_{64=2^6} + C_{20} \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{86=2^6+22} \equiv C_{64=2^6} + C_{22} \quad \left(\mathrm{mod}\ \ 2^{11}\right).$$

Dazu benötigt man folgende Inverse Bernoulli Zahlen:

$$C_{76} \equiv 2^4 + 2^5 + 2^7 \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{64} \equiv 2^8 \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{12} \equiv 2^4 + 2^5 + 2^7 + 2^8 + 2^9 + 2^{10} \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$

$$C_{78} \equiv 2^3 + 2^4 + 2^8 \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{64} \equiv 2^8 \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{14} \equiv 2^3 + 2^4 \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$

$$C_{80} \equiv 2^6 + 2^8 \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$
$$C_{64} \equiv 2^8 \quad \left(\mathrm{mod}\ \ 2^{11}\right)$$

$$C_{16} \equiv 2^6 \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{82} \equiv 2^3 + 2^5 + 2^8 + 2^9 + 2^{10} \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{64} \equiv 2^8 \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{18} \equiv 2^3 + 2^5 + 2^9 + 2^{10} \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{84} \equiv 2^4 + 2^6 + 2^7 \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{64} \equiv 2^8 \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{20} \equiv 2^4 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10} \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{86} \equiv 2^3 + 2^4 + 2^5 + 2^{10} \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{64} \equiv 2^8 \qquad \left(\text{mod}\ \ 2^{11}\right)$$

$$C_{22} \equiv 2^3 + 2^4 + 2^5 + 2^8 + 2^9 \qquad \left(\text{mod}\ \ 2^{11}\right).$$

- $p = 3, \quad r = 6$

Wählt man der Einfachheit halber $t=0$ so erhält man als Restklasse
$C = \{0,2,4,6,8,10,12,14,16,18,20,22,24,.....\}$. Es ergeben sich folgende *k*'s:

$k_1 = 8+0 \cdot 2 = 8$
$k_2 = 8+1 \cdot 2 = 10$
$k_3 = 8+2 \cdot 2 = 12$
$k_4 = 8+3 \cdot 2 = 14$
$k_5 = 8+4 \cdot 2 = 16$
$k_6 = 8+5 \cdot 2 = 18$

Also sind folgende Kongruenzen zu testen:

$$
\begin{aligned}
C_{62=2¥3^3+8} &\equiv C_{54=2¥3^3} + C_8 && \left(\mathrm{mod}\, 3^6\right)\\
C_{64=2¥3^3+10} &\equiv C_{54=2¥3^3} + C_{10} && \left(\mathrm{mod}\, 3^6\right)\\
C_{66=2¥3^3+12} &\equiv C_{54=2¥3^3} + C_{12} && \left(\mathrm{mod}\, 3^6\right)\\
C_{68=2¥3^3+14} &\equiv C_{54=2¥3^3} + C_{14} && \left(\mathrm{mod}\, 3^6\right)\\
C_{70=2¥3^3+16} &\equiv C_{54=2¥3^3} + C_{16} && \left(\mathrm{mod}\, 3^6\right)\\
C_{72=2¥3^3+18} &\equiv C_{54=2¥3^3} + C_{18} && \left(\mathrm{mod}\, 3^6\right).
\end{aligned}
$$

Mit

$$
\begin{aligned}
C_{62} &\equiv 2¥3 + 2¥3^4 + 3^5 && \left(\mathrm{mod}\, 3^6\right)\\
C_{54} &\equiv 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_8 &\equiv 2¥3 + 3^5 && \left(\mathrm{mod}\, 3^6\right)
\end{aligned}
$$

$$
\begin{aligned}
C_{64} &\equiv 3 + 2¥3^2 + 2¥3^4 + 3^5 && \left(\mathrm{mod}\, 3^6\right)\\
C_{54} &\equiv 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{10} &\equiv 3 + 2¥3^2 + 3^5 && \left(\mathrm{mod}\, 3^6\right)
\end{aligned}
$$

$$
\begin{aligned}
C_{66} &\equiv 3^2 + 3^3 + 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{54} &\equiv 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{12} &\equiv 3^2 + 3^3 && \left(\mathrm{mod}\, 3^6\right)
\end{aligned}
$$

$$
\begin{aligned}
C_{68} &\equiv 2¥3 + 2¥ 3^2 + 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{54} &\equiv 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{14} &\equiv 2¥3 + 2¥3^2 && \left(\mathrm{mod}\, 3^6\right)
\end{aligned}
$$

$$
\begin{aligned}
C_{70} &\equiv 3 + 3^2 + 3^3 + 3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{54} &\equiv 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{16} &\equiv 3 + 3^2 + 3^3 + 2¥3^4 + 2¥3^5 && \left(\mathrm{mod}\, 3^6\right)
\end{aligned}
$$

$$
\begin{aligned}
C_{72} &\equiv 2¥ 3^3 + 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{54} &\equiv 2¥3^4 && \left(\mathrm{mod}\, 3^6\right)\\
C_{18} &\equiv 2¥ 3^3 && \left(\mathrm{mod}\, 3^6\right)
\end{aligned}
$$

kann man diese Kongruenzen überprüfen.

- $p = 5, \quad r = 4$

Wählt man wieder $t=0$ und als Restklasse $C = \{2,6,10,14,18,22,...\}$ so erhält man

$$k_1 = 6+0¥4 = 6$$
$$k_2 = 6+1¥4 = 10$$
$$k_3 = 6+2¥4 = 14$$
$$k_4 = 6+3¥4 = 18.$$

Es sind somit folgende Kongruenzen zu testen:

$$C_{26=4¥5+6} \equiv C_{20=4¥5} + C_6 \qquad (\mathrm{mod}\, 5^4)$$
$$C_{30=4¥5+10} \equiv C_{20=4¥5} + C_{10} \qquad (\mathrm{mod}\, 5^4)$$
$$C_{34=4¥5+14} \equiv C_{20=4¥5} + C_{14} \qquad (\mathrm{mod}\, 5^4)$$
$$C_{38=4¥5+18} \equiv C_{20=4¥5} + C_{18} \qquad (\mathrm{mod}\, 5^4).$$

Die dafür nötigen Inversen Bernoulli Zahlen sind:

$$C_{26} \equiv 4 + 2¥5^2 + 4¥5^3 \qquad (\mathrm{mod}\, 5^4)$$
$$C_{20} \equiv 2¥5^2 \qquad (\mathrm{mod}\, 5^4)$$
$$C_6 \equiv 4 + 4¥5^3 \qquad (\mathrm{mod}\, 5^4)$$

$$C_{30} \equiv 4 + 2¥5 + 2¥5^2 + 2¥5^3 \qquad (\mathrm{mod}\, 5^4)$$
$$C_{20} \equiv 2¥5^2 \qquad (\mathrm{mod}\, 5^4)$$
$$C_{10} \equiv 4 + 2¥5 + 2¥5^3 \qquad (\mathrm{mod}\, 5^4)$$

$$C_{34} \equiv 4 + 4¥5 + 2¥5^2 \qquad (\mathrm{mod}\, 5^4)$$
$$C_{20} \equiv 2¥5^2 \qquad (\mathrm{mod}\, 5^4)$$
$$C_{14} \equiv 4 + 4¥5 \qquad (\mathrm{mod}\, 5^4)$$

$$C_{38} \equiv 4 + 5 + 3¥5^2 + 4¥5^3 \qquad (\mathrm{mod}\, 5^4)$$
$$C_{20} \equiv 2¥5^2 \qquad (\mathrm{mod}\, 5^4)$$
$$C_{18} \equiv 4 + 5 + 5^2 + 4¥5^3 \qquad (\mathrm{mod}\, 5^4).$$

- $p = 7, \quad r = 3$

Setzt man erneut $t = 0$ und wählt die Restklasse $C = \{6,12,18,24,30,...\}$ so ergeben sich folgende k's:

$$k_1 = 6 + 0 \cdot 6 = 6$$
$$k_2 = 6 + 1 \cdot 6 = 12$$
$$k_3 = 6 + 2 \cdot 6 = 18$$

Somit sind diese Kongruenzen zu über prüfen:

$$C_{48=6\cdot 7+6} \equiv C_{42=6\cdot 7} + C_6 \qquad \left(\mathrm{mod}\, 7^3\right)$$
$$C_{54=6\cdot 7+12} \equiv C_{42=6\cdot 7} + C_{12} \qquad \left(\mathrm{mod}\, 7^3\right)$$
$$C_{60=6\cdot 7+18} \equiv C_{42=6\cdot 7} + C_{18} \qquad \left(\mathrm{mod}\, 7^3\right).$$

Dies geschieht mit Hilfe folgender Inversen Bernoulli Zahlen:

$$C_{48} \equiv 2\cdot 7 + 5\cdot 7^2 \qquad \left(\mathrm{mod}\ \ 7^3\right)$$
$$C_{42} \equiv 2\cdot 7^2 \qquad \left(\mathrm{mod}\ \ 7^3\right)$$
$$C_6 \equiv 2\cdot 7 + 3\cdot 7^2 \qquad \left(\mathrm{mod}\ \ 7^3\right)$$

$$C_{54} \equiv 4\cdot 7 \qquad \left(\mathrm{mod}\ \ 7^3\right)$$
$$C_{42} \equiv 2\cdot 7^2 \qquad \left(\mathrm{mod}\ \ 7^3\right)$$
$$C_{12} \equiv 4\cdot 7 + 5\cdot 7^2 \qquad \left(\mathrm{mod}\ \ 7^3\right)$$

$$C_{60} \equiv 6\cdot 7 + 7^2 \qquad \left(\mathrm{mod}\ \ 7^3\right)$$
$$C_{42} \equiv 2\cdot 7^2 \qquad \left(\mathrm{mod}\ \ 7^3\right)$$
$$C_{48} \equiv 6\cdot 7 + 6\cdot 7^2 \qquad \left(\mathrm{mod}\ \ 7^3\right).$$

5. Kongruenzen für Bernoulli Zahlen

Es sei hier noch mal daran erinnert, dass $C_k = \frac{2k}{B_k}$, mit als *k*-te Bernoulli Zahl, wobei *k* eine gerade natürliche Zahl ist.

Mit Hilfe des im vorigen Kapitel vorgestellten Beweisprinzip können einige Kongruenzen für C_k, und somit für Bernoulli Zahlen, bewiesen werden.

5.1 Erste Kongruenzen

Es sei $k \geq 6$ eine gerade natürliche Zahl.

1. Für $2 \leq t \leq 14$ gilt:

$$C_{k+2^t} \equiv C_k + C_{2^t} \qquad \left(\mathrm{mod}\, 2^{t+5}\right).$$

2. Für $1 \leq t \leq 8$ gilt:

$$C_{k+2 \cdot 3^t} \equiv C_k + C_{2 \cdot 3^t} \qquad \left(\mathrm{mod}\, 3^{t+3}\right).$$

3. Für $0 \leq t \leq 5$ gilt:

$$C_{k+4 \cdot 5^t} \equiv C_k + C_{4 \cdot 5^t} \qquad \left(\mathrm{mod}\, 5^{t+3}\right).$$

4. Für $0 \leq t \leq 4$ gilt:

$$C_{k+6 \cdot 7^t} \equiv C_k + C_{6 \cdot 7^t} \qquad \left(\mathrm{mod}\, 7^{t+2}\right).$$

Beweis

Siehe hierzu Kapitel 4.

t

Obige Kongruenzen lassen die Vermutung zu, dass solche Kongruenzen auch für weitere Primzahlen gelten. Allerdings stellte sich heraus, dass zwar ähnliche Kongruenzen gelten, aber lange nicht so scharfe und, dass die Kongruenzen stark von der Restklasse der *k* modulo *p-1* abhängt.

Im nächsten Satz sind einige dieser Kongruenzen für C_k aufgelistet. Weitere Kongruenzen konnten nicht untersucht werden, da das vorhandene Datenmaterial nur die ersten 20.000 Bernoulli Zahlen umfasste. Vermutlich ist es mit größerem Datenmaterial möglich, weitere Kongruenzen dieser Art aufzustellen.

5.2 Weitere Kongruenz-Vermutungen

Es sei k eine gerade natürliche Zahl größer als 6.

1.)

a) Für $k \equiv \begin{Bmatrix} 0 & \mathrm{mod}\,10 \\ 4 & \mathrm{mod}\,10 \end{Bmatrix}$ gilt:

$$C_{k+10 \cdot 11^2} \equiv C_k + C_{10 \cdot 11^2} \quad (\mathrm{mod}\,11^4).$$

b) Für $k \equiv 2 \pmod{10}$ gilt:

$$C_{k+10 \cdot 11^2} \equiv C_k + C_{10 \cdot 11^2} + 159720 \quad (\mathrm{mod}\,11^4).$$

c) Für $k \equiv 6 \pmod{10}$ gilt:

$$C_{k+10 \cdot 11^2} \equiv C_k + C_{10 \cdot 11^2} + 119790 \quad (\mathrm{mod}\,11^4).$$

d) Für $k \equiv 8 \pmod{10}$ gilt:

$$C_{k+10 \cdot 11^2} \equiv C_k + C_{10 \cdot 11^2} + 95832 \quad (\mathrm{mod}\,11^4).$$

2.)

a) Für $k \equiv \begin{Bmatrix} 0 & (\mathrm{mod}\,12) \\ 2 & (\mathrm{mod}\,12) \end{Bmatrix}$ gilt:

$$C_{k+12 \cdot 13^2} \equiv C_k + C_{12 \cdot 13^2} \quad (\mathrm{mod}\,13^4).$$

b) Für $k \equiv 4 \pmod{12}$ gilt:

$$C_{k+12 \cdot 13^2} \equiv C_k + C_{12 \cdot 13^2} + 24167 \quad (\mathrm{mod}\,13^4).$$

c) Für $k \equiv \begin{Bmatrix} 6 & (\mathrm{mod}\,12) \\ 10 & (\mathrm{mod}\,12) \end{Bmatrix}$ gilt:

$$C_{k+12 \cdot 13^2} \equiv C_k + C_{12 \cdot 13^2} + 10985 \quad (\mathrm{mod}\,13^4).$$

d) Für $k \equiv 8 \pmod{12}$ gilt:

$$C_{k+12 \cdot 13^2} \equiv C_k + C_{12 \cdot 13^2} + 4394 \quad (\mathrm{mod}\,13^4).$$

3.)

a) Für $k \equiv 0 \pmod{16}$ gilt:

$$C_{k+16 \cdot 17^2} \equiv C_k + C_{16 \cdot 17^2} \pmod{17^4}.$$

b) Für $k \equiv 2 \pmod{16}$ gilt:

$$C_{k+16 \cdot 17^2} \equiv C_k + C_{16 \cdot 17^2} + 68782 \pmod{17^4}.$$

c) Für $k \equiv 4 \pmod{16}$ gilt:

$$C_{k+16 \cdot 17^2} \equiv C_k + C_{16 \cdot 17^2} + 73695 \pmod{17^4}.$$

d) Für $k \equiv 6 \pmod{16}$ gilt:

$$C_{k+16 \cdot 17^2} \equiv C_k + C_{16 \cdot 17^2} + 49130 \pmod{17^4}.$$

e) Für $k \equiv \left\{ \begin{matrix} 8 \pmod{16} \\ 14 \pmod{16} \end{matrix} \right\}$ gilt:

$$C_{k+16 \cdot 17^2} \equiv C_k + C_{16 \cdot 17^2} + 34391 \pmod{17^4}.$$

f) Für $k \equiv 10 \pmod{16}$ gilt:

$$C_{k+16 \cdot 17^2} \equiv C_k + C_{16 \cdot 17^2} + 58956 \pmod{17^4}.$$

g) Für $k \equiv 12 \pmod{16}$ gilt:

$$C_{k+16 \cdot 17^2} \equiv C_k + C_{16 \cdot 17^2} + 63869 \pmod{17^4}.$$

4.)

a) Für $k \equiv 0 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} \pmod{19^4}.$$

b) Für $k \equiv 2 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} + 75449 \pmod{19^4}.$$

c) Für $k \equiv 4 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} + 6859 \pmod{19^4}.$$

d) Für $k \equiv 6 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} + 96026 \pmod{19^4}.$$

e) Für $k \equiv 8 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} + 68590 \pmod{19^4}.$$

f) Für $k \equiv 10 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} + 48013 \pmod{19^4}.$$

g) Für $k \equiv 12 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} + 20577 \pmod{19^4}.$$

h) Für $k \equiv 14 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} + 891676 \pmod{19^4}.$$

i) Für $k \equiv 16 \pmod{18}$ gilt:

$$C_{k+18 \cdot 19^2} \equiv C_k + C_{18 \cdot 19^2} + 123462 \pmod{19^4}.$$

5.)

a) Für $k \equiv 0 \pmod{22}$ gilt:

$$C_{k+22 \cdot 23^2} \equiv C_k + C_{22 \cdot 23^2} \pmod{23^4}.$$

b) Für $k \equiv 2 \pmod{22}$ gilt:

$$C_{k+22 \cdot 23^2} \equiv C_k + C_{22 \cdot 23^2} + 36501 \pmod{23^4}.$$

c) Für $k \equiv 4 \pmod{22}$ gilt:

$$C_{k+22 \cdot 23^2} \equiv C_k + C_{22 \cdot 23^2} + 85169 \pmod{23^4}.$$

d) Für $k \equiv 6 \pmod{22}$ gilt:

$$C_{k+22 \cdot 23^2} \equiv C_k + C_{22 \cdot 23^2} + 146004 \pmod{23^4}.$$

e) Für $k \equiv 8 \pmod{22}$ gilt:

$$C_{k+22 \cdot 23^2} \equiv C_k + C_{22 \cdot 23^2} + 121670 \pmod{23^4}.$$

f) Für $k \equiv \left\{\begin{matrix} 10 & (\mathrm{mod}\, 22) \\ 16 & (\mathrm{mod}\, 22) \\ 18 & (\mathrm{mod}\, 22) \end{matrix}\right\}$ gilt:

$$C_{k+22 \cdot 23^2} \equiv C_k + C_{22 \cdot 23^2} + 133837 \quad (\mathrm{mod}\, 23^4).$$

g) Für $k \equiv 12 \quad (\mathrm{mod}\, 22)$ gilt:

$$C_{k+22 \cdot 23^2} \equiv C_k + C_{22 \cdot 23^2} + 170338 \quad (\mathrm{mod}\, 23^4).$$

h) Für $k \equiv \left\{\begin{matrix} 14 & (\mathrm{mod}\, 22) \\ 20 & (\mathrm{mod}\, 22) \end{matrix}\right\}$ gilt:

$$C_{k+22 \cdot 23^2} \equiv C_k + C_{22 \cdot 23^2} + 24334 \quad (\mathrm{mod}\, 23^4).$$

5.3 Bemerkung

Die in 5.2 vorgestellten Kongruenzvermutungen gelten für die ersten 20.000 Inversen Bernoulli Zahlen.

Literaturverzeichnis

[Gek] Ernst-Ulrich Gekeler, A Series of New Congruences for Bernoulli Numbers and Eisenstein Series, Journal of Number Theory , Vol. 9, 2002

[Ir.&Ro.] K.Ireland and M. Rosen, A Cassical Introduction To Modern Number Theory, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, 2nd Edition, 1990

[Iwa] Kenkechi Iwasawa, Lectures on p-Adic L-Functions, Princeton University Press und University of Tokyo Press, Princeton 1972

[Kel 1] Bernd Christian Kellner, Über irreguläre Paare höherer Ordnung. Diplomarbeit. Mathematisches Institut der Georg August Universität zu Göttingen. http://www.bernoulli.org/~bk/irrpairord.pdf,2002

[Kel 2] Bernd Christian Kellner, The Equivalence of Giuga's and Agoh's Conjectures, http://www.bernoulli.org/~bk/equivalence.pdf

[Kel 3] http://www.bernoulli.org

[Kob] Neal Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer Verlag

[Mur] M.Ram Murty, Introduction to p-adic Analytic Number Theory, Studies in Advanced Mathematics vol. 27, American Mathematical Society / International Press

[Neu] J. Neukirch, Algebraische Zahlentheorie, Springer Verlag, 1992

[Pari] http://www.pari.math.u-bordeaux.fr/

[Ser] J.-P. Serre, Formes modulaires et fonctions zêta p-adique, Lecture Notes in Mathematics, Vol.350, Springer Verlag, Berlin 1973