Eisensteinreihen aus arithmetischer Sicht

Johannes Lengler

13. Oktober 2004

Ich erkläre hiermit an Eides statt, diese Arbeit selbständig geschrieben und keine Hilfsmittel außer den angegebenen verwendet habe.

Inhaltsverzeichnis

Teil I

0.1 Vorwort

Diese Diplomarbeit richtet sich hauptsächlich an Mathematikstudenten und Mathematiker, die wenig oder nichts über Modulformen und Eisensteinreihen richten, sich aber aus dem einen oder anderen Grund über diese Themen informieren möchten. Jedoch können vor allem die späteren Kapitel auch durchaus für Mathematiker interessant sein, die schon etwas mehr über Eisensteinreihen gehört haben. In der vorliegenden Arbeit werden Eisensteinreihen und Eisensteinpolynome von einem arithmetischen Standpunkt her untersucht. Der Schwerpunkt liegt dabei auf den beiden Fragen:

- Welche arithmetischen Zusammenhänge bestehen zwischen den einzelnen Eisensteinreihen?
- Wie lassen sich Eisensteinreihen und ihre Polynome effizient berechnen?

Die Arbeit ist dabei wie folgt strukturiert: In Kapitel 1 werden (klassische) Eisensteinreihen definiert. Dem Leser wird eine kleine Motivation gegeben, indem der Zusammenhang mit der Weierstraßschen $\wp$-Funktion angedeutet wird. Dann werden fundamentale Eigenschaften der Eisensteinreihen erarbeitet, insbesondere der Zusammenhang mit der modularen Gruppe und die entsprechenden Transformationsgleichungen.
Im zweiten Kapitel werden die Eisensteinreihen dann in den Kontext der Modulformen eingebettet. Im Anschluss wird der Raum der Modulformen in der üblichen Weise als $\mathbb{C}[E_4, E_6]$ charakterisiert. Schließlich werden die Eisensteinpolynome in diesem Kapitel eingeführt.
Kapitel 3 widmet sich dem Problem, in wie weit arithmetische Fragestellungen für Eisensteinreihen und -polynome überhaupt sinnvoll sind. Insbesondere wird gezeigt, dass die Eisensteinpolynome ebenso wie die q-Entwicklungen der Eisensteinreihen rationale Koeffizienten haben. Ferner werden explizite Formeln für die Koeffizienten der Eisensteinreihen und der Δ-Funktion angegeben.
In Kapitel 4 geht es um die Berechnung der Eisensteinpolynome mit Computerhilfe. Zunächst wird die bisher verwendete Methode nach Swinnerton-Dyer erklärt. Diese wurde 1999 von Bernd Kremling in seiner Diplomarbeit in ein Computerprogramm umgesetzt. Anschließend wird ein anderes Verfahren von Prof. Ernst-Ulrich Gekeler vorgestellt, welches in Hinblick auf die Laufzeit eine deutliche Verbesserung versprach. Leider haben sich die in diese Methode gesetzten Erwartungen nur teilweise erfüllt, wie auch aus den ebenfalls in diesem Kapitel angestellten Laufzeitanalysen der beiden Vorgehensweisen deutlich wird. Im Rahmen dieser Diplomarbeit habe ich das neue Verfahren implementiert und für verschiedene Berechnungen benutzt.

Im letzten Kapitel gehe ich schließlich auf Fragen der Kongruenz zwischen Koeffizienten verschiedener Eisensteinreihen ein. Hier habe ich mich vor allem auf einen Typ Kongruenzen konzentriert, der durch endlich viele Berechnungen verifiziert werden kann. Diese Kongruenzen können also mit mäßigem Berechnungsaufwand von Computern bewiesen werden. Das Prinzip, dass für diese Beweise nur endlich viele Berechnungen notwendig sind, wurde 2001 von Prof. Gekeler erstmals publiziert.

In den Anhängen habe ich Stoff zusammengefasst, der für die meisten Leser vermutlich vertraut ist. In Anhang A geht es um die Frage der Konvergenz von Gittersummen. Diese Frage wurde exemplarisch anhand der Eisensteinreihen bearbeitet. In Anhang B sind einige Aussagen zu den Bernoullizahlen zusammengestellt. Anhang C befasst sich schließlich mit dem Begriff des asymptotischen Wachstums und den O-Notationen.

0.2 Danksagung

Ich bedanke mich an erster Stelle bei meinem Mentor, Professor Ernst-Ulrich Gekeler, dafür, dass er mich auf dieses spannende Thema aufmerksan gemacht hat. Außerdem bin ich Ute Staemmler und Thomas Bieler dankbar für ihre große Hilfe beim Ausmerzen von Unsauberkeiten, sowohl inhaltlicher als auch stilistischer Art. Schließlich möchte ich mich für die schier unendliche Geduld von Alice Keller bedanken, die mich bei vielen Fragen zu LaTeX immer nach besten Kräften beraten hat.

0.3 Bezeichnungen

Ich werde während der gesamten Diplomarbeit die hier folgenden Bezeichnungen und Symbole verwenden. Bezeichnungen, die erst im Laufe der Arbeit eingeführt werden, sind gesondert im Index aufgeführt.

$\mathbb{N} = \mathbb{N}_0 = 0, 1, 2, 3, \ldots$	= die Menge der natürlichen Zahlen.
$\mathbb{Z} = \ldots, -2, -1, 0, 1, 2, \ldots$	= die Menge der ganzen Zahlen.
$\mathbb{Q}$	= die Menge der rationalen Zahlen.
$\mathbb{C}$	= die Menge der komplexen Zahlen.
$\mathbb{F}_q$	= der endliche Körper mit q Elementen.
$\mathbb{Z}_p$	= die Menge der p-adischen Zahlen.
$\mathbb{P}$	= die Menge der positiven Primzahlen.
$\Im(z)$	= der Imaginärteil von z.
$\Re(z)$	= der Realteil von z.
$a \mid b$	= a ist ein Teiler von b.
(c, d)	= größter gemeinsamer Teiler von c und d.

$f \in O(g)$[1] $= f$ wächst asymptotisch höchstens so schnell wie g, d.h. $\frac{f(x)}{g(x)}$ bleibt beschränkt, wenn $x \to \infty$.

$f \in o(g)$[1] $= f$ wächst asymptotisch langsamer als g, d.h. $\frac{f(x)}{g(x)} \to 0$, wenn $x \to \infty$.

$f \in \Omega(g)$[1] $= f$ wächst asymptotisch mindestens so schnell wie g, d.h. $\frac{g(x)}{f(x)}$ bleibt beschränkt, wenn $x \to \infty$.

$f \in \omega(g)$[1] $= f$ wächst asymptotisch schneller als g, d.h. $\frac{g(x)}{f(x)} \to 0$, wenn $x \to \infty$.

$f \in \Theta(g)$[1] $= f$ und g wachsen asymptotisch gleich schnell, d.h es gilt $f \in O(g)$ und $g \in O(f)$.

[1] In Anhang C wird etwas über die Verwendung dieser Symbole im Kontext der Laufzeitanalyse gesagt.

Teil II

Kapitel 1

Eisensteinreihen

In diesem Kapitel werden wir auf elementare Weise Eisensteinreihen einführen, das letztendliche Objekt unseres Interesse. Indem wir uns den Zusammenhang mit der Weierstraßschen $\wp$-Funktion anschauen, werden wir außerdem eine erste Idee dafür bekommen, warum diese Reihen so einen wichtigen Platz in der Zahlentheorie haben. Wir werden diesen Aspekt jedoch recht knapp halten, denn das Hauptaugenmerk liegt bei dieser Diplomarbeit darauf, die Eisensteinreihen arithmetisch zu untersuchen.

1.1 Definition von Eisensteinreihen

Im Folgenden wird mit $\mathbb{H}$ immer die komplexe obere Halbebene bezeichnet, d.h.

$$\mathbb{H} = \{z \in \mathbb{C} | \Im(z) > 0\}.$$

1.1.1 Definition. *Sei $k \in \mathbb{N}$, $k \geq 3$.*
Die k-TE EISENSTEINREIHE E_k ist die Funktion von $\mathbb{H}$ nach $\mathbb{R}$, die durch

$$E_k(z) := \frac{1}{2\zeta(k)} \sum_{m,n}{}' \frac{1}{(mz+n)^k}$$

definiert wird.
Dabei ist $\zeta(k) := \sum_{n=1}^{\infty} \frac{1}{n^k}$ die RIEMANNSCHE ZETA-FUNKTION.
Das Symbol $\sum'_{m,n}$ bedeutet, dass über alle Werte $(m,n) \in \mathbb{Z} \times \mathbb{Z} \backslash \{(0,0)\}$ summiert wird.

1.1.2 Bemerkung. *Zu dieser Definition ist folgendes zu sagen:*

- *Für $k \geq 3$ konvergiert die Eisensteinreihe $E_k(z)$ absolut. Die Konvergenz ist gleichmäßig auf kompakten Teilmengen von $\mathbb{H}$. Genauer gesagt, ist die Konvergenz sogar für jedes $\epsilon > 0$ gleichmäßig auf der verschobenen oberen Halbebene $\{z \in \mathbb{C} | \Im(z) \geq \epsilon\}$. Eine Beweisskizze hierfür wird in Anhang A gegeben.*

- *Der aufmerksame Leser wird schnell bemerken, dass sich bei ungeradem k die Summanden für (m, n) und für $(-m, -n)$ gegenseitig aufheben, sodass insgesamt $E_k \equiv 0$ für alle ungeraden k gilt.*

- *Der Vorfaktor $1/2\zeta(k)$ ist nur ein konstanter Faktor, der qualitativ nichts an der Funktion ändert. Der Grund für diesen Faktor wird später noch ersichtlich werden. Der Wert der Zeta-Funktion an den relevanten Stellen ist wohlbekannt, z.B.:*

$$
\begin{aligned}
\zeta(2) &= \frac{\pi^2}{6}, \\
\zeta(4) &= \frac{\pi^4}{90}, \\
\zeta(6) &= \frac{\pi^6}{945}
\end{aligned}
$$

  (siehe z.B. [Mat, Riemann Zeta Function]).
  Eine genauere Behandlung der Zeta-Funktion wird erst später erforderlich sein. In Anhang B (Abschnitt 7.2) wird ein Zusammenhang zwischen den Werten $\zeta(k)$ und den Bernoullizahlen *B_k (für gerades k) angegeben.*

Ein wichtiger Zusammenhang besteht zwischen Eisensteinreihen und Gittern in $\mathbb{C}$. Ein *Gitter* L ist dabei eine Menge der Form $L = w_1 \cdot \mathbb{Z} \oplus w_2 \cdot \mathbb{Z}$, wobei w_1 und w_2 zwei $\mathbb{R}$-linear unabhängige komplexe Zahlen sind.
Zunächst ist offenbar die Menge $\{nz+m|n, m \in \mathbb{Z}\}$ selbst ein Gitter mit Basis $\{z, 1\}$, sofern $z \in \mathbb{H}$ ist. Man kann also die Eisensteinreihe auch schreiben als

$$E_k(z) = \frac{1}{2\zeta(k)} \sum_{\omega \in L}{}' \frac{1}{\omega^k},$$

wobei L das Gitter $\omega \cdot \mathbb{Z} \oplus 1 \cdot \mathbb{Z}$ bezeichnet. Umgekehrt gilt: Ist ein Gitter $L = \{w_1 \cdot m + w_2 \cdot n \,|m, n \in \mathbb{Z}\}$ gegeben, so lässt sich dieses auch schreiben als

$$
\begin{aligned}
L &= w_1 \cdot \{m + \frac{w_2}{w_1} \cdot n \,|m, n \in \mathbb{Z}\} \\
&= w_2 \cdot \{n + \frac{w_1}{w_2} \cdot m \,|m, n \in \mathbb{Z}\}.
\end{aligned}
$$

Von den beiden komplexen Zahlen $\frac{w_2}{w_1}$ und $\frac{w_1}{w_2}$ ist dabei genau eine aus der oberen Halbebene (aus $\mathbb{R}$ kann sie nicht sein, da w_1 und w_2 $\mathbb{R}$-linear unabhängig sein müssen), da sie sich zu 1 aufmultiplizieren. Ist zum Beispiel $\frac{w_2}{w_1} \in \mathbb{H}$, so ergibt sich:

$$\frac{1}{2\zeta(k)} \sum_{\omega \in L}{}' \frac{1}{\omega^k} = \frac{1}{w_1^k} E_k(\frac{w_2}{w_1}).$$

Wir sehen also, dass die Eisensteinreihen bis auf Vorfaktoren mit den Reihen der Form $\sum'_{\omega \in L} \frac{1}{\omega^k}$ identisch sind.

1.2 Zusammenhang mit $\wp$-Funktionen

Bevor wir uns den Zusammenhang zwischen Eisensteinreihen und Gittern genauer ansehen, möchte ich mich kurz der Frage zuwenden: Warum interessiert man sich eigentlich für diese Eisensteinreihen?
Nun, zunächst mal treten sie als recht natürliche Übertragung der Riemannschen ζ-Funktion auf den zweidimensionalen Fall auf (man summiert nur über ein zweidimensionales statt über ein eindimensionales Gitter), sodass man hoffen kann, durch ihr Studium auch diese Funktion besser zu verstehen.
Ein zweiter, schon etwas feinerer Zusammenhang besteht zu den Weierstraß'schen $\wp$-Funktionen:

1.2.1 Definition. *Ist L ein Gitter in $\mathbb{C}$, so ist die zugehörige* WEIERSTRASS'SCHE $\wp$-FUNKTION

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Diese Funktion konvergiert auf $\mathbb{C} \setminus L$ kompakt gleichmäßig. Der Beweis dieser Aussage verläuft ähnlich wie der Nachweis der Konvergenz der Eisensteinreihen in Anhang A.

1.2.2 Bemerkung. *Die Weierstraß'schen $\wp$-Funktionen spielen eine große Rolle bei der Untersuchung von* elliptischen Kurven*. Eine solche Kurve wird durch das Gitter L charakterisiert. Konkret ist die zu L gehörige Kurve $\mathbb{C}/L$. Das Gitter wiederum bestimmt die Weierstraß'sche $\wp$-Funktion, sodass diese Funktionen mit den elliptischen Kurven in Bijektion stehen. Die zu einer elliptischen Kurve gehörende Weierstraß'sche $\wp$-Funktion kann dann in natürlicher Weise auch als holomorphe Funktion auf dieser Kurve aufgefasst werden. Für Details und entsprechende Beweise siehe z.B. [Sil].*

1.2.3 Proposition. *Für ein gegebenes Gitter L ist die Laurentreihenentwicklung von $\wp$:*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=2}^{\infty} (k+1)2\zeta(k)G_k(L) \cdot z^k.$$

Hierbei wird mit $G_k(L)$ der Wert der Reihe

$$\sum_{\omega \in L}{}' \frac{1}{\omega^k}$$

bezeichnet, der sich ja unter Berücksichtigung der Vorfaktoren als ein Wert der k-ten Eisensteinreihe berechnen lässt.

Beweisskizze. Der ganze Anteil von $\wp$ heiße

$$\wp_{ganz}(z) := \sum_{\omega \in L}{}' \left(\frac{1}{(\omega - z)^2} - \frac{1}{\omega^2} \right).$$

Der nullte Taylorkoeffizient verschwindet wegen $\wp_{ganz}(0) = 0$.
Der erste Taylorkoeffizient (wie sowieso alle ungeraden) muss verschwinden, da die Funktion gerade ist.
Den k-ten Taylorkoeffizienten a_k $(k > 1)$ erhält man im Wesentlichen durch k-faches Ableiten.
Wir gehen davon aus, dass die kompakt gleichmäßige Konvergenz der Reihe schon etabliert ist. Dies kann man beispielsweise zeigen, indem man zeigt, dass die Reihe der Ableitungen $\sum \frac{1}{(\omega - z)^3}$ kompakt gleichmäßig konvergiert (dies läuft nun analog zu den Eisensteinreihen, siehe 7.1), und sich danach von der punktweisen Konvergenz in einem Punkt, nämlich in $z = 0$, überzeugt.
Hat man dies getan, darf man Differenzieren und Reihenbildung vertauschen, wodurch folgende Rechnung gerechtfertigt wird:

$$\begin{aligned}
a_k &= \frac{1}{k!} \frac{d^k}{dz^k} \wp_{ganz}(z) \bigg|_{z=0} \\
&= \frac{1}{k!}(k+1)! \sum_{\omega \in L}{}' \frac{1}{(\omega - z)^{k+2}} \bigg|_{z=0} \\
&= (k+1) \sum_{\omega \in L}{}' \frac{1}{\omega^{k+2}} \\
&= (k+1)2\zeta(k)G_{k+2}(L).
\end{aligned}$$

$\square$

Noch direkter tritt der Zusammenhang zwischen Eisensteinreihen und elliptischen Kurven in der folgenden Proposition zu Tage:

1.2.4 Proposition. *Sei L ein Gitter. Setze $g_2 := 60G_2(L)$, $g_3 := 140G_3(L)$, $x := \wp(z)$ und $y := \wp'(z)$. Mit diesen Bezeichnungen ist die Differenzialgleichung*

$$y^2 = 4x^3 - g_2 x - g_3 \tag{1.1}$$

erfüllt.
Der Beweis dieser Aussage erfolgt durch Einsetzen und Ausmultiplizieren.

Die Proposition hat eine wichtige Konsequenz: Da man die elliptische Kurve des Gitters L auch auffassen kann als die Punktmenge $\{(\wp(z), \wp'(z)) \,|\, z \in \mathbb{C})\}$, lässt sich die Kurve als Lösungsmenge der obigen, kubischen Gleichung beschreiben, die wiederum nur die freien Parameter g_2 und g_3 enthält.

1.2.5 Bemerkung. *Aufgrund des oben beschriebenen Zusammenhangs bezeichnen viele Autoren auch die Reihen g_2 und g_3 als Eisensteinreihen, d.h. sie benutzen eine andere Normierung als ich. Andere wiederum definieren die G_k als Eisensteinreihen. Auch wenn sich diese Bezeichnungen nur um Vorfaktoren unterscheiden, muss man doch große Sorgfalt walten lassen, wenn man mit verschiedenen Quellen arbeitet. Eine einheitliche Standardnotation ist leider nicht in Sicht.*

1.2.6 Bemerkung. *Um dem Leser etwas Verwirrung zu ersparen, habe ich die Dinge in diesem Abschnitt teilweise etwas vereinfacht dargestellt. Die angegebenen Korrespondenzen machen nur dann wirklich Sinn, wenn man statt mit $\mathbb{C}$ mit der projektiven Ebene $\mathbb{C} \cup \{\infty\}$ arbeitet. Tatsächlich ist sonst etwa der Ausdruck $\wp(z)$ gar nicht für alle $z \in \mathbb{C}$ erklärt. Es handelt sich dabei aber um eine rein technische Verkomplizierung, die die Einfachheit der Zusammenhänge nicht schmälert. Eine technisch korrekte Behandlung ist natürlich trotzdem nötig und wird zum Beispiel in [Car, Kap. V] vorgenommen.*

1.3 Eigenschaften von Gittern

Wir haben schon gesehen, dass Eisensteinreihen sich auch als Gittersummen auffassen lassen. Bisher haben wir Gitter über eine Basis (w_1, w_2) beschrieben. Nun können natürlich verschiedene Basen dasselbe Gitter liefern. In diesem Abschnitt werden wir diesen Sachverhalt genauer unter die Lupe nehmen.

1.3.1 Operation von $GL(2,\mathbb{Z})$

Sei L ein Gitter in $\mathbb{C}$ mit $\mathbb{Z}$-Basis (w_1, w_2). Zunächst einmal ist L ein $\mathbb{Z}$ -Modul vom Rang 2. Ist daher $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine invertierbare 2×2-Matrix über $\mathbb{Z}$ (d.h. eine Matrix mit Determinante ±1 und ganzzahligen Einträgen), so ist natürlich auch $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} aw_1 + bw_2 \\ cw_1 + dw_2 \end{pmatrix}$ eine Basis von L.
Erinnern wir uns nun daran, wie die Gittersummen mit den Eisensteinreihen zusammenhängen: Die Gittersumme $\sum'_{\omega\in L} \frac{1}{\omega^k}$ entsprach im Wesentlichen der Eisensteinreihe $E_k(z)$, wobei z eine der beiden Zahlen $\frac{w_1}{w_2}$ oder $\frac{w_2}{w_1}$ war. Gehen wir zunächst mal davon aus, dass es sich um den ersten Bruch handelt.
Geht man nun auf Gitterseite zur transformierten Basis (aw_1+bw_2, cw_1+dw_2) über, so entspricht dem auf Seiten der Eisensteinreihe der Bruch

$$\frac{aw_1 + bw_2}{cw_1 + dw_2} = \frac{a\frac{w_1}{w_2} + b}{c\frac{w_1}{w_2} + d} = \frac{az + b}{cz + d}$$

oder der Kehrwert dieses Bruches. Wir werden daher eben diese Transformation genauer studieren.
Zunächst einmal sehen wir uns genauer an, welcher der beiden in Frage kommenden Brüche denn nun der richtige ist. (D.h.: welcher der Brüche liegt in der oberen Halbebene?) Gehen wir dafür erst einmal davon aus, dass die Determinante $ad - bc = +1$ ist. Dann bekommt man:

$$\begin{aligned} \frac{az+b}{cz+d} &= \frac{(az+b)\overline{(cz+d)}}{(cz+d)\overline{(cz+d)}} \\ &= \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} \\ &= \frac{ac|z|^2 + bd + adz + bc\overline{z}}{|cz+d|^2}, \end{aligned}$$

wobei mit $\overline{x}$ die zu x komplex konjugierte Zahl gemeint ist. Der Imaginärteil dieses Bruches ist demzufolge:

$$\begin{aligned}
\Im\left(\frac{az+b}{cz+d}\right) &= \Im\left(\frac{ac|z|^2+bd+adz+bc\overline{z}}{|cz+d|^2}\right) \\
&= \frac{ad\cdot\Im(z)+bc\cdot\Im(\overline{z})}{|cz+d|^2} \\
&= \frac{\Im(z)(ad-bc)}{|cz+d|^2} \\
&= \frac{\Im(z)}{|cz+d|^2} \\
&> 0.
\end{aligned}$$

Diese Rechnung zeigt also, dass für $z \in \mathbb{H}$ auch $\frac{az+b}{cz+d} \in \mathbb{H}$ ist. Ist die Determinante $ad-bc$ dagegen -1, so liegt gerade der Kehrwert in $\mathbb{H}$. Auf Seite der Gitter entspricht der Übergang zum Kehrwert einfach dem Wechsel zwischen den Basen (w_1, w_2) und (w_2, w_1). Daher genügt es, sich im Folgenden auf solche Matrizen zu beschränken, die Determinante $+1$ haben.

1.3.1 Definition. *Sei $SL(2,\mathbb{Z})$ die Gruppe aller 2×2-Matrizen mit Koeffizienten in $\mathbb{Z}$ und Determinante $+1$.*
Die Gruppe $SL(2,\mathbb{Z})/\{+E,-E\}$ wird MODULARE GRUPPE *G genannt. Dabei sei E die 2×2-Einheitsmatrix.*
Ist der Zusammenhang klar, wird die Einheitsmatrix im Folgenden meist schlicht mit 1 bezeichnet.

Die Definition der modularen Gruppe wird sich deshalb als nützlich herausstellen, weil die Matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ die Zahl z unverändert lässt.
Trotzdem ist der Übergang zur Faktorgruppe natürlich nur deshalb sinnvoll, weil die Transformation mit der Gruppenstruktur der Matrizen verträglich ist:

1.3.2 Proposition. *Die modulare Gruppe G operiert auf $\mathbb{H}$ vermittels*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

Die Operation ist treu.

Beweis. Nachrechnen. □

1.3.3 Bemerkung. *Lässt man nicht nur Matrizen mit Einträgen aus $\mathbb{Z}$, sondern auch solche mit Einträgen aus $\mathbb{R}$ zu, so operieren diese natürlich immer noch auf $\mathbb{H}$. Es lässt sich zeigen, dass sich* alle *analytischen Automorphismen von $\mathbb{H}$ durch die Operation der Gruppe $PSL(2,\mathbb{R}) = SL(2,\mathbb{R})/\{\pm 1\}$ darstellen lassen.*

1.3.2 Struktur der modulare Gruppe

Bevor wir aber die Gruppenoperation in Formeln für die Eisensteinreihen ummünzen, werfen wir noch einen kurzen Blick auf die Struktur der modularen Gruppe. Dazu benutzen wir die Bezeichnungen

$$S := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

und

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

1.3.4 Proposition.

(a) Es gilt $S^2 = 1$ und $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ für alle $n \in \mathbb{Z}$.
Ferner gilt $(ST)^3 = 1$.

(b) Die modulare Gruppe G wird von S und T erzeugt.

Beweis.
(a) rechnet man einfach nach.
(b) Sei eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ gegeben. Wir zeigen, dass man diese Matrix durch sukzessives Multiplizieren mit S, T, S^{-1} und T^{-1} in die Matrix ± 1 überführen kann (es war ja $G = SL(2,\mathbb{Z})/\{\pm 1\}$). Dazu geben wir zunächst einen Algorithmus an, der den Wert $I := |c| + |d|$ so lange verkleinert, bis entweder c oder d verschwindet. (Dabei werden die Bezeichnungen a, b, c, d und I generisch verwendet, d.h. die Matrix, die man nach Durchlaufen eines Schrittes erhält, wird wiederum mit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ bezeichnet.)

(i) Ist $|d| \geq |c| > 0$, so ist der Wert I entweder für die Matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} T = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

oder für die Matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} T^{-1} = \begin{pmatrix} a & -a+b \\ c & -c+d \end{pmatrix}$$

kleiner als für $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, denn entweder ist $|c+d| < |d|$ oder $|-c+d| < |d|$.

(ii) Ist $|c| > |d| > 0$, so erfüllt die Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} S = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$ die Bedingung aus (i), daher muss die Zahl I entweder für $\begin{pmatrix} a & b \\ c & d \end{pmatrix} ST$ oder für $\begin{pmatrix} a & b \\ c & d \end{pmatrix} ST^{-1}$ kleiner werden.

Solange also sowohl $|c| > 0$ als auch $|d| > 0$ sind, verkleinert sich in jedem Schritt die Zahl I. Da es sich bei I aber um eine natürliche Zahl handelt, muss der Algorithmus irgendwann zu einem Ende kommen, d.h. es muss $c = 0$ oder $d = 0$ gelten.
Im zweiten Fall ersetze die Matrix $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$ durch die Matrix $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} S = \begin{pmatrix} -b & a \\ 0 & c \end{pmatrix}$. Auf diese Weise kann sichergestellt werden, dass man am Ende eine Matrix erhält, für die der linke untere Eintrag $= 0$ ist.
Da diese Matrix nach wie vor in der modularen Gruppe G liegt, muss die Determinante $ad - bc = ad = 1$ sein. Es gilt daher entweder $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = T^n$ oder $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} = -T^{-n}$ für ein $n \in \mathbb{Z}$.
Damit haben wir die Ausgangsmatrix also tatsächlich durch Multiplikationen mit S, T, S^{-1} und T^{-1} in ± 1 überführt. Die Matrizen S und T erzeugen also in der Tat die modulare Gruppe. $\square$

1.4 Eigenschaften der Eisensteinreihen

1.4.1 Die Transformationsgleichung

Wir wollen in diesem Abschnitt nun endlich erste Früchte der vorangegangenen Untersuchung der modularen Gruppe ernten. Sei ein Gitter L mit Basis (w_1, w_2) gegeben. Wir wissen schon, dass dadurch eine Gittersumme $\sum'_{\omega \in L} \frac{1}{\omega^k}$ definiert wird, die in engem Zusammenhang mit der Eisensteinreihe $E_k(z)$ steht, wobei $z = \frac{w_1}{w_2}$ ist (gegebenenfalls müssen w_1 und w_2 vertauscht werden, damit z in der oberen Halbebene liegt). Nun ist die Gittersumme aber von der gewählten Basis unabhängig. Wenn wir daher einen Basiswechsel durchführen, können wir die Gittersumme auf zwei verschiedene Arten über

die Eisensteinreihe ausdrücken und können uns somit eine Formel für die Eisensteinreihe erschließen.
Sei also eine modulare Matrix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ gegeben. Dann ist auch $\begin{pmatrix} w_1' \\ w_2' \end{pmatrix} := \begin{pmatrix} aw_1 + bw_2 \\ cw_1 + dw_2 \end{pmatrix} = g \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$ eine Basis von L und daher ist

$$\frac{1}{w_2^k} E_k \left(\frac{w_1}{w_2} \right) = \frac{1}{2\zeta(k)} \sum_{\omega \in L}{}' \frac{1}{\omega^k} = \frac{1}{(w_2')^k} E_k \left(\frac{w_1'}{w_2'} \right).$$

Aufgelöst nach $E_k(z)$ hat man

$$\begin{aligned} E_k(z) &= E_k \left(\frac{w_1}{w_2} \right) \\ &= \frac{w_2^k}{(w_2')^k} E_k \left(\frac{w_1'}{w_2'} \right) \\ &= \frac{w_2^k}{(cw_1 + dw_2)^k} E_k \left(\frac{az+b}{cz+d} \right) \\ &= \frac{1}{(cz+d)^k} E_k \left(\frac{az+b}{cz+d} \right) \\ &= (cz+d)^{-k} E_k \left(\frac{az+b}{cz+d} \right). \end{aligned}$$

Diese Gleichung wird Ausgangspunkt dafür sein, die Eisensteinreihen im folgenden Kapitel in einen allgemeineren Kontext einzubetten.

1.4.2 Verhalten in ∞

Zuvor soll jedoch noch auf eine weitere wichtige Eigenschaft eingegangen werden: Wir haben in Abschnitt 1.2 schon angedeutet, dass Eisensteinreihen eng mit elliptischen Kurven zusammenhängen. In diesem Abschnitt habe ich etwas vereinfachend gesagt, eine elliptische Kurve sei $\mathbb{C}/L$, wobei L ein Gitter in $\mathbb{C}$ sei.
Diese Konstruktion hat aber einen Schönheitsfehler: Die Kurve, die man auf diese Weise bekommt, ist nicht kompakt. Dieses Problem lässt sich jedoch leicht umgehen, indem man nicht von $\mathbb{C}$, sondern von der *Riemannschen Zahlkugel* $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ ausgeht.
Entsprechend würde man auch gerne Eisensteinreihen nicht bloß auf $\mathbb{H}$, sondern auf $\mathbb{H} \cup \{\infty\}$ definieren. Und in der Tat liefert die Abschätzung aus 7.1, dass sich die Reihe E_k für jedes k holomorph auf $\mathbb{H} \cup \{\infty\}$ fortsetzen lässt,

indem man $E_k(\infty) := 0$ setzt.
Allerdings tritt nun ein neues Problem auf: Wir hätten natürlich auch gerne, dass sich die Operation der modularen Gruppe G auf die erweiterte Menge fortsetzen lässt. Dies lässt sich mit einer weiteren Ausdehnung des Definitionsbereiches erreichen, nämlich durch Hinzunahme der rationalen Punkte.
Wir definieren daher:

1.4.1 Definition. *Sei* $\mathbb{H}_\infty := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.
Die Punkte aus $\mathbb{Q} \cup \{\infty\} \subset \mathbb{H}_\infty$ *werden als* SPITZEN *bezeichnet.*

Die Operation von G wird wie folgt auf $\mathbb{H}_\infty$ fortgesetzt:
Sei $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ und $x \in \mathbb{Q} \cup \{\infty\}$.

$$gx := \begin{cases} \frac{ax+b}{cx+d} & , \; x \in \mathbb{Q} \text{ und } cx+d \neq 0 \\ \infty & , \; x \in \mathbb{Q} \text{ und } cx+d = 0 \\ \frac{a}{c} & , \; x = \infty \text{ und } c \neq 0 \\ \infty & , \; x = \infty \text{ und } c = 0 \neq a \end{cases}$$

Man beachte bei dieser Definition, dass für $x \in \mathbb{Q}$ niemals gleichzeitig $ax + b = 0$ und $cx + d = 0$ auftreten kann, da die Matrix g sonst keinen vollen Rang hätte. Aus dem gleichen Grund können auch a und c nie gleichzeitig verschwinden.
Der Nachweis, dass es sich hierbei tatsächlich um eine Operation handelt, erfolgt durch einfache Fallunterscheidung. Die Punkte $\mathbb{Q} \cup \{\infty\}$ bilden eine Bahn unter der Operation von G, denn zu jedem gegebenen Bruch $q = \frac{a}{c} \in \mathbb{Q}$ mit teilerfremden a und c kann man zwei Zahlen b, $d \in \mathbb{Z}$ finden, sodass $ad - bc = 1$ (chinesischer Restsatz). Die Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ liegt daher in G und bildet den Punkt ∞ auf q ab.

1.4.2 Bemerkung.

- *Die Operation ist so eingerichtet, dass man intuitiv mit der Definition* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$ *auskommt, wenn man die üblichen Konventionen über die Arithmetik des Symbols* ∞ *einhält. Durch die obige Defintion liefert beispielsweise die „Rechnung“*

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \infty = \frac{2 \cdot \infty + 1}{1 \cdot \infty + 1} = \frac{2 \cdot \infty}{1 \cdot \infty} = \frac{2}{1} = 2$$

das korrekte Ergebnis.

- *Ebenso gilt (mit der Konvention* $E_k(q) := 0$ *für alle* $k \in \mathbb{Q}$*) generell unsere Transformationsformel: Ist* $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ *und* $z \in \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$*, so ist*
$$E_k(z) = (cz + d)^{-k} E_k(gz).$$

1.4.3 Bemerkung. *Auch hier muss man wieder etwas Vorsicht walten lassen: Fasst man* $\mathbb{H} \cup \mathbb{Q}$ *als Teilmenge von* $\mathbb{C}$ *auf, so wird* E_k *durch die Konvention* $E_k(q) = 0$ *nicht automatisch zu einer holomorphen Funktion (nicht einmal zu einer stetigen). Dies liegt aber nicht am Wert der Eisensteinreihe, sondern daran, dass es in der vorliegenden Situation unangebracht ist,* $\mathbb{Q}$ *als Teilmenge von* $\mathbb{C}$ *aufzufassen, denn die Punkte in* $\mathbb{Q}$ *haben ihren Ursprung ja als Bilder von* ∞ *unter der Operation von* G*. Wählt man aber die Topologie dementsprechend, so erhält man automatisch auch die Holomorphie der fortgesetzten Eisensteinreihe. Eine Möglichkeit, die Topologie konkret zu definieren, ist die folgende:*
Sei $q \in \mathbb{Q}$*. Eine Teilmenge* $M \subset \mathbb{H}_\infty$*, die* q *enthält, ist genau dann eine Umgebung von* q*, wenn es ein* $g \in G$ *gibt mit:*

- $gq = \infty$ *und*

- $gM \cap \overline{\mathbb{C}}$ *ist eine Umgebung von* ∞ *im Sinne der Topologie von* $\overline{\mathbb{C}}$*, d.h. sie enthält die Menge* $\{z \in \mathbb{C} | \Im(z) > C\}$ *für ein hinreichend großes* $C > 0$*.*

Kapitel 2

Modulformen

Um eine Funktion besser zu verstehen, ist es oft hilfreich, sich gleich eine ganze Klasse von ähnlich gearteten Funktionen anzuschauen. Dazu gilt es, die strukturellen Merkmale der Funktion zu extrahieren. Genau diese Vorgehensweise ermöglicht es auch, viele wichtige Dinge über Eisensteinreihen zu lernen. Die wichtigsten Eigenschaften haben wir schon im letzten Kapitel herausgearbeitet, sodass die nun folgenden Definitionen dem Leser (hoffentlich) als eine ganz natürliche Verallgemeinerung erscheinen werden.

2.1 Einführung von Modulformen

2.1.1 Definition. *Sei $k \in \mathbb{Z}$. Eine meromorphe Funktion $f : \mathbb{H} \to \overline{\mathbb{C}}$ heißt* SCHWACH MODULAR *vom Gewicht k, wenn sie für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ die Gleichung*

$$f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) \tag{2.1}$$

erfüllt.

2.1.2 Lemma. *Sei f meromorph auf $\mathbb{H}$, $k \in 2\mathbb{Z}$. Dann ist f genau dann schwach modular vom Gewicht k, wenn für alle $z \in \mathbb{H}$ die beiden folgenden Gleichungen erfüllt sind:*

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

Beweis. Wir haben in Abschnitt 1.3.2 gesehen, dass die modulare Gruppe G von den beiden Matrizen $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ erzeugt wird. Diese

beiden Matrizen liefern genau die beiden oben angeführten Gleichungen. Es genügt daher nachzurechnen, dass die Transformationsgleichung (2.1) mit der Gruppenoperation verträglich ist.
Dieses Nachrechnen kann natürlich ohne Weiteres von Hand geschehen. Es gibt aber auch einen etwas aufschlussreicheren Ansatz von Jean-Pierre Serre ([Ser]): Fasst man $g \in G$ als Automorphismus von $\mathbb{H}$ auf, so gilt

$$\frac{d(gz)}{dz} = (cz+d)^{-2}.$$

Die Transformationsgleichung kann daher auch geschrieben werden als

$$\frac{f(gz)}{f(z)} = \left(\frac{d(gz)}{dz}\right)^{-k/2}$$

bzw. als

$$f(gz)d(gz)^{k/2} = f(z)dz^{k/2}.$$

Die Transformationsgleichung sagt also nichts anderes aus, als dass der Ausdruck $f(z)dz^{k/2}$ invariant unter der Operation von G ist. In dieser Formulierung ist es natürlich klar, dass es genügt, die Invarianz unter den beiden erzeugenden Elementen S und T der modularen Gruppe nachzuprüfen.
Der Ausdruck „$f(z)dz^{k/2}$" ist dabei eine Differenzialform vom Gewicht $k/2$. Da wir das Konzept der Differenzialformen jedoch im Folgenden nicht benötigen werden, verzichte ich darauf, es hier einzuführen. Der interessierte Leser kann Details zum Beispiel in [Fre] nachlesen. □

2.1.3 Bemerkung. *Ist $k \in \mathbb{Z}$ ungerade, so ist die einzige schwach modulare Funktion vom Gewicht k die 0-Funktion.*

Beweis. Substituiert man in der Funktionalgleichung $f\left(-\frac{1}{z}\right) = z^{-k}f(z)$ den Wert $z' := -\frac{1}{z}$, so erhält man die Gleichung

$$\begin{aligned} f(z') &= \left(-\frac{1}{z'}\right)^{-k} f(-\frac{1}{z'}) \\ &= -(z')^k\left((z')^{-k}f(z')\right) \\ &= -f(z'). \end{aligned}$$

Es muss daher $f(z') = 0$ für alle z' gelten.
Also verschwindet jede schwach modulare Funktion von ungeradem Gewicht.
□

Die Gleichung $f(z+1) = f(z)$ hat noch einen besonderen Effekt: Da die Funktion periodisch mit Periode 1 ist, lässt sie sich auch in der Variablen $q = e^{2\pi iz}$ ausdrücken. Das bedeutet nichts anderes, als dass es eine meromorphe Funktion $\tilde{f}$ gibt, sodass gilt:

$$\tilde{f}(e^{2\pi iz}) = f(z) \quad \text{für alle } z \in \mathbb{H}.$$

Der Definitionsbereich von $\tilde{f}$ muss dabei offenbar die punktierte Einheitskreisscheibe $\{z \in \mathbb{C} \mid |z| < 1\} \backslash \{0\}$ sein.

2.1.4 Vereinbarung. *Die Funktion $\tilde{f}$ wird im Folgenden ebenfalls mit f bezeichnet werden. Um Missverständnisse zu vermeiden, wird die Variable in diesen Fällen nicht mehr z, sondern q genannt. Aufgrund der Umrechnungsgleichung hat es sich eingebürgert, in diesem Fall zu sagen, dass man f* IN DER VARIABLEN $q = e^{2\pi iz}$ *angibt.*

2.1.5 Definition. *Der Punkt $q = 0$ entspricht offenbar genau dem Punkt $z = \infty \in \mathbb{H}_\infty$.*
Wir nennen daher eine schwach modulare Funktion f MEROMORPH IN ∞, *wenn sie als Funktion in $q = e^{2\pi iz}$ eine meromorphe Fortsetzung im Punkt 0 besitzt. In diesem Fall nennen wir die Funktion f* MODULAR.
Ist die Fortsetzung in diesem Punkt sogar holomorph mit Wert a, nennen wir a auch DEN WERT VON f IM PUNKT ∞ *und schreiben $f(\infty) = a$.*

2.1.6 Definition. *Eine modulare Funktion heißt* MODULFORM, *wenn sie auf ganz $\mathbb{C}$ und in ∞ holomorph ist.*
Erfüllt sie zusätzlich noch die Bedingung $f(\infty) = 0$, so wird sie SPITZENFORM *genannt.*

2.1.7 Lemma.

- *Die Menge der schwach modularen Funktionen (der modularen Funktionen, der Modulformen, der Spitzenformen) bildet einen $\mathbb{C}$-Vektorraum.*
- *Sind f und f' Modulformen vom Gewicht k und k', so ist ihr Produkt ff' eine Modulform vom Gewicht $k + k'$.*

Beweis. triviales Nachrechnen. □

2.1.8 Beispiele.

- *Die Eisensteinreihe E_k ist natürlich eine Modulform vom Gewicht k. Wir haben bereits in 7.1 gesehen, dass jede Eisensteinreihe gleichmäßig in einer Umgebung von ∞ konvergiert (nämlich für jedes $c > 0$*

auf der Menge $\{z \in \mathbb{C} | \Im(z) > c\}$). Wir können daher den Grenzwert $\lim_{\Im(z)\to\infty} E_k(z)$ ausrechnen, indem wir Reihen- und Grenzwertbildung vertauschen:

$$\begin{aligned}
\lim_{\Im(z)\to\infty} E_k(z) &= \lim_{\Im(z)\to\infty} \frac{1}{2\zeta(k)} \sum_{m,n}{}' \frac{1}{(mz+n)^k} \\
&= \frac{1}{2\zeta(k)} \sum_{m,n}{}' \underbrace{\lim_{\Im(z)\to\infty} \frac{1}{(mz+n)^k}}_{=0,\ \textit{falls}\ m\neq 0} \\
&= \frac{1}{2\zeta(k)} \sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{1}{n^k} \\
&= \frac{1}{2\zeta(k)} 2 \sum_{n=1}^{\infty} \frac{1}{n^k} \\
&= 1
\end{aligned}$$

Diese Rechnung gilt natürlich nur für gerades k, für ungerades k verschwindet E_k sowieso.
Nun wird auch endlich ersichtlich, warum wir die Eisensteinreihen mit Vorfaktoren versehen haben: Dadurch wurde der Wert im Punkt ∞ auf 1 normiert.

- *Wir sind nun soweit, unsere erste nichttriviale Spitzenform zu definieren:*
  Wir wissen, dass E_4 und E_6 Modulformen vom Gewicht 4 bzw. 6 sind. Daher sind nach Lemma 2.1.7 auch $(E_4)^3$ und $(E_6)^2$ Modulformen, und zwar beide vom Gewicht 12. Nach demselben Lemma ist also auch

  $$\Delta := \frac{1}{1728}\left(E_4^3 - E_6^2\right)$$

  eine Modulform vom Gewicht 12 und es gilt

  $$\Delta(\infty) = \frac{1}{1728}\left((E_4(\infty))^3 - (E_6(\infty))^2\right) = \frac{1}{1728}(1-1) = 0.$$

  Damit ist Δ eine Spitzenform vom Gewicht 12.

2.1.9 Bemerkung. *Die Spitzenform Δ wird später noch eine zentrale Rolle spielen. Wir werden uns an gegebener Stelle überlegen, dass sie nicht identisch verschwindet (Abschnitt 2.2.7).*
Außerdem werden wir später noch feststellen, dass die Normierung von Δ dazu führt, dass das Residuum an der Stelle ∞ genau 1 ist.

2.2 Der Vektorraum der Modulformen

In diesem Abschnitt werden wir uns schrittweise auf das Ziel zubewegen, den Vektorraum der Modulformen vollständig zu beschreiben. Damit machen wir einen deutlichen Schritt auf das eigentliche Ziel dieser Arbeit hin. Wir werden nämlich sehen, dass sich alle Modulformen (insbesondere auch alle Eisensteinreihen) über die beiden Reihen E_4 und E_6 beschreiben lassen. Insbesondere besteht also ein Zusammenhang zwischen den Eisensteinreihen höheren Gewichts mit E_4 und E_6. Diesen Zusammenhang werden wir dann schließlich genauer untersuchen.

2.2.1 Der Fundamentalbereich

Um die Modulformen zu beschreiben, wenden wir uns erst einer Fragestellung zu, die auf den ersten Blick nicht ganz zielgerichtet scheint:
Wir haben für unsere Modulformen per Definition Funktionalgleichungen zur Verfügung. Wenn wir den Wert einer Modulform an einer bestimmten Stelle kennen, können wir den Wert an gewissen anderen Stellen daraus errechnen (z.B. lässt sich $f(-\frac{1}{z})$ aus $f(z)$ berechnen). Die Frage lautet nun:
An welchen Stellen müssen wir die Funktion kennen, damit wir alle anderen Werte aus den gegebenen Daten errechnen können?
Diese Frage ist nicht nur für sich genommen recht natürlich, sondern wir werden später noch sehen, dass uns die Antwort helfen wird, den Vektorraum der Modulformen genauer zu verstehen.

Ich behaupte nun, dass die Menge $\mathcal{F} := \{z \in \mathbb{C} | |\Re(z)| \leq \frac{1}{2} \text{ und } |z| \geq 1\}$ (siehe Abb. 2.1) ausreicht, um eine Modulform vollständig zu definieren.
Genauer gesagt:

2.2.1 Satz.

(i) Zu jedem $z \in \mathbb{H}$ gibt es ein $g \in G$, sodass $gz \in \mathcal{F}$ ist.

(ii) Zwei Punkte z und z' aus $\mathcal{F}$ sind nur dann kongruent modulo G, wenn

- *entweder $\Re(z) = \pm\frac{1}{2}$ und $z' = z \mp 1$*
- *oder $|z| = 1$ und $z' = -\frac{1}{z}$.*

(iii) Ist $z \in \mathcal{F}$, so gilt für den Stabilisator $I(z) := \{g \in G | gz = z\}$:

$$I(z) := \begin{cases} \{1, S\} & \text{, falls } \quad z = i, \\ \{1, ST, (ST)^2\} & \text{, falls } \quad z = \rho = e^{2\pi i/3}, \\ \{1, TS, (TS)^2\} & \text{, falls } \quad z = -\overline{\rho} = e^{\pi i/3}, \\ \{1\} & \text{, sonst} \end{cases}$$

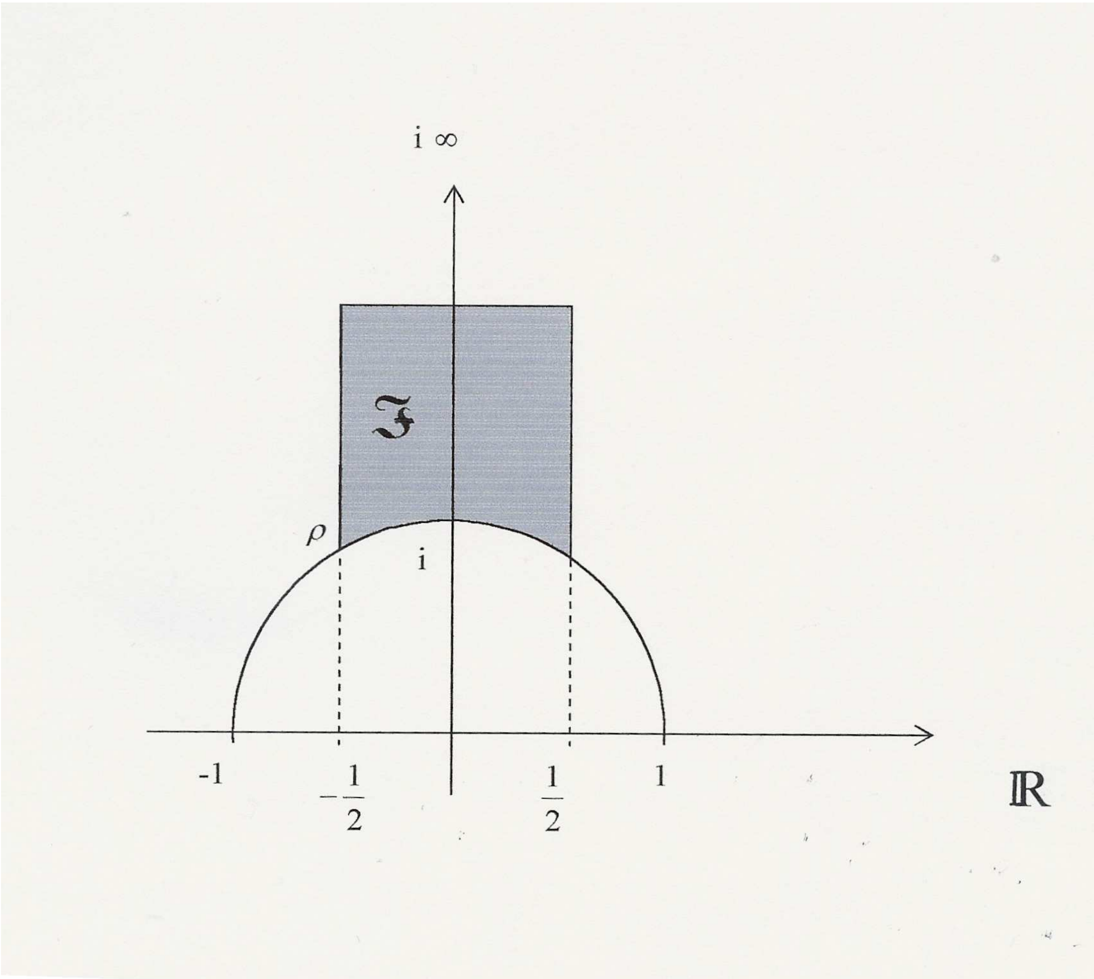

Abbildung 2.1: Fundamentalbereich

Man nennt die Menge $\mathcal{F}$ auch einen FUNDAMENTALBEREICH *der Operation von G auf* $\mathbb{H}$.

Beweisskizze. Wir haben schon gesehen, dass wir uns auf die beiden Funktionalgleichungen

$$f(z+1) = f(z)$$

und

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

beschränken können (siehe 2.1.2).
Die Beschränkung $|\Re(z)| \leq \frac{1}{2}$ überrascht sicherlich nicht, denn mit der ersten Formel können wir diese Bedingung sofort erreichen.
Die Einschränkung $|z| \geq 1$ wird durch folgende Überlegung plausibel: Startet man mit einem $z \in \mathbb{H}$ mit $|z| < 1$, so erhält man durch den Übergang $z \to -\frac{1}{z}$ einen Wert, dessen Imaginärteil auf jeden Fall größer ist als der von z. Durch geeignetes, mehrfaches Anwenden der Transformation $z \to z \pm 1$ erhält man also ein z_1 mit größerem Imaginärteil, das wieder $-\frac{1}{2} \leq \Re(z_1) \leq \frac{1}{2}$ erfüllt.
Ist nun $|z_1| \geq 1$, so ist man fertig.
Ansonsten führt man den obigen Schritt erneut aus. Dadurch erhält man wiederum ein neues z_2 mit $-\frac{1}{2} \leq \Re(z_2) \leq \frac{1}{2}$, dessen Imaginärteil noch größer als der von z_1 ist. Man kann mit einer relativ einfachen Rechnung einsehen, dass dieses Verfahren terminieren muss, sodass man am Ende tatsächlich mit einem z aus $\mathcal{F}$ endet.
Ein ausführlicher Beweis steht in [Ser, Kapitel VII, Par.1, Th.1]. □

2.2.2 Die Residuenformel

Nun sind wir soweit, die zentrale Formel für Modulformen aufzustellen. Aus ihr wird sich dann automatisch viel über die Struktur der Modulformen ergeben. Ich werde dabei im Wesentlichen dem Buch von Serre ([Ser]) folgen, ohne dabei die technischen Details auszuführen. Diese kann der Leser bei Bedarf in obigem Buch nachlesen.

2.2.2 Bezeichnungen. Sei f eine modulare Funktion auf $\mathbb{H}_\infty$, nicht identisch verschwindend. Sei p ein Punkt aus $\mathbb{H}_\infty$. Wir bezeichnen mit $v_p(f)$ die ORDNUNG VON f IN p (also $v_p(f) = n$, wenn f eine n-fache Nullstelle in p hat, und $v_p(f) = -n$, wenn f eine n-fache Polstelle in p hat). Aufgrund der Funktionalgleichungen von f ist für jedes $g \in G$ die Ordnung an den Stellen

p und gp gleich.
Ist p eine Spitze, so bezeichnet $v_p(f)$ die Ordnung der Funktion $f(q)$ mit $q = e^{2\pi iz}$ an der entsprechenden Stelle (also ist zum Beispiel $v_\infty(f)$ die Ordnung von $f(q)$ an der Stelle 0).
Weiter sei e_p die Mächtigkeit des Stabilisators von p unter G. Diese wurde in 2.2.1*(iii)* explizit für $p \in \mathbb{H}$ angegeben. Ist p dagegen eine Spitze, so gilt $e_p = 1$.

2.2.3 Satz. *Sei $f \neq 0$ eine Modulform vom Gewicht k. Dann gilt die* RESIDUENFORMEL*:*

$$\sum_{p \in (\mathbb{H}_\infty/G)} \frac{v_p(f)}{e_p} = \frac{k}{12}.$$

Beweis. Zunächst einmal ist $\mathbb{H}_\infty/G$ eine kompakte Riemannsche Fläche, daher verschwinden fast alle Summanden auf der linken Seite. Die Summe ist also endlich.
Um die Formel zu etablieren, schaue man sich die Funktion $\frac{f'}{f}$ an. Diese Funktion integriert man (nach z) über den Rand des Fundamentalbereiches $\mathcal{F}$. Da man eine meromorphe Funktion vorliegen hat, kann man dieses Integral über die auftretenden Residuen im Inneren ausrechnen. Diese ergeben dann genau die in der Formel auftretenden Terme. Einen ausführlichen Beweis kann der Leser wiederum bei Serre nachlesen [Ser, Kap. VII, Par.1, Th.3]. □

2.2.4 Bemerkung. *Setzt man die Werte für e_p in die Residuenformel ein, so erhält man die etwas explizitere Formel*

$$v_{\infty(f)} + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\textit{sonstige } p \in (\mathbb{H}_\infty/G)} v_p(f) = \frac{k}{12}.$$

Aus dieser Formel lässt sich nun Einiges herauslesen. Dazu zunächst noch ein paar Bezeichnungen:

2.2.5 Definition/Proposition. *Sei $k \in \mathbb{Z}$. Wir bezeichnen den Raum aller Modulformen vom Gewicht k mit M_k.*
Der Raum aller Spitzenformen vom Gewicht k heiße M_k^0.
Offenbar ist dann die Kodimension von M_k^0 in M_k entweder 0 oder 1. Wir haben aber schon gesehen, dass für gerades $k \geq 4$ die Eisensteinreihe E_k eine Modulform vom Gewicht k, aber keine Spitzenform ist ($E_k(\infty) = 1$, siehe 2.1.8). Also ist für solches k:

$$M_k = M_k^0 \oplus \mathbb{C}E_k.$$

2.2.6 Korollar.

(i) *Es gibt keine (nicht-trivialen) Modulformen von negativem Gewicht.*

(ii) *Es ist* $M_0 = \mathbb{C}$ *(= konstante Funktionen),* $M_0^0 = \{0\}$ *und* $M_2 = \{0\}$.

(iii) *Für* $k \in \{4, 6, 8, 10\}$ *ist* M_k *eindimensional mit* $M_k = \mathbb{C}E_k$.
Für diese k *ist* $M_k^0 = \{0\}$.

Beweis.

(i) Für $k < 0$ wäre die rechte Seite unserer Residuenformel negativ. Auf der linken Seite stehen aber nur nicht-negative Terme, da f als Modulform keine Pole hat. Also kann kein f diese Gleichung erfüllen.

(ii) Sei $f \in M_0 \backslash \{0\}$. Da auf der rechten Seite der Residuengleichung eine 0 steht, müssen auch auf der linken Seite alle Summanden verschwinden (negative Terme tauchen wieder nicht auf). Also hat f keine Nullstellen. Eine holomorphe Funktion ohne Nullstellen ist aber konstant. Also ist $f \in \mathbb{C}$ und $f \notin M_0^0$.
Nehmen wir nun an, es gäbe ein $f \in M_2 \backslash \{0\}$. Dann stünde auf der rechten Seite der Residuengleichung $\frac{1}{6}$. Damit kann aber kein Summand auf der linken Seite $\neq 0$ sein, denn jeder dieser Summanden wäre schon größer als $\frac{1}{6}$. Die Gleichung ist also nicht erfüllbar, im Widerspruch zur Annahme.

(iii) Wir beweisen diese Aussage exemplarisch für $k = 4$. Sei also $f \in M_4 \backslash \{0\}$. Dann steht auf der rechten Seite der Residuengleichung $\frac{1}{3}$. Damit die Gleichung erfüllt sein kann, muss daher $v_\rho(f) = 1$ sein und alle anderen Terme müssen verschwinden. f hat also eine einfache Nullstelle in ρ (genauer: in ρ und allen seinen Translaten unter G), und nirgendwo sonst. Dies trifft auf alle Elemente aus M_4 zu, also auch auf E_4. Damit ist auch $\frac{f}{E_4}$ eine holomorphe Funktion, und zwar wieder eine Modulform vom Gewicht 0. Nach Punkt (ii) muss dieser Quotient daher konstant sein, $\frac{f}{E_4} \equiv c$ bzw. $f = cE_4$ für ein $c \in \mathbb{C}$. Wir haben somit bewiesen, dass $M_4 = \mathbb{C}E_4$ ist. Wegen $E_4(\infty) = 1$ folgt $M_4^0 = \{0\}$.
Analog überlegt man sich die Behauptung für die anderen k. Es ergibt sich dabei, dass E_6 genau eine einfache Nullstelle in i hat, E_8 genau eine doppelte Nullstelle in ρ und E_{10} jeweils eine einfache Nullstelle in i und in ρ.

$\square$

2.2.7 Korollar.

(i) Die Funktion Δ (vgl. 2.1.8) ist nichttrivial, und sie hat außer in den Spitzen keine Nullstellen. Die Nullstelle in den Spitzen ist einfach.

(ii) Für $k \geq 0$ wird durch Multiplikation mit Δ ein Isomorphismus zwischen M_k und M^0_{k+12} definiert.
Insbesondere ist $M_{k+12} = \Delta M_k \oplus \mathbb{C}E_{k+12}$ und somit $\dim(M_{k+12}) = \dim(M_k) + 1$.

Beweis.

(i) Wir wissen bereits, dass $\Delta = \frac{1}{1728}\left((E_4)^3 - (E_6)^2\right)$ eine Modulform vom Gewicht 12 ist. Wegen $E_4(i) \neq 0$ und $E_6(i) = 0$ ist $\Delta(i) \neq 0$. Damit ist Δ nichttrivial und unsere Residuenformel anwendbar.
Bei dieser steht rechts eine 1, und wir wissen bereits, dass Δ in ∞ eine Nullstelle hat, also $v_\infty(\Delta) \geq 1$ ist. Damit die Gleichung erfüllt werden kann, muss schon $v_\infty(\Delta) = 1$ sein, und Δ darf keine weiteren Nulstellen haben.

(ii) Es ist klar, dass die Multiplikation mit Δ einen Homomorphismus definiert. Ist jedoch ein $f \in M^0_{k+12}$ gegeben, so ist wegen (i) auch die Funktion $\frac{f}{\Delta}$ eine holomorphe Funktion, mithin ein Element von M_k. Also ist auch die Umkehrabbildung (Division durch Δ) wohldefiniert. Die beiden Mengen sind also in der gewünschten Weise isomorph. Der zweite Teil der Aussage ist klar, da $M_k = M^0_k \oplus \mathbb{C}E_k$ für alle $k \geq 4$ gilt.

□

Wir können die obige Rekursionsformel für $\dim(M_k)$ natürlich auch in eine explizite Formel verwandeln:

2.2.8 Korollar. *Für gerades $k \geq 0$ gilt:*

$$\dim M_k = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor & \text{, falls } k \equiv 2 \mod 12 \\ \left\lfloor \frac{k}{12} \right\rfloor + 1 & \text{, sonst.} \end{cases}$$

Dabei bezeichnet $\lfloor x \rfloor$ den ganzzahligen Anteil von x.

Beweis. Vollständige Induktion. □

Aus den oben angestellten Überlegungen erhält man schließlich eine vollständige Charakterisierung der Modulformen:

2.2.9 Satz. *Sei* $M = \bigoplus_{k \in 2\mathbb{N}} M_k$ *die graduierte Algebra der* M_k*. Dann ist* $M \cong \mathbb{C}[E_4, E_6]$.
Anders ausgedrückt: Für alle $k \geq 0$*,* k *gerade, ist die Menge*

$$\{E_4^\alpha E_6^\beta \,|\, \alpha,\, \beta \in \mathbb{N}_0 \textit{ und } 4\alpha + 6\beta = k\}$$

eine Basis von M_k.

Beweis. Wir zeigen, dass die obigen Monome ein linear unabhängiges Erzeugendensystem darstellen.
Erzeugendensystem (durch vollständige Induktion):
Die Aussage wurde für $k \leq 6$ schon in 2.2.6 gezeigt.
Sei also $k > 6$ und $f \in M_k$ gegeben. Wähle ein Paar $(\alpha_0,\, \beta_0)$ mit $\alpha_0 + \beta_0 = k$ (solch ein Paar existiert immer für gerades $k \geq 4$). Dann ist $g := E_4^{\alpha_0} E_6^{\beta_0} \in M_k$. Folglich ist auch $f - f(\infty)g \in M_k$ und diese Funktion erfüllt außerdem

$$(f - f(\infty) \cdot g)(\infty) = f(\infty) - f(\infty) \cdot \underbrace{g(\infty)}_{=1} = 0.$$

Demnach ist $f - f(\infty) \cdot g$ sogar eine Spitzenform, und wegen 2.2.7 muss daher $f - f(\infty) \cdot g = \Delta \cdot h$ sein, für ein $h \in M_{k-12}$. Nun lässt sich h aber nach Induktionsvoraussetzung als Polynom in E_4 und E_6 ausdrücken; ebenso sind g und Δ trivialerweise Polynome in E_4 und E_6, und somit ist auch $f = f(\infty) \cdot g + \Delta \cdot h$ ein Polynom in E_4 und E_6.
Lineare Unabhängigkeit:
Wir nehmen an, die Monome wären linear abhängig, d.h. es würden nichttriviale $\lambda_i \in \mathbb{C}$ existieren mit

$$\sum_{i=0}^{n} \lambda_i E_4^{\alpha_i} E_6^{\beta_i} = 0,$$

wobei jeweils $4\alpha_i + 6\beta_i = k$ ist. Schauen wir uns zunächst die Paare $(\alpha_i,\, \beta_i)$ genauer an. Sei dazu o.B.d.A. $(\alpha_0,\, \beta_0)$ dasjenige Paar mit dem kleinsten α. Dann haben alle anderen Paare die Form $(\alpha_0 + 3m,\, \beta_0 - 2m)$ für ein geeignetes $m \in \mathbb{N}$. Durch eventuelles Umnummerieren können wir erreichen, dass jeweils $\alpha_i = \alpha_0 + 3i$ und $\beta_i = \beta_0 - 2i$ ist. Wir haben also

$$\sum_{i=0}^{n} \lambda_i E_4^{\alpha_0 + 3i} E_6^{\beta_0 - 2i} = 0.$$

Dann multiplizieren wir die Summe mit $E_4^{-\alpha_0} E_6^{-\beta_0}$ und erhalten:

$$\begin{aligned} 0 &= \sum_i \lambda_i E_4^{3i} E_6^{-2i} \\ &= \sum_i \lambda_i \frac{E_4^{3i}}{E_6^{2i}} \\ &= \sum_i \lambda_i \left(\frac{E_4^3}{E_6^2} \right)^i . \end{aligned}$$

Die meromorphe Funktion $\frac{E_4^3}{E_6^2}$ erfüllt also eine nichttriviale polynomiale Gleichung mit Koeffizienten aus $\mathbb{C}$. Dies impliziert aber bereits, dass diese Funktion konstant sein muss. Dies wiederum ist ein Widerspruch zu der Tatsache, dass sie einen Pol im Punkt ρ hat. (Denn $E_4(\rho) \neq 0$ und $E_6(\rho) = 0$). Also muss die Annahme falsch gewesen sein; die Monome $E_4^\alpha E_6^\beta$ sind linear unabhängig. □

Wir sind nun fast soweit, dass wir zu den eigentlichen Objekten unseres Interesses, den Polynomen ϕ_k, vorstoßen können. Bisher können wir immerhin schon einmal folgendes festhalten: Ist eine Eisensteinreihe E_k gegeben, so können wir ein Polynom Φ_k in zwei Variablen angeben, sodass $E_k = \Phi_k(E_4, E_6)$ ist. Wir können E_k also durch Angabe endlich vieler Koeffizienten beschreiben. Im folgenden Abschnitt werden wir noch eine weitere Vereinfachung vornehmen, durch die wir sogar mit einem Polynom in nur einer Variablen auskommen. Hierzu müssen wir jedoch erst eine neue Funktion einführen.

2.3 Die j-Variable

2.3.1 Definition. *Setze* $j := \frac{E_4^3}{\Delta}$.
Dann ist j offenbar eine modulare Funktion vom Gewicht 0. *Das heißt insbesondere, dass j invariant ist unter der Operation von G. Daher wird j manchmal auch als* MODULARE INVARIANTE *bezeichnet. Desweiteren ist j holomorph auf $\mathbb{H}$ und hat einen einfachen Pol in ∞.*

Wir werden im Folgenden j häufig wie eine Variable behandeln (im Sinne der Vereinbarung 2.1.4, d.h.: Mit $f(j)$ bezeichnen wir diejenige Funktion $\tilde{f}$, für die $f(z) = \tilde{f}(j(z))$ gilt.)

2.3.2 Proposition. *(i) j definiert eine Bijektion zwischen $\mathbb{H}_\infty/G$ und $\overline{\mathbb{C}}$.*

(ii) Sei f eine modulare Funktion vom Gewicht 0. Dann ist f eine rationale Funktion in j, d.h. es gibt eine rationale Funktion $R = \frac{P}{Q}$ (wobei P und Q Polynome sind) mit $f = R(j)$.

Beweis. (i) Es ist klar, dass j nur den Punkt $\infty \in \mathbb{H}_\infty/G$ auf $\infty \in \overline{\mathbb{C}}$ abbildet.
Wir müssen also noch zeigen, dass für jedes $\lambda \in \mathbb{C}$ das Urbild $j^{-1}(\lambda)$ aus genau einem Punkt besteht. Mit anderen Worten, wir müssen zeigen, dass für gegebenes λ die Gleichung

$$\lambda = j(z) = \left(\frac{E_4^3}{\Delta}\right)(z)$$

genau eine Lösung $z \in \mathbb{H}/G$ hat.
Diese Gleichung lässt sich aber umformen in

$$\left(E_4^3 - \lambda\Delta\right)(z) = 0.$$

Wir müssen uns also nur überlegen, dass die Funktion $(E_4^3 - \lambda\Delta)$ genau eine Nullstelle in $\mathbb{H}$ hat. Bei dieser Funktion handelt es sich aber um eine Modulform vom Gewicht 12, sodass die Residuenformel hier anwendbar ist. Da wir außerdem wissen, dass $E_4(\infty) = 1$ und $\Delta(\infty) = 0$ ist, hat unsere Funktion keine Nullstelle im Punkt ∞. Die Residuenformel lautet daher in unserem Fall:

$$\frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\text{sonstige } p\in(\mathbb{H}/G)} v_p(f) = 1.$$

Man sieht sofort, dass nur ein einziger Summand $\neq 0$ sein kann, nämlich entweder $v_i = 2$ oder $v_\rho = 3$ oder $v_p = 1$ für ein sonstiges p.
Damit hat unsere Funktion also tatsächlich genau eine Nullstelle in $\mathbb{H}/G$, und die Behauptung ist bewiesen.

(ii) Diese Aussage ist klar, wenn man die Funktionentheorie mit dem Satz zitiert, dass die einzigen meromorphen Funktionen auf der Riemannschen Zahlkugel $\overline{\mathbb{C}}$ die rationalen Funktionen sind.
Wem jedoch ein elementarer (und konstruktiver) Beweis lieber ist, der findet ihn zum Beispiel bei Serre, [Ser, Ch. VII, Par. 3, Prop. 6].

□

2.3.3 Bemerkung. • *Wir haben schon früher angedeutet, dass $\mathbb{H}_\infty/G$ eine kompakte Riemannsche Fläche ist, den Beweis für diese Tatsache aber unterschlagen. Mit Hilfe der j-Funktion wird diese Tatsache endlich offensichtlich, denn man kann die (meromorphe) j-Funktion natürlich auch als holomorphe Funktion zwischen den beiden Riemannschen Flächen $\mathbb{H}_\infty/G$ und $\overline{\mathbb{C}}$ auffassen.*

- *Man kann das Urbild der reellen Zahlen unter j genau angeben: Es handelt sich um den Bereich*

$$\{z \in \mathcal{F}|\ \Re(z) = 0\} \cup \{z \in \mathcal{F}|\ |z| = 1\} \cup \{z \in \mathcal{F}|\ \Re(z) = \frac{1}{2}\}$$

(bzw. um die Restklassen dieser Punkte unter der Operation von G). Insbesondere wird also der Rand des Fundamentalbereiches $\mathcal{F}$ in die reellen Zahlen abgebildet. Weiter gilt $j(\rho) = 0$ und $j(i) = 1728$, sodass die Menge $\{z \in \mathbb{H}/G|\ |z| = 1\}$ bijektiv auf das Intervall $[0, 1728]$ abgebildet wird.
Diese Aussagen kann man mit vertretbarem Rechenaufwand überprüfen, sobald man die arithmetischen Aussagen über die Funktionen j und Δ aus dem nächsten Kapitel zur Verfügung hat. Ich werde trotzdem in dieser Arbeit auf einen Beweis verzichten, weil ich (zumindest bei meinem Ansatz) keine strukturellen Zusammenhänge in den Rechnungen gefunden habe.

2.4 Die Eisensteinpolynome ϕ_k

Wie können wir nun die j-Funktion benutzen, um unsere Eisensteinreihen E_k zu beschreiben? Nun, gehen wir zunächst einmal davon aus, dass k durch 12 teilbar ist, $k = 12k'$. Dann hat $\Delta^{k'}$ das selbe Gewicht wie E_k, und somit ist $\frac{E_k}{\Delta^{k'}}$ eine modulare Funktion vom Gewicht 0. Wir können sie daher als rationale Funktion $R(j)$ schreiben.
Ich behaupte nun, dass bei dieser rationalen Funktion kein Nenner auftreten kann. Gäbe es nämlich einen Faktor $j(z) - \lambda$ im Nenner von R, so hätte R einen Pol an der Stelle $z = j^{-1}(\lambda) \in \mathbb{C}$. Aber der einzige Pol der Funktion $\frac{E_k}{\Delta^{k'}}$ liegt im Punkt ∞ (ein k'-facher Pol). Also muss der Nenner von R trivial sein; R ist also in Wahrheit sogar ein Polynom.
Man beachte auch, dass wir bei obiger Argumentation nur eine einzige Eigenschaft der Reihe E_k verwendet haben, nämlich dass es sich um eine Modulform handelt. Wir können diese Vorgehensweise daher auf alle Modulformen vom Gewicht $k \equiv 0 \mod 12$ übertragen.
Ist k dagegen nicht durch 12 teilbar, so müssen wir, bevor wir durch eine Potenz von Δ teilen, erst noch in geeigneter Form E_4 bzw. E_6 herausdividieren, sodass der Rest dann ein durch 12 teilbares Gewicht hat.
Im Einzelnen sieht das folgendermaßen aus:

2.4.1 Definition/Proposition. *Sei $k \in 2\mathbb{N}$, $k \geq 4$ und f eine Modulform vom Gewicht k. Dann gibt es genau ein Polynom ϕ, sodass*

$$f = \phi(j)\Delta^{n(k)} E_4^{\alpha(k)} E_6^{\beta(k)}$$

gilt, wobei $n(k)$, $\alpha(k)$ und $\beta(k)$ über die folgende Tabelle definiert sind:

$k \mod 12$	$n(k)$	$\alpha(k)$	$\beta(k)$
0	$\frac{k}{12}$	0	0
2	$\lfloor \frac{k}{12} \rfloor - 1$	2	1
4	$\lfloor \frac{k}{12} \rfloor$	1	0
6	$\lfloor \frac{k}{12} \rfloor$	0	1
8	$\lfloor \frac{k}{12} \rfloor$	2	0
10	$\lfloor \frac{k}{12} \rfloor$	1	1

Dabei muss natürlich immer $12n(k) + 4\alpha(k) + 6\beta(k) = k$ sein, damit die Gewichte in der Formel auf beiden Seiten übereinstimmen.
Diese Aussage gilt insbesondere auch für die Eisensteinreihen E_k. Das zu E_k gehörende Polynom werden wir in Zukunft als DAS k-TE EISENSTEINPOLYNOM *ϕ_k bezeichnen.*
Das heißt, es gilt immer

$$E_k = \phi_k(j)\Delta^{n(k)}E_4^{\alpha(k)}E_6^{\beta(k)}.$$

Beweis. Die Eindeutigkeit der Polynome ϕ_k ist eine direkte Konsequenz aus der Tatsache $M \cong \mathbb{C}[E_4, E_6]$ (Satz 2.2.9), denn könnte man eine Modulform auf zwei verschiedene Weisen in obiger Form schreiben, so erhielte man sofort eine nichttriviale polynomiale Gleichung zwischen E_4 und E_6.
Wir brauchen uns also nur noch um die Existenz der ϕ_k zu kümmern. Für $k \equiv 0 \mod 12$ haben wir schon gezeigt, dass es ein solches Polynom gibt. Wir werden die Existenz vpn ϕ_k noch exemplarisch im Falle $k \equiv 4 \mod 12$ beweisen.
Sei also $k \equiv 4 \mod 12$. Die Modulform f hat das Gewicht k, erfüllt also die

Residuenformel

$$\frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\text{sonstige } p \in (\mathbb{H}_\infty/G)} v_p(f) = \frac{k}{12}.$$

Dabei ist $\frac{k}{12} = n + \frac{1}{3}$ für ein $n \in \mathbb{N}$. Man sieht sofort, dass die Gleichung nur lösbar ist, falls $v_\rho(f) \geq 1$ ist. Also hat f eine Nullstelle in ρ. Deswegen ist aber auch $f' := \frac{f}{E_4}$ holomorph, also eine Modulform vom Gewicht $k-4$ (denn die einzige, einfache Nullstelle von E_4 liegt gerade in ρ). Nun ist $k-4$ aber durch 12 teilbar, daher sind wir mit der Funktion f' in einer Situation, für die wir die Aussage schon bewiesen haben. Wir können also f' schreiben als $\phi(j)\Delta^{\frac{k-4}{12}}$. Also ist

$$f = \phi(j)\Delta^{\frac{k-4}{12}}E_4.$$

Wegen $n(k) = \frac{k-4}{12}$, $\alpha(k) = 1$ und $\beta(k) = 0$ ist dies die Behauptung.
Für andere k verfährt man analog. $\square$

2.4.2 Bemerkung. *Zwei Eigenschaften der ϕ_k sind sofort offensichtlich:*

- *Alle Eisensteinpolynome sind normiert, haben also Leitkoeffizienten* 1.
- *Der Grad von ϕ_k ist $n(k)$.*

Wir werden später noch intensiver auf die Eisensteinpolynome eingehen. Vor allem zwei Punkte werden dabei im Fokus stehen:
- Welche arithmetischen Eigenschaften haben die Eisensteinpolynome?
- Wie lassen sie sich effizient berechnen?

Damit ist natürlich untrennbar die Frage nach der Arithmetik der Eisensteinreihen verbunden. Im folgenden Kapitel werden wir uns daher die E_k von einem arithmetischen Standpunkt aus genauer ansehen.

Kapitel 3

Darstellungen wichtiger Modulformen

Zunächst einmal scheint die Frage nach der Arithmetik der Eisensteinreihen und -polynome etwas verwegen zu sein: Beide haben ja zunächst reelle Koeffizienten, es ist also a priori gar kein rechnerischer Zusammenhang zwischen verschiedenen solcher Reihen bzw. Polynome zu erwarten. In diesem Abschnitt werden wir aber feststellen, dass die Koeffizienten nicht nur in $\mathbb{R}$, sondern in $\mathbb{Q}$ und sogar fast in $\mathbb{Z}$ liegen, wenn man sie unter dem richtigen Blickwinkel betrachtet.

3.1 Die q-Entwicklung der Eisensteinreihen

Wir wissen bereits aus 2.1.4, dass wir jede Modulform auch in der Variable $q = e^{2\pi iz}$ darstellen können. Dies gilt also insbesondere für die Eisensteinreihen. Die explizite Angabe der Funktion $E_k(q)$ kann auf verschiedene Arten geschehen, als besonders hübsch stellt sich jedoch die Taylorentwicklung um den Punkt $q = 0$ heraus. Da dieser Punkt der Stelle $z = \infty$ entspricht, spricht man auch von der Entwicklung der Funktion $E_k(z)$ um den Punkt ∞.

Zunächst führen wir zur Vereinfachung der Formeln noch eine (Standard-) Notation ein:

3.1.1 Bezeichnung. Seien $k, n \in \mathbb{N}$, $n \geq 1$. Mit $\sigma_k(n)$ bezeichnen wir die k-te Teilersumme von n, d.h. die Summe der k-ten Potenzen der positiven Teiler von n:

$$\sigma_k(n) := \sum_{d|n,\ d>0} d^k.$$

Um eine Formel für die q-Entwicklung der E_k aufstellen zu können, benötigen wir noch eine Hilfsformel, die wir mit dem folgenden Lemma bereitstellen:

3.1.2 Lemma. *Für alle $k \geq 2$ gilt:*

$$\sum_{k \in \mathbb{Z}} \frac{1}{(z+m)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n. \tag{3.1}$$

Beweis. Einem Beweis aus [Lan] folgend, starten wir mit der trigonometrischen Formel:

$$\frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right) = \pi \cot(\pi z). \tag{3.2}$$

Man beachte, dass die Summe auf der linken Seite fast die gewünschte Reihe $\sum_{k \in \mathbb{Z}} \frac{1}{(m+z)^k}$ für $k = 1$ ist. Da man jedoch bei dieser Reihe keine absolute Konvergenz hat, macht die Formel nur dann Sinn, wenn man die Summanden in der „richtigen“ Reihenfolge aufsummiert. Genau dies wird mit der obigen Formel (3.2) getan. Tatsächlich hat man in dieser Form der Summation die gewünschte absolute Konvergenz, welche die nun folgenden Schritte erst legitimiert. Die Formel kann im Übrigen in den meisten Formelsammlungen nachgelesen werden, zum Beispiel in [Jef, Par.2.4: „Trigonometric Identities.“].
Es ist nun ein Leichtes, die rechte Seite von Formel (3.2) in eine brauchbare Form zu bringen:

$$\begin{aligned}
\pi \cot(\pi z) &= \pi \frac{\cos(\pi z)}{\sin(\pi z)} \\
&= \pi \frac{\frac{e^{i\pi z/2} + e^{-i\pi z/2}}{2}}{\frac{e^{i\pi z/2} - e^{-i\pi z/2}}{2i}} \\
&= \pi i \frac{e^{i\pi z} + 1}{e^{i\pi z} - 1} \\
&= \pi i \frac{q+1}{q-1} \\
&= \pi i - 2\pi i \frac{1}{1-q} \\
&= \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.
\end{aligned}$$

Insgesamt erhalten wir also

$$\frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

Um von dem Summanden $\frac{1}{z+m}$ zu $\left(\frac{1}{z+m}\right)^k$ zu kommen, benutzt man nun einen Standardtrick: Man differenziert beide Seiten $(k-1)$-mal nach z. Man beachte, dass man hier die absolute Konvergenz der Reihe benutzt, um Differenziation und Reihenbildung vertauschen zu dürfen.
Man muss beim Differenzieren natürlich berücksichtigen, dass man eine innere Ableitung erhält:

$$\frac{d}{dz} = \frac{dq}{dz}\frac{d}{dq} = \frac{d(e^{2\pi iz})}{dz}\frac{d}{dq} = 2\pi i e^{2\pi iz}\frac{d}{dq} = 2\pi i q\frac{d}{dq}.$$

Wir bekommen daher die Formel

$$\frac{d}{dz}\left(\sum_{n=0}^{\infty} q^n\right) = 2\pi i\sum_{n=1}^{\infty} nq^n,$$

welche sich induktiv fortsetzt zu

$$\frac{d^k}{dz^k}\left(\sum_{n=0}^{\infty} q^n\right) = (2\pi i)^k\sum_{n=1}^{\infty} n^k q^n.$$

Sollte der Leser im Übergang zwischen verschiedenen Variablen noch ungeübt sein, so empfiehlt es sich, die Variable q tatsächlich als bloße Abkürzung zu interpretieren und q in jeder auftretenden Formel durch den Ausdruck $e^{2\pi iz}$ zu ersetzen.
Mit der obigen Umrechnung ergibt sich nun:

$$\begin{aligned}
&(-1)^{k-1}\left(\frac{1}{z^k} + \sum_{m=1}^{\infty}\left(\frac{1}{(z+m)^k} + \frac{1}{(z-m)^k}\right)\right) \\
&\qquad = \frac{d^{k-1}}{dz^{k-1}}\left(\frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right)\right) \\
&\qquad = \frac{d^{k-1}}{dz^{k-1}}\left(\pi i - 2\pi i\sum_{n=0}^{\infty} q^n\right) \\
&\qquad = -2\pi i(2\pi i)^{k-1}\sum_{n=1}^{\infty} n^{k-1}q^n.
\end{aligned}$$

Da es sich bei $\frac{1}{z^k} + \sum_{m=1}^{\infty}\left(\frac{1}{(z+m)^k} + \frac{1}{(z-m)^k}\right)$ um eine absolut konvergente Reihe handelt, darf man diese auch als $\sum_{m\in\mathbb{Z}}\frac{1}{(z+m)^k}$ schreiben.
Fasst man außerdem noch die Vorfaktoren zusammen, so ergibt sich wie behauptet Formel (3.1). $\square$

Nun sind wir soweit, die q-Entwicklung der E_k angeben zu können:

3.1.3 Proposition. *Sei $k \geq 4$ gerade. Für die k-te Eisensteinreihe E_k gilt:*

$$E_k(z) = 1 + \frac{(2\pi i)^k}{(k-1)!\zeta(k)} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Beweis. Betrachten wir der Übersichtlichkeit halber die Reihe

$$G_k(z) := 2\zeta(k) E_k(z) = \sum_{(n,m)\in\mathbb{Z}^2}{}' \frac{1}{(nz+m)^k}.$$

Wir können die Summe G_k in Teilsummen für $n = 0$, $n < 0$ und $n > 0$ aufspalten:

$$\begin{aligned} G_k(z) &= \sum_{(n,m)\in\mathbb{Z}^2}{}' \frac{1}{(nz+m)^k} \\ &= \sum_{m\in\mathbb{Z}}{}' \frac{1}{m^k} + \sum_{n=1}^{\infty} \sum_{m\in\mathbb{Z}} \frac{1}{(nz+m)^k} + \sum_{n=-1}^{-\infty} \sum_{m\in\mathbb{Z}} \frac{1}{(nz+m)^k} \\ &= 2\zeta(k) + 2\sum_{n=1}^{\infty} \sum_{m\in\mathbb{Z}} \frac{1}{(nz+m)^k}. \end{aligned}$$

Wir wollen nun Formel (3.1) anwenden. Dazu müssen wir nz anstelle von z einsetzen. Da auf der rechten Seite von Formel (3.1) ein $q = e^{2\pi i z}$ auftaucht, müssen wir entsprechend anstatt q den Wert $q^n = e^{2\pi i(nz)}$ einsetzen:

$$\begin{aligned} G_k(z) &= 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sum_{d=1}^{\infty} d^{k-1} (q^n)^d \\ &= 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!} \sum_{d=1}^{\infty} \sum_{n=1}^{\infty} d^{k-1} q^{nd}. \end{aligned}$$

Nun wollen wir die Summanden nach den Potenzen von q sortieren. Dazu müssen wir die Frage stellen: Ist ein $N \in \mathbb{N}$ gegeben, wann (und mit welchem Vorfaktor) taucht dann der Ausdruck q^N auf?
Die Antwort ist natürlich: Wir erhalten immer dann einen Summanden mit q^N, wenn d ein Teiler von N ist. Der Vorfaktor ist in diesem Fall einfach d^{k-1}.
Es gilt daher:

$$G_k(z) = 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!} \sum_{N=1}^{\infty} \underbrace{\sum_{d|N} d^{k-1}}_{\sigma_{k-1}(N)} q^N.$$

Dividiert man nun noch beide Seiten durch $2\zeta(k)$, so erhält man die behauptete Formel. $\square$

Diese Gleichung lässt sich nun in der Tat noch verbessern. In 7.2 wird ein Zusammenhang zwischen den Werten der Riemannschen ζ-Funktion und den Bernoullizahlen B_k hergestellt, nämlich $\zeta(k) = (-1)^{\frac{k}{2}-1} \cdot \frac{2^{k-1}}{k!} \pi^k B_k$ für gerades $k > 1$. Verwendet man diesen Zusammenhang, so erhält man die endgültige Formel:

3.1.4 Satz. *Sei $k \geq 4$ gerade. Dann gilt:*

$$E_k(z) = 1 + \frac{-2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Beweis. Einsetzen. $\square$

Diese Formel ist gleich in mehrerer Hinsicht bemerkenswert. Zunächst einmal liefert sie eine effiziente Methode, die Eisensteinreihen zu berechnen. Zum Beispiel hat man

$$\begin{aligned}
E_4 &= 1 + 240q + 2160q^2 + 6720q^3 + \ldots \\
E_6 &= 1 - 504q - 16632q^2 - 122976q^3 + \ldots \\
E_8 &= 1 + 480q + 61920q^2 + 1050240q^3 + \ldots \\
E_{10} &= 1 - 264q - 135432q^2 - 5196576q^3 + \ldots \\
E_{12} &= 1 + \frac{65520}{691} q + \frac{134250480}{691} q^2 + \frac{11606736960}{691} q^3 + \ldots
\end{aligned}$$

Wir wollen einige der wichtigsten Konsequenzen in den nun folgenden Korollaren zusammenfassen.

3.1.5 Korollar. *Die q-Entwicklung der Eisensteinreihe E_k hat rationale Koeffizienten.*
Die Nenner der Koeffizienten (zu einem fest vorgegebenen k) sind beschränkt durch den Zähler des Bruches $\frac{B_k}{2k}$. Dieser tritt auch tatsächlich als Nenner auf, da die Eisensteinreihe mit $E_k(q) = 1 + \frac{2k}{B_k} q + O(q^2)$ beginnt.

3.1.6 Korollar. *Die Koeffizienten der q-Entwicklung von E_k wachsen mit der Geschwindigkeit $O(\sigma_{k-1}(n)) = O(n^{k-1})$.*

Beweis. An dieser Aussage ist nur beweisbedürftig, dass $\sigma_{k-1}(n) \in O(n^{k-1})$ ist. Dies wird anhand der folgenden Abschätzung deutlich:

$$\begin{aligned}
\sigma_{k-1}(n) &= \sum_{d|n} d^{k-1} \\
&\leq n^{k-1} + \left(\frac{n}{2}\right)^{k-1} + \left(\frac{n}{3}\right)^{k-1} + \left(\frac{n}{4}\right)^{k-1} + \dots \\
&= n^{k-1} \underbrace{\sum_{j=1}^{\infty} \frac{1}{j^{k-1}}}_{=:C<\infty} \\
&= Cn^{k-1}.
\end{aligned}$$

Diese Abschätzung gilt, sofern $k > 2$ ist (damit $C < \infty$ ist). □

An dieser Stelle möchte ich kurz erwähnen, dass es eine sehr viel allgemeinere, analoge Aussage über Spitzenformen gibt, die als RAMANUJAN-PETERSSON-VERMUTUNG bekannt ist. Diese ist inzwischen als Folgerung aus der WEIL-VERMUTUNG bewiesen. In einer ihrer Formulierungen besagt sie:

3.1.7 Satz (Ramanujan-Petersson). *Ist a_n der n-te Koeffizient in der q-Entwicklung einer (normierten) Spitzenform vom Gewicht k, so gilt für alle $\epsilon > 0$*

$$|a_n| \in O(n^{\frac{k-1}{2}+\epsilon}).$$

3.2 q-Entwicklung der Δ-Funktion

Ziel dieses Abschnittes ist es, die q-Entwicklung der Δ-Funktion zu beweisen:

3.2.1 Satz (Jacobi). *Es gilt* $\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$.

Es gibt hierzu zwei verschiedene Ansätze:
Wir wissen bereits, dass der Raum der Spitzenformen vom Gewicht 12 eindimensional ist. Wenn wir beweisen können, dass sowohl Δ als auch das angegebene Produkt in diesem Raum liegen (und von Δ ist dies aufgrund der Definition klar), dann müssen die beiden Funktionen schon proportional zueinander sein. Es ist dann ein Leichtes, sich zu überlegen, dass der Proportionalitätsfaktor tatsächlich 1 ist, dass also die beiden Funktionen übereinstimmen.
Diese Vorgehensweise ist wohl am Elementarsten, und meines Wissens auch

die historisch ursprüngliche. Sie hat jedoch den großen Nachteil, dass die obige Formel vom Himmel fällt. Ich will deshalb nicht verschweigen, dass es auch eine zweite Beweismöglichkeit gibt, die dieses Problem nicht hat.
Diese beruht im Wesentlichen auf dem Zusammenhang zwischen den Eisensteinreihen und der Weierstraß'schen $\wp$-Funktion (Abschnitt 1.2). Ich habe bereits gesagt, dass man die zu einem Gitter (und damit zu einem $z \in \mathbb{H}_\infty/G$) gehörende elliptische Kurve über eine kubische Gleichung beschreiben kann (Gleichung (1.1)). Es stellt sich nun heraus, dass $\Delta(z)$ gerade die Diskriminante dieser Gleichung ist. In [Hur, Bd. I, Seite 578-595] findet der Leser eine Herleitung der obigen Gleichung, die diesen Zugang benutzt.
Wir werden uns jedoch damit begnügen, einen (allerdings recht hübschen) Beweis zu geben, der den ersten Weg beschreitet:

Beweis von Satz 3.2.1. Setze

$$F(q) := q \prod_{n=1}^{\infty} (1-q^n)^{24}.$$

Da wir die q-Entwicklung der Eisensteinreihen bereits kennen, können wir natürlich auch die ersten Terme von $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$ berechnen. Dabei wird ersichtlich, dass der Vorfaktor $\frac{1}{1728}$ genau so gewählt war, dass der erste Koeffizient in der q-Entwicklung von Δ gerade 1 ist, also $\Delta(q) = q + O(q^2)$.
Die q-Entwicklung von F fängt natürlich auch mit $F(q) = q + O(q^2)$ an. Wir brauchen daher nur noch zu zeigen, dass F eine Spitzenform vom Gewicht 12 ist. Da die Funktionen dann proportional sein müssen und im ersten Term übereinstimmen, müssen sie dann auch schon identisch sein.
Die Tatsache, dass F an der Stelle $q = 0$ (also in $z = \infty$) verschwindet, ist offensichtlich.
Wir müssen daher nur noch zeigen, dass F eine Modulform ist, d.h. dass F die beiden Gleichungen

$$F(z+1) = F(z) \tag{3.3}$$

und

$$F(-\frac{1}{z}) = z^{12} F(z) \tag{3.4}$$

erfüllt.
Die erste Gleichung ist aber trivial, da wir F über die Variable q definiert haben. Denn fasst man q als Funktion in z auf, $q = e^{2\pi i z}$, so ist $q(z) = q(z+1)$, und damit auch $F(q(z)) = F(q(z+1))$.
Es bleibt also nur noch zu zeigen, dass $F(-\frac{1}{z}) = z^{12}F(z)$ ist.
Um dies zu beweisen, benutzen wir wiederum einen Standardtrick: Wir betrachten die Ableitung der Funktionen auf der rechten und der linken Seite

und zeigen, dass diese übereinstimmen. Daraus können wir dann folgern, dass die Funktionen selbst auch bis auf eine Konstante übereinstimmen. Da wir es jedoch mit Produkten zu tun haben, benutzen wir nicht die „normale", sondern vielmehr die *logarithmische Ableitung* $\frac{1}{f}df$. Der Vorteil dieser Vorgehensweise liegt in der folgenden Tatsache:
Hat man ein Produkt $f(z) = f_1(z) \cdot f_2(z)$ gegeben und berechnet von diesem die logarithmische Ableitung, so ergibt sich

$$\begin{aligned} \frac{1}{f}df &= \frac{1}{f_1 f_2} d(f_1 f_2) \\ &= \frac{1}{f_1 f_2}(f_2 df_1 + f_1 df_2) \\ &= \frac{1}{f_1} df_1 + \frac{1}{f_2} df_2. \end{aligned}$$

Die logarithmische Ableitung verwandelt Produkte also in Summen. Man kann sich überlegen, dass diese Formel bei absoluter Konvergenz auch auf unendliche Produkte übertragbar ist, d.h. für ein unendliches Produkt $f = \prod_{n=1}^{\infty} f_n$ ist auch $\frac{1}{f}df = \sum_{n=1}^{\infty} \frac{1}{f_n} df_n$, sofern beide Seiten absolut konvergieren (wobei aus der absoluten Konvergenz der rechten Seite schon die absolute Konvergenz der linken Seite folgt, nicht jedoch umgekehrt).
Die logarithmische Ableitung hat noch einen weiteren Vorteil. Sie erlaubt, einfach zwischen den Variablen q und z zu wechseln. Es ist nämlich

$$\begin{aligned} \frac{1}{q}dq &= \frac{1}{e^{2\pi i z}} d(e^{2\pi i z}) \\ &= \frac{1}{e^{2\pi i z}} 2\pi i e^{2\pi i z} dz \\ &= 2\pi i dz. \end{aligned}$$

Mit diesem Werkzeug ausgerüstet berechnen wir zunächst die logarithmische Ableitung von F:

$$\begin{aligned} \frac{dF}{F} &= \frac{1}{q}dq + \sum_{n=1}^{\infty} 24 \frac{1}{1-q^n} d(1-q^n) \\ &= \frac{1}{q}dq + 24 \sum_{n=1}^{\infty} \frac{1}{1-q^n}(-n)q^{n-1}dq \\ &= \left(1 + 24 \sum_{n=1}^{\infty} \frac{1}{1-q^n}(-nq^n)\right) \frac{1}{q}dq \end{aligned}$$

Nun benutzen wir noch die geometrische Reihe $\frac{1}{1-q^n} = \sum_{m=0}^{\infty} q^{mn}$, um zu sehen, dass

$$\begin{aligned}\frac{dF}{F} &= \left(1-24\sum_{n=1}^{\infty}\sum_{m=0}^{\infty} nq^{n(m+1)}\right)\frac{1}{q}dq\\ &= \left(1-24\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} nq^{nm}\right)\frac{1}{q}dq\\ &= \left(1-24\sum_{n=1}^{\infty}\sigma_1(n)q^n\right)\frac{1}{q}dq,\end{aligned}$$

wobei man sich die letzte Identität wie im Beweis von 3.1.3 überlegt.
Natürlich findet hierbei eine Umordnung statt. Diese (sowie die zuvor erfolgte Vertauschung von logarithmischer Ableitung und Grenzwertbildung) wird dadurch gerechtfertigt, dass die zuletzt vorliegende Reihe absolut konvergiert. Um dies einzusehen, schätze man sie zum Beispiel gegen die Majorante $\sum_{n=1}^{\infty}(n^2q^n)$ ab (denn $\sigma_1(n) \leq n^2$ für alle n). Man beachte dabei, dass wegen $z \in \mathbb{H}$ nur solche q mit $|q| < 1$ relevant sind.
Damit können wir die rechte Seite von Gleichung (3.4) schon logarithmisch differenzieren. Es ist

$$\frac{1}{z^{12}F(z)}d(z^{12}F(z)) = 12\frac{1}{z}dz + \frac{1}{F}dF.$$

Um die linke Seite unserer Gleichung auch differenzieren zu können, müssen wir herausfinden, was die logarithmische Ableitung von $F(-\frac{1}{z})$ ist. Dazu müssten wir jedoch wissen, wie sich der Ausdruck $1-24\sum_{n=1}^{\infty}\sigma_1(n)q^n$ verändert, wenn man z durch $-\frac{1}{z}$ ersetzt. Dabei erinnert uns der Ausdruck stark an die Eisensteinreihen $E_k = 1 + \frac{-2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$ (sogar der Vorfaktor $\frac{-2\cdot 2}{B_2} = -24$ passt).
Wir erinnern uns daher daran, dass wir dieses Transformationsverhalten für die Eisensteinreihen geschenkt bekamen, und definieren deshalb mutig

$$E_2(z) := \frac{1}{2\zeta(2)}\sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}}{}' \frac{1}{(mz+n)^2}.$$

Dabei meinen wir mit $\sum'$ natürlich, dass der Summand $(m,n) = (0,0)$ weggelassen wird.
Von dieser Reihe wissen wir zunächst allerdings nicht einmal, ob sie konvergiert (indem man das Argument aus Anhang A etwas verfeinert, sieht man sehr schnell, dass sie zumindest einmal nicht *absolut* konvergiert). Aber unter der Annahme der Konvergenz können wir tatsächlich wie im Beweis zu

Proposition 3.1.3 ausrechnen, dass

$$\begin{aligned}
G_2(z) &:= \sum_{n\in\mathbb{Z}} {\sum_{m\in\mathbb{Z}}}' \frac{1}{(nz+m)^2} \\
&= {\sum_{m\in\mathbb{Z}}}' \frac{1}{m^2} + \sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}} \frac{1}{(nz+m)^2} + \sum_{n=-1}^{-\infty}\sum_{m\in\mathbb{Z}} \frac{1}{(nz+m)^2} \\
&= 2\zeta(2) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}} \frac{1}{(nz+m)^2}.
\end{aligned}$$

In Lemma 3.1.2 hatten wir nun für alle $k \geq 2$ die Formel (3.1),

$$\sum_{k\in\mathbb{Z}} \frac{1}{(z+m)^k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty} d^{k-1}q^d,$$

bewiesen, mit deren Hilfe wir nun weiterrechnen können:

$$\begin{aligned}
\sum_{n\in\mathbb{Z}} {\sum_{m\in\mathbb{Z}}}' \frac{1}{(mz+n)^2} &= 2\zeta(2) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}} \frac{1}{(nz+m)^2} \\
&= 2\zeta(2) + 2(-2\pi i)^2 \sum_{n=1}^{\infty}\sum_{d=1}^{\infty} d\,(q^n)^d \\
&= 2\zeta(2) - 8\pi^2 \sum_{d=1}^{\infty}\sum_{n=1}^{\infty} dq^{nd} \\
&= 2\zeta(2) - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n)q^n.
\end{aligned}$$

Teilt man nun beide Seiten noch durch $2\zeta(2) = \frac{\pi^2}{3}$, so folgt tatsächlich wie erhofft

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n.$$

Insbesondere sehen wir, dass $E_2(z)$ für alle $z \in \mathbb{H}$ konvergiert.

Aus der Definition von G_2 erhalten wir sofort

$$\begin{aligned}
G_2(-\frac{1}{z}) &= \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}}{}' \frac{1}{(-\frac{n}{z}+m)^2} \\
&= \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}}{}' \frac{1}{(\frac{n}{z}+m)^2} \\
&= z^2\sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}}{}' \frac{1}{(n+mz)^2} \\
&= z^2\sum_{m\in\mathbb{Z}}\sum_{n\in\mathbb{Z}}{}' \frac{1}{(nz+m)^2} \\
&=: z^2 G(z)
\end{aligned}$$

Die interessante Frage, die wir beantworten müssen, ist also: Wie unterscheiden sich die (bis auf Umordnung identischen) Reihen G und G_2 voneinander? Bisher wissen wir nichts weiter, als dass die Reihe G konvergiert.
Wir beantworten die Frage, indem wir die beiden Reihen so abändern, dass sie absolut konvergent werden. Dazu definieren wir zwei weitere Reihen

$$H_2(z) := \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}}{}' \frac{1}{(m-1+nz)(m+nz)}$$

und

$$H(z) := \sum_{m\in\mathbb{Z}}\sum_{n\in\mathbb{Z}}{}' \frac{1}{(m-1+nz)(m+nz)}.$$

Diesmal bedeutet $\sum'$, dass die Summanden $(m,n) = (0,0)$ und $(m,n) = (1,0)$ weggelassen werden.
Man kann auf recht elementarem Wege ausrechnen, dass H_2 und H konvergieren, und man kann die Werte explizit angeben; es ist nämlich $H_2(z) = 2$ und $H(z) = 2 - \frac{2\pi i}{z}$ für alle $z \in \mathbb{H}$. Die hierzu notwendigen Rechnungen habe ich in das nachfolgende Lemma 3.2.2 ausgelagert.

Fassen wir nochmal zusammen, wo wir momentan im Beweis stehen:

- Wir wollen die logarithmische Ableitung von $F(-\frac{1}{z})$ berechnen. Diese wollen wir dann mit der (schon ausgerechneten) Ableitung von $z^{12}F(z)$ vergleichen. Aus diesem Vergleich wollen wir letzlich schlussfolgern, dass die beiden Funktionen gleich sind, sodass F deshalb eine Modulform vom Gewicht 12 ist. Wir haben bereits genug über F herausgefunden, um dann zu wissen, dass F mit Δ übereinstimmen muss.

- Um die Ableitung von $F(-\frac{1}{z})$ zu berechnen, müssen wir $G_2(-\frac{1}{z})$ ausrechnen, denn es gilt $\frac{1}{F}dF = E_2\frac{1}{q}dq$. (Dabei war $G_2 = 2\zeta(2)E_2$.)

- $G_2(-\frac{1}{z})$ steht in engem Verhältnis zu $G(z)$, nämlich durch die Formel $G_2(-\frac{1}{z}) = z^2G(z)$. Wir wollen daher $G(z)$ durch $G_2(z)$ ausdrücken. G und G_2 unterscheiden sich nur durch die Summationsreihenfolge.

- Dazu haben wir zwei Reihen H_2 und H definiert, deren Werte wir explizit kennen ($H_2(z) = 2$, $H(z) = 2 - \frac{2\pi i}{z}$). Diese unterscheiden sich ebenfalls nur durch die Summationsreihenfolge.

Wir werden diese Punkte nun von hinten nach vorne abarbeiten.
Wir stellen zunächst fest, dass

$$\frac{1}{(m-1+nz)(m+nz)} - \frac{1}{(m+nz)^2} = \frac{1}{(m-1+nz)(m+nz)^2}$$

ist. Die Reihe $\sum'_{m,n\in\mathbb{Z}} \frac{1}{(m-1+nz)(m+nz)^2}$ konvergiert aber absolut (dies sieht man analog zum Beweis der Konvergenz der Eisensteinreihe in Anhang A).
Wegen

$$G_2(z) - H_2(z) = \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(m-1+nz)(m+nz)^2} = G(z) - H(z)$$

folgt nun aber, dass G und G_2 konvergieren müssen, und dass gilt:

$$G_2(z) - G(z) = H_2(z) - H(z) = 2 - (2 - \frac{2\pi i}{z}) = \frac{2\pi i}{z}.$$

Damit haben wir den Zusammenhang zwischen G_2 und G gefunden und kombinieren:

$$\begin{aligned} G_2(-\frac{1}{z}) &= z^2G_(z) \\ &= z^2\left(G_2(z) - \frac{2\pi i}{z}\right) \\ &= z^2G_2(z) - 2\pi iz. \end{aligned}$$

Dividieren wir beide Seiten durch $2\zeta(2) = \frac{\pi^2}{3}$, so wird aus G_2 wieder E_2:

$$E_2(-\frac{1}{z}) = z^2E_2(z) - \frac{6iz}{\pi}.$$

Nun können wir endlich die logarithmische Ableitung von $F(-\frac{1}{z})$ berechnen. Wir erinnern uns daran, dass $\frac{1}{F}dF = E_2\frac{1}{q}dq = E_2 2\pi i dz$ ist. Entsprechend gilt

$$\begin{aligned}
\frac{1}{F(-\frac{1}{z})}dF(-\frac{1}{z}) &= E_2(-\frac{1}{z})2\pi i d(-\frac{1}{z}) \\
&= \left(z^2E_2(z) - \frac{6iz}{\pi}\right)2\pi i\frac{1}{z^2}dz \\
&= 2\pi i E_2(z)dz + \frac{12}{z}dz.
\end{aligned}$$

Damit hat $F(-\frac{1}{z})$ tatsächlich dieselbe logarithmische Ableitung wie $z^{12}F(z)$. Die beiden Funktionen müssen deshalb proportional sein. Da aber für $z = i$ sogar $i^{12}F(i) = F(i) = F(-\frac{1}{i})$ gilt (und $F(i) \neq 0$ ist), sind die beiden Funktionen identisch.

Also erfüllt F die geforderte Gleichung und ist demzufolge eine Modulform vom Gewicht 12. Wie wir uns schon zu Beginn des Beweises überlegt haben, bleibt F nichts anderes übrig, als mit Δ übereinzustimmen. Damit ist die Behauptung (modulo des nachfolgenden Lemmas) bewiesen. □

3.2.2 Lemma. *Die Reihen H_2 und H aus dem obigen Beweis konvergieren und es ist*

$$H_2(z) = 2$$

und

$$H(z) = 2 - \frac{2\pi i}{z}$$

für alle $z \in \mathbb{H}$.

Beweis. Wenden wir uns zunächst der Reihe H_2 zu. Es ist

$$\frac{1}{(m-1+nz)(mz+n)} = \frac{1}{m-1+nz} - \frac{1}{m+nz},$$

sodass (für $n \neq 0$)

$$\sum_{m\in\mathbb{Z}}\left(\frac{1}{m-1+nz} - \frac{1}{m+nz}\right) = 0 \text{ (Teleskopsumme)}$$

und ergo

$$\begin{aligned}
H_2(z) &= \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}}{}'\left(\frac{1}{m-1+nz} - \frac{1}{m+nz}\right) \\
&= \sum_{m\in\mathbb{Z}\setminus\{0,1\}}\left(\frac{1}{m-1} - \frac{1}{m}\right) \\
&= -\frac{1}{-1} + \frac{1}{2-1} = 2 \text{ (wieder Teleskopsumme)}
\end{aligned}$$

ist.
Für H schreiben wir den Summanden ebenfalls etwas um. Es ist

$$\begin{aligned}\frac{1}{(m-1+nz)(m+nz)} &= \frac{1}{m-1+nz} - \frac{1}{m+nz} \\ &= \frac{1}{z}\left(\frac{1}{n+\frac{m-1}{z}} - \frac{1}{n+\frac{m}{z}}\right).\end{aligned}$$

Nun ist aber aus der Funktionentheorie allgemein bekannt, dass

$$\sum_{n\in\mathbb{Z}}\left(\frac{1}{n+x} - \frac{1}{n+y}\right) = \pi\cot(\pi x) - \pi\cot(\pi y)$$

ist, sofern bei der Summe alle Summanden wohldefiniert sind. (Diese Identität ist eine Anwendung des Residuensatzes. Der Leser kann sie in vielen Formelsammlungen nachlesen).
Auf unsere Situation bezogen:

$$\begin{aligned}\sum_{n\in\mathbb{Z}}\frac{1}{(m-1+nz)(m+nz)} &= \frac{1}{z}\sum_{m\in\mathbb{Z}}\left(\frac{1}{n+\frac{m-1}{z}} - \frac{1}{n+\frac{m}{z}}\right) \\ &= \frac{1}{z}\left(\pi\cot\left(\pi\frac{m-1}{z}\right) - \pi\cot\left(\pi\frac{m}{z}\right)\right),\end{aligned}$$

falls $m \notin \{0,1\}$ ist. Die beiden verbleibenden Summanden ($m = 0,\ 1$) behandelt man am besten zusammen. Man hat nämlich

$$\begin{aligned}&\sum_{n\in\mathbb{Z}\setminus\{0\}}\frac{1}{(-1+nz)(nz)} + \sum_{n\in\mathbb{Z}\setminus\{0\}}\frac{1}{(nz)(1+nz)} \\ &\qquad= \sum_{n\in\mathbb{Z}\setminus\{0\}}\left(\frac{1}{-1+nz} - \frac{1}{nz}\right) + \left(\frac{1}{nz} - \frac{1}{1+nz}\right) \\ &\qquad= \sum_{n\in\mathbb{Z}\setminus\{0\}}\left(\frac{1}{-1+nz} - \frac{1}{1+nz}\right) \\ &\qquad= 2 + \sum_{n\in\mathbb{Z}}\left(\frac{1}{-1+nz} - \frac{1}{1+nz}\right) \\ &\qquad= 2 + \frac{1}{z}\left(\pi\cot\left(\pi\frac{-1}{z}\right) - \pi\cot\left(\frac{1}{z}\right)\right).\end{aligned}$$

Also ist auch H eine teleskopierende Reihe. Es gilt

$$\sum_{m=-M_1}^{M_2}\sum_{n\in\mathbb{Z}}{}'\frac{1}{(m-1+nz)(m+nz)}$$

$$= \quad 2 + \frac{\pi}{z}\underbrace{\left(\cot\left(\pi\frac{-M_1-1}{z}\right) - \cot\left(\pi\frac{M_2}{z}\right)\right)}_{=:S(M_1,M_2)}.$$

wobei M_1 und M_2 (große) natürliche Zahlen sein sollen.
Nun kann man $H(z) = 2+\frac{\pi}{z}\lim_{M_1,M_2\to\infty} S(M_1, M_2)$ berechnen. Dazu schreibt man cot auf zwei verschiedene Weisen, nämlich als $\cot(z) = i\frac{e^{2\pi ix}+1}{e^{2\pi ix}-1}$ und als $\cot(z) = i\frac{1+e^{-2\pi ix}}{1-e^{-2\pi ix}}$. Berücksichtigt man nun noch, dass $\Im(\frac{1}{z}) > 0$ ist, so sieht man

$$\lim_{M_1\to\infty} \cot\left(\pi\frac{-M_1-1}{z}\right) = \lim_{M_1\to\infty}\left(i\cdot\frac{\overbrace{e^{2\pi i\frac{-M_1-1}{z}}}^{\to 0}+1}{\underbrace{e^{2\pi i\frac{-M_1-1}{z}}}_{\to 0}-1}\right) = -i$$

und

$$\lim_{M_2\to\infty} \cot\left(\pi\frac{M_2}{z}\right) = \lim_{M_2\to\infty}\left(i\cdot\frac{1+\overbrace{e^{-2\pi i\frac{M_2}{z}}}^{\to 0}}{1-\underbrace{e^{-2\pi i\frac{M_2}{z}}}_{\to 0}}\right) = i.$$

Damit ergibt sich insgesamt $\lim_{M_1,M_2\to\infty} S(M_1, M_2) = (i-(-i)) = 2i$, womit wir unseren Wert für H endlich gefunden haben: $H(z) = 2 + \frac{2\pi i}{z}$.

□

3.2.3 Bemerkung. *Der n-te Koeffizient der q-Entwicklung von Δ wird mit $\tau(n)$ bezeichnet. Die Funktion $n \mapsto \tau(n)$ wird auch* Ramanujan-Funktion *genannt, da Ramanujan sie zum ersten Mal eingeführt hat.*
Die Ramanujan-Funktion $\tau(n)$ ist schwach multiplikativ, *d.h. es gilt $\tau(mn) = \tau(m)\tau(n)$ für teilerfremde m, $n \in \mathbb{N}$.*
Außerdem erfüllt sie für $p \in \mathbb{P}$ und $n > 1$ die Gleichung

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}).$$

Diese und viele andere Aussagen finden sich bereits bei ihrem Namenspaten Ramanujan [Ram, S.159ff.].

Natürlich gibt es auch wieder einige unmittelbare Konsequenzen aus der Produktdarstellung von Δ. Insbesondere gilt:

3.2.4 Korollar.

(i) Die q-Entwicklung von Δ hat nur ganzzahlige Koeffizienten.

(ii) Die q-Entwicklung der j-Funktion hat nur ganzzahlige Koeffizienten.

(iii) Die Koeffizienten der Eisensteinpolynome ϕ_k sind rational. Der Nenner von ϕ_k stimmt mit dem Nenner von E_k überein und ist damit gleich dem Zähler von $\frac{B_k}{2k}$.

Beweis. (i) ist klar.

(ii) Es ist aufgrund der Definition $j = \frac{E_4^3}{\Delta}$ sofort klar, dass die Koeffizienten aus $\mathbb{Q}$ sind. Den Beweis, dass sie sogar aus $\mathbb{Z}$ sind, führt man mit Hilfe einiger der bekannten Kongruenzen für Bernoullizahlen (Abschnitt 7.2). Ich möchte hier auf die Details des Beweises verzichten.

(iii) Sei $\phi_k(x) = x^{n(k)} + a_{n(k)-1}x^{n(k)-1} + \ldots + a_0$.
Zunächst überlegen wir uns, dass der Nenner von ϕ_k schlimmstenfalls so groß wie der Nenner von E_k sein kann: Gäbe es einen Faktor λ im Nenner von ϕ_k, der im Nenner von E_k nicht vorkommt, so sei a_l der erste Koeffizient (= Koeffizient mit höchstem Index) von ϕ_k, in dem λ auftritt. (Man kann o.B.d.A. λ als Primzahlpotenz annehmen, dann muss λ auch wirklich in einem a_l auftreten.) Betrachte nun die Gleichung
$$E_k = \phi_k(j)\Delta^{n(k)}E_4^{\alpha(k)}E_6^{\beta(k)}$$
und von dieser Gleichung den Vorfaktor von $q^{n(k)-l}$. Dieser setzt sich auf der rechten Seite als Summe verschiedener Produkte zusammen. In keinem dieser Produkte kann ein Faktor a_{l-1} oder a_{l-2} oder $\ldots$ oder a_0 auftreten, denn die q-Potenz, zu der dieses Produkt gehören würde, wäre mindestens $(q^{-1})^{l-1} \cdot q^{n(k)} = q^{n(k)-l+1}$. Der Faktor a_l selbst kann nur in einem einzigen Produkt auftauchen, nämlich in dem Produkt $a_l \cdot 1^l \cdot 1 = a_l$. In allen weiteren Produkten tauchen nur die Koeffizienten $a_{n(k)}, \ldots, a_{l+1}$ sowie (ganzzahlige) Koeffizienten der Reihen j, Δ, E_4 und E_6 auf. Insgesamt hat man auf der rechten Seite also den Term $(a_l + \sum_i r_i)q^{n(k)-l}$, wobei der Nenner von r_i nicht durch λ teilbar ist. Damit kann sich aber der Faktor λ nicht herauskürzen, und der Nenner von $a_l + \sum_i r_i$ muss durch λ teilbar sein. Da aber $a_l + \sum_i r_i$ mit dem entsprechenden Koeffizienten auf der linken Seite identisch sein muss, hat einer der Koeffizienten von E_k den Faktor λ im Nenner, *Widerspruch.*
Wir müssen nun noch zeigen, dass der Nenner von $\frac{2k}{B_k}$ auch tatsächlich als Nenner von ϕ_k auftritt. Hierzu betrachten wir den linearen Term in

der Formel $E_k = \phi_k(j)\Delta^{n(k)}E_4^{\alpha(k)}E_6^{\beta(k)}$. Auf der linken Seite ist dies einfach $\frac{2k}{B_k}$ (Korollar 3.1.5). Da E_4, E_6, j und Δ ganzzahlige Koeffizienten haben, und da alle auftretenden Reihen als führenden Koeffizienten eine 1 haben, ist der lineare Term auf der rechten Seite aber $N + a_{n(k)-1} \cdot 1$, wobei $N \in \mathbb{Z}$ ist. Damit muss aber $a_{n(k)-1}$ denselben Nenner haben wie $\frac{2k}{B_k}$, womit die Aussage gezeigt ist.

□

Wir haben es also insgesamt entweder mit ganzzahligen Potenzreihen u.Ä. zu tun (z.B. Δ, j), oder zumindest mit Objekten, deren Nenner endlich ist, und den wir gut kontrollieren können (z.B. E_k, ϕ_k). Damit ergibt sich für uns die Möglichkeit, die Koeffizienten arithmetisch zu behandeln. Dies wird in den nun folgenden Kapiteln in Angriff genommen.

Kapitel 4

Berechnung der Eisensteinpolynome

Wir wissen nun genug über die auftretenden Reihen, um die Frage der konkreten Berechenbarkeit avisieren zu können. In erster Linie ist uns daran gelegen, die Eisensteinpolynome ϕ_k mit Computerhilfe auszurechnen. Ich werde in diesem Kapitel zunächst den alten Ansatz hierzu vorstellen, der aber einige Effizienzprobleme aufwirft. Danach werde ich eine neue Methode vorstellen, die im Grundsatz von meinem Betreuer, Prof. Gekeler, stammt, und die ich im Rahmen dieser Diplomarbeit ausgearbeitet und implementiert habe. Schließlich werde ich in diesem Kapitel noch verschiedene Laufzeitabschätzungen für diese Methode angeben und sie mit der alten vergleichen.

4.1 Berechnung nach Swinnerton-Dyer

Zunächst wenden wir uns der alten Methode zu. Diese wurde 1999 von Bernd Kremling im Rahmen seiner Diplomarbeit ([Kre]) in ein Computerprogramm umgesetzt. Es war bislang der einzige mir bekannte Versuch, die Eisensteinpolynome computationell zu berechnen.
Das Verfahren von Kremling beruht auf einer Rekursionsformel für Eisensteinreihen, die Swinnerton-Dyer in [Swi] erstmals (ohne Beweis) angegeben hat. Ein Beweis dazu findet sich in der Diplomarbeit [Kre] von Kremling.

4.1.1 Die Formel

4.1.1 Satz. *Sei* $k \geq 4$ *gerade. Setze* $F_k(z) := -\frac{B_k}{(k-2)!2k} E_k$.
Dann gilt die Rekursionsformel

$$
\begin{aligned}
(k-6)(k+1)F_k(z) &= 12 \sum_{i=2}^{\frac{k-2}{2}} F_{2i}(z)F_{k-2i}(z) \\
&= 12\left(F_4(z)F_{k-4}(z) + F_6(z)F_{k-6}(z) + \ldots + F_{k-4}(z)F_4(z)\right). \qquad (4.1)
\end{aligned}
$$

4.1.2 Bemerkung. *Die* F_k *wurden nur der Übersichtlichkeit halber eingeführt. Aus obiger Rekursionsformel lässt sich natürlich sofort eine Rekursionsformel für die* E_k *ableiten, die vom selben Typ ist. Ebenso lässt sich leicht eine Rekursion für die Eisensteinpolynome* ϕ_k *ableiten. Dazu muss man sich nur daran erinnern, dass die* ϕ_k *über die Gleichung*

$$E_k = \phi_k(j)\Delta^{n(k)}E_4^{\alpha(k)}E_6^{\beta(k)}$$

definiert sind.
Die Rekursion für die ϕ_k *hat den kleinen Nachteil, dass sie ein wenig unübersichtlich ist, weil die auftretenden* $n(k)$, $\alpha(k)$ *und* $\beta(k)$ *von der Restklasse* $k \bmod 12$ *abhängen. Aus diesem Grund möchte ich sie hier auch nicht explizit wiedergeben.*

4.1.2 Die Laufzeit

Es gibt jedoch auch noch einen schwerwiegenderen Haken. Schauen wir uns dazu einmal an, wie Laufzeit dieser Rekursion aussieht. Wir nehmen hierzu vereinfachend (und unrealistischerweise) an, die Koeffizienten der Eisensteinpolynome seien in $O(1)$.
Um ϕ_k aus den vorhergehenden ϕ_i zu berechnen, muss man Folgendes tun:

(i) Setze die Gleichung $E_k = \phi_k(j)\Delta^{n(k)}E_4^{\alpha(k)}E_6^{\beta(k)}$ in die Rekursionsformel (4.1) (bzw. in die entsprechende Rekursionsformel für die E_k) ein.

(ii) Multipliziere die Terme $\Delta^{n(k)}E_4^{\alpha(k)}E_6^{\beta(k)}$ zusammen. Wo es notwendig ist, substituiere $E_4^3 = j\Delta$ bzw. $E_6^2 = E_4^3 - 1728\Delta = (j-1728)\Delta$.

(iii) In jedem der Faktoren F_iF_{k-i}, multipliziere die Polynome ϕ_i und ϕ_{k-i} miteinander und gegebenfalls noch mit dem Faktor j bzw. $(j-1728)$, der aus Schritt (ii) hinzugekommen ist.

(iv) Summiere die entstandenen Polynome auf.

(v) Multipliziere das Endergebnis mit den Vorfaktoren aus der Rekursionsformel.

Bei dieser Vorgehensweise haben die Schritte (ii) und (v) keinen Einfluss auf die asymptotische Laufzeit und werden deshalb vernachlässigt. Entscheidend sind allein die Schritte (iii) und (iv).
Um die Laufzeit angeben zu können, stellen wir fest:

- Will man zwei Polynome der Grade m und n miteinander multiplizieren, so benötigt man i.A. $(m+1)(n+1)$ viele Multiplikationen (man muss Koeffizienten des einen Polynoms mit jedem des anderen Polynoms multiplizieren) und mn viele Additionen. (Man hat $(m+1)(n+1)$ viele Summanden. Bei jeder Summenbildung werden zwei Summanden durch einen neuen Wert, nämlich die Summe ersetzt. Die Zahl der Werte verringert sich also bei jeder Summenbildung um 1. Am Ende müssen noch $m+n+1$ Werte übrig bleiben, da das Ergebnispolynom den Grad $m+n$ hat. Also muss man $(m+1)(n+1)-(m+n+1)=mn$ mal addieren).
  Hat man zwei normierte Polynome vorliegen, so verringert sich die Zahl der Multiplikationen auf mn. Die Zahl der Additionen liegt unverändert bei mn.

- Das Polynom ϕ_i hat Grad $n(i) \approx \left\lfloor \frac{i}{12} \right\rfloor$. Wir werden zur Vereinfachung stattdessen mit dem Wert $\frac{i}{12}$ rechnen.
  Es ergibt sich als Zahl der Multiplikationen
  $$\begin{aligned}
  \sum_{i=2}^{\frac{k-2}{2}} \frac{2i}{12}\frac{(k-2i)}{12} &\approx \frac{1}{144}\sum_{i=1}^{\frac{k-2}{2}}\left(2ik-4i^2\right) \\
  &= \frac{1}{144}\left(2k\sum_{i=1}^{\frac{k-2}{2}} i - 4\sum_{i=1}^{\frac{k-2}{2}} i^2\right) \\
  &= \frac{1}{144}\left(2k\frac{\frac{(k-2)}{2}\frac{k}{2}}{2} - 4\frac{\frac{(k-2)}{2}\frac{k}{2}\frac{(2k-2)}{2}}{6}\right) \\
  &\approx \frac{1}{144}\left(\frac{k^3}{4}-\frac{k^3}{6}\right) \\
  &= \frac{k^3}{1728}.
  \end{aligned}$$
  Hinzu kommen noch einmal ebenso viele Additionen.

- Schließlich muss man die Produkte noch aufaddieren, wodurch noch einmal etwa $\frac{k}{2}\cdot\frac{k}{12}=\frac{k^2}{24}$ Additionen hinzukommen.

Wir sehen also, dass diese Rekursion ein zweischneidiges Schwert ist: Auf der einen Seite hat man recht gute Vorfaktoren ($\frac{1}{1728}$), die zumindest für kleine k eine hohe Effizienz zu gewährleisten scheinen, auf der anderen Seite ist die Laufzeit in $O(k^3)$, was normalerweise für größere Berechnungen eine unüberwindliche Hürde darstellt.
Tatsächlich ist die Situation noch in doppelter Hinsicht schlimmer:
Zum Einen war die Annahme, man habe es mit Koeffizienten beschränkter Größe zu tun, grundfalsch. Schon für relativ kleine Werte von k (etwa für $k \approx 300$) beansprucht die Dezimaldarstellung eines einzelnen Koeffizienten bereits eine ganze Bildschirmseite. Diese Zahlen müssen nun noch miteinander multipliziert werden. Selbst bei sehr effizienten Algorithmen wie in [LEDA] wird nur eine Laufzeit von $O(n^{\log_2(3)}) \approx O(n^{1,58})$ erreicht (zur Multiplikation zweier Zahlen der Länge n), und die gängigen Computeralgebraprogramme dürften dafür vermutlich sogar $O(n^2)$ brauchen.
Ein zweiter Nachteil der Swinnerton-Dyer-Rekursion ist, dass man zur Berechnung eines Eisensteinpolynoms alle vorhergehenden Polynome braucht. Man muss daher zur Berechnung eines einzelnen ϕ_k alle ϕ_k berechnen, was die Laufzeit sogar auf $O(k^4)$ hinaufschraubt.

4.2 Berechnung mittels linearer Gleichungssysteme

Im kommenden Abschnitt werden wir die folgenden Bezeichnungen verwenden:

4.2.1 Bezeichnungen. Gewöhnlich werden wir mit einem festen k arbeiten. Daher ersparen wir es uns auch, immer den Index k mitzuschleppen.

- Der i-te Koeffizient in der q-Entwicklung der Eisenstenreihe E_k heiße e_i. Es ist also $E_k(q) = \sum_{i=0}^{\infty} e_i q^i$. Insbesondere ist $e_0 = 1$.

- Der i-te Koeffizient in der q-Entwicklung von Δ heiße δ_i. Es ist also $\Delta(q) = \sum_{i=1}^{\infty} \delta_i q^i$. Insbesondere ist $\delta_1 = 1$.

- Der i-te Koeffizient in der q-Entwicklung von j heiße j_i. Es ist also $j(q) = \sum_{i=-1}^{\infty} j_i q^i$. Insbesondere ist $j_{-1} = 1$.

- Das Eisensteinpolynom ϕ_k habe die Koeffizienten a_k und den Grad $n = n(k)$, also ist $\phi_k(X) = \sum_{i=0}^{n} a_i X^i$. Insbesondere ist $a_n = 1$.

4.2.1 Das Gleichungssystem

Die Idee hinter der neuen Methode ist eigentlich recht einfach: Man schaut sich die definierende Gleichung $E_k = \phi_k(j)\Delta^{n(k)}E_4^{\alpha(k)}E_6^{\beta(k)}$ der ϕ_k an. Wir haben im Beweis von Korollar 3.2.4 schon gesehen, dass man durch Betrachten des Koeffizienten von q^l eine Gleichung der Form $e_l = a_l + \sum_i r_i$ erhält. Dabei sind die r_i Produkte, in die nur

- die Koeffizienten der Reihen j, Δ, E_4 und E_6 und
- die Koeffizienten a_n, a_{n-1}, …, a_{l+1} des Eisensteinpolynoms

einfließen. Stellen wir diese Gleichung um, so erhalten wir eine Rekursionsgleichung $a_l = e_l - \sum_i r_i$ für die a_l (startend bei a_n und endend bei a_0).

Globale Vorbereitungen

Die eingehenden Größen sind dabei leicht zu beschaffen: Die Koeffizienten von E_k, Δ, E_4 und E_6 erhält man über die Formeln, die in Kapitel 3 hergeleitet wurden. Die Koeffizienten von j gewinnt man aus der Formel $j\Delta = E_4^3$. Diese Formel stellt nämlich nichts anderes dar als ein lineares Gleichungssystem für die Koeffizienten. Es ist

$$\begin{pmatrix} j_{-1} & 0 & 0 & 0 & \cdots \\ j_0 & j_{-1} & 0 & 0 & \cdots \\ j_1 & j_0 & j_{-1} & 0 & \cdots \\ j_2 & j_1 & j_0 & j_{-1} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} \delta_1 \\ \delta_2 \\ \delta_3 \\ \delta_4 \\ \vdots \end{pmatrix} = \begin{pmatrix} e_0^{(3)} \\ e_1^{(3)} \\ e_2^{(3)} \\ e_3^{(3)} \\ \vdots \end{pmatrix}.$$

Mit $e_i^{(3)}$ ist dabei einfach der i-te Koeffizient von E_4^3 gemeint.
Es handelt sich hierbei zwar zunächst um ein unendliches lineares Gleichungssystem, aber alle vorkommenden Summen sind endlich. Da man es außerdem mit einer Dreiecksmatrix zu tun hat, lassen sich die gesuchten Variablen j_i einfach und effizient berechnen. (Die Situation ist sogar noch einfacher, denn auf der Diagonalen der Matrix steht überall 1).

Schauen wir uns nun an, welche der Koeffizienten wir überhaupt brauchen. Wir betrachten von der Formel $E_k = \phi_k(j)\Delta^{n(k)}E_4^{\alpha(k)}E_6^{\beta(k)}$ nur die Vorfaktoren zu q^l, wo $l \in \{0, \ldots, n\}$.
Das heißt zunächst einmal, dass wir von der Eisensteinreihe genau die Einträge $e_0, \ldots, e_n$ brauchen. Auf der rechten Seite müssen wir schon etwas genauer hinschauen: Die Funktion j beginnt mit dem Term $q^{-1} + \ldots$, daher

beginnt $\phi_k(j)$ mit dem Term $q^{-n}+\ldots$. Andererseits beginnt Δ mit $q+\ldots$, also beginnt Δ^n mit $q^n+\ldots$. Die Reihen E_4 und E_6 beginnen einfach mit $1+\ldots$. Da wir an den ersten $n+1$ Stellen des Ergebnisses interessiert sind, dürfen wir jede Reihe nach den ersten $n+1$ Stellen abschneiden. Wir brauchen also E_4 und E_6 nur bis zum q^n-Term (einschließlich), Δ bis zum q^{n+1}-Term, und j bis zum q^{n-1}-Term.
Damit haben wir es zumindest schon einmal mit einem endlichen Problem zu tun: Wir haben die Potenzreihen durch Polynome ersetzt. Außerdem sollten wir im Hinterkopf behalten, dass wir jede Multiplikation zweier Polynome nur bis auf $n+1$ Terme genau berechnen müssen. (In gewisser Weise rechnen wir mod q^{n+1}; das bedeutet aber nicht, dass wir jeden einzelnen Term mod q^{n+1} reduzieren dürfen, da auch negative q-Potenzen auftreten).
Eine Berechnung können wir schon vorbereitend ausführen, nämlich die Berechnung von j^i für $i \in \{0,\ldots,n\}$. Diese tauchen in dem Ausdruck $\phi_k(j)$ auf. Man beachte dabei, dass die Berechnung der j^i unabhängig vom gerade betrachteten k ist (abgesehen davon, dass k angibt, wie viele dieser Potenzen man braucht und mit welcher Genauigkeit man sie benötigt). Will man daher mehrere ϕ_k berechnen, so empfiehlt es sich, die j^i zuerst global auszurechnen und dann einfach zu speichern.
Ebenso bietet es sich an, die Produkte $E_4^{\alpha(k)}E_6^{\beta(k)}$ global zu berechnen, da $\alpha(k)$ und $\beta(k)$ ja nur von der Restklasse $k \mod 12$ abhängen. Das Paar $(\alpha(k),\beta(k))$ stammt immer aus der Menge $\{(0,0),(2,1),(1,0),(0,1),(2,0),(1,1)\}$. Auch diese 6 Produkte sollte man global speichern.

Vorbereitungen bei gegebenem k

Eine Berechnung gibt es noch, die wir anstellen sollten, bevor wir uns in die eigentliche Rekursion stürzen: Der Ausdruck $D := \Delta^n E_4^{\alpha(k)}E_6^{\beta(k)}$ wird in jedem Rekursionschritt auftauchen, weshalb wir ihn noch vorher ausrechnen und speichern sollten. Wir benötigen ihn wieder mit einer Genauigkeit von $n+1$ Termen (allerdings werden wir tatsächlich im l-ten Rekursionsschritt nur die ersten $l+1$ Terme benutzen). Wir bezeichnen den Koeffizienten vor q^{n+i} dieser Reihe mit d_i, also

$$D = \underbrace{d_0}_{=1} q^n + d_1 q^{n+1} + d_2 q^{n+2} + \ldots \ .$$

Die Rekursion

Schauen wir uns nun an, welche Rechnungen wir wirklich anstellen müssen, um a_l aus $a_{l+1},\ldots,a_n$ zu bekommen. Dazu berechnen wir zunächst den relevanten Anteil von $\phi_k(j)$; genauer gesagt benötigen wir

$$S_l := \sum_{i=l+1}^{n} a_i j^i.$$

Wir beschreiben die Summe S_l als

$$S_l = \underbrace{s_0}_{=1} q^{-n} + s_1 q^{-n+1} + s_2 q^{-n+2} + \ldots + s_n q^0 + O(q).$$

In diesem Moment würden wir nur die ersten $n - l + 1$ Terme jeder Rechnung benötigen. Mit Blick auf die noch kommenden Rekursionsschritte sehen wir aber, dass wir die Terme $a_i j^i$ sowieso letzendlich mit voller Genauigkeit aufsummieren müssen (spätestens im letzten Rekursionsschritt). Wir sparen also insgesamt Rechenzeit, wenn wir die obige Summe in voller Genauigkeit (d.h. auf $n + 1$ Terme) ausrechnen und das Ergebnis dann speichern. Das bedeutet jedoch nicht, dass wir auch jeden einzelnen *Summanden* mit voller Genauigkeit brauchen. Da nämlich j^i mit dem Term q^{-i} beginnt, genügt es, nur die ersten $i + 1$ Terme dieses Summanden zu benutzen.
(Strenggenommen braucht man den Ausdruck j^i insgesamt nur mit dieser Genauigkeit, sodass die zu Anfang ausgeführte Berechnung auf $n + 1$ Terme eigentlich eine Verschwendung darstellt. Allerdings braucht man ausgerechnet die höchste Potenz j^n mit voller Genauigkeit. Für die Berechnung von j^n braucht man aber doch wieder einige der kleineren Potenzen j^i auf $n + 1$ Terme genau, wenn auch nur für manche i. Die mögliche Zeitersparnis stand deshalb hier in meinen Augen in keinem Verhältnis zur Verkomplizierung des Programms, die für diese Ersparnis nötig gewesen wäre, weshalb ich diese Unsauberkeit in Kauf genommen habe.)
Wir haben also jetzt die Gleichung $E_k = \left(S_l + a_l q^{-l}\right) D$. Diese ist modulo q^{n-l+1} korrekt. Von dieser Gleichung betrachten wir den Koeffizienten bei q^{n-l}. Auf der linken Seite ist dieser Koeffizient natürlich einfach e_{n-l}, auf der rechten Seite ist es $a_l \underbrace{d_0}_{=1} + \sum_{i=0}^{n-l} s_i d_{n-l-i}$. Setzen wir diese beiden Ausdrücke also gleich und lösen nach a_l auf, so erhalten wir unsere Rekursion

$$a_l = e_{n-l} - \sum_{i=0}^{n-l} s_i d_{n-l-i}.$$

4.2.2 Laufzeit der linearen Methode

Nun wollen wir natürlich auch noch die Laufzeit unserer alternativen Berechnungsmethode analysieren. Dies tun wir auf zwei Arten: Einmal vernachlässigen wir, dass die Koeffizienten aller beteiligten Reihen stark wachsen, einmal berücksichtigen wir es.

... bei beschränkten Koeffizienten

Wir gehen also zunächst mal davon aus, dass alle Koeffizienten klein bleiben, und man daher jede Multiplikation und Addition in Zeit $O(1)$ ausführen kann.
Die Berechnung von E_4, E_6, E_k und Δ kann man getrost vernachlässigen. Um einen Koeffizienten einer Eisensteinreihe auszurechnen, müssen wir im Wesentlichen die Funktion σ_{k-1} auswerten. Diese Funktion ist in den meisten Computeralgebraprogrammen fest implementiert. Ebenso wenig Mühe macht es, Δ über die Produktdarstellung auszurechnen.
Auch die Berechnung der Funktion j kann man unter den Tisch fallen lassen. Wir müssen dazu ein dreieckiges, lineares Gleichungssystem der Größe n lösen (um n Stellen von j zu berechnen). Dies geht in der Zeit $O(n^2)$ mit sehr günstigen Vorfaktoren.
Etwas mehr Arbeit steckt darin, die Potenzen j^i auszurechnen. Für jede neue Potenz müssen wir zwei Polynome vom Grad n miteinander multiplizieren. Auch wenn wir nicht alle Teilergebnisse brauchen (sondern nur etwa die Hälfte), weil wir vom Ergebnis nur die ersten n Terme wollen, bleibt die Multiplikation in $\Theta(n^2)$. Da wir n solche Berechnungen anstellen müssen, sind wir insgesamt schon bei $\Theta(n^3)$.
Mit der gleichen Überlegung sieht man, dass die Berechnung von $E_4^{\alpha(k)}E_6^{\beta(k)}$ in Zeit $O(n^2)$ geschieht. Da man nur 6 solcher Produkte berechnen muss, bleibt die Laufzeit für die globalen Vorbereitungen bei $\Theta(n^3)$.

Nun kommen wir zu der Vorbereitung, die man ausführen muss, wenn man sich auf ein k festgelegt hat: Diese besteht in der Berechnung des Produktes $\Delta^n E_4^{\alpha(k)}E_6^{\beta(k)}$. Wieder müssen wir eine n-te Potenz einer Reihe berechnen, aber im Gegensatz zu j^n brauchen wir hier keine kleineren Potenzen. Die Erhebung in die n-te Potenz ist allgemein mit $O(\log(n))$ vielen Multiplikationen möglich, sodass die Laufzeit insgesamt $O(\log(n)n^2)$ ist. (Man benutzt dazu im Wesentlichen eine Rekursion, die den Exponenten vermöge der Formel $M^n = M^{\frac{n}{2}} \cdot M^{\frac{n}{2}}$ in jedem Schritt verdoppelt. Details findet der Leser in jedem Buch über effiziente Algorithmen, zum Beispiel in [Meh, Ch. V]).
Hat man vor, eine ganze Serie von Eisensteinpolynomen auszurechnen, so benötigt man natürlich alle Potenzen von Δ. In diesem Fall hat man auch die Möglichkeit, sie ebenso wie die Potenzen von j schon zu Beginn auszurechnen. Insgesamt (für alle Potenzen) benötigt man dann nur die Rechenzeit $O(n^3)$ (und nicht etwa $O(n \cdot \log(n)n^2)$).
Die eigentliche Rekursion zur Berechnung der a_l geht dann ziemlich schnell: Im l-ten Schritt (d.h. zur Berechnung von a_{n-l}) muss man zuerst die Summe S_{n-l} ausrechnen. Unter Zuhilfenahme der schon berechneten Summe S_{n-l+1}

geht dies mit l Multiplikationen und l Additionen. Danach muss man noch die Rekursionsgleichung $a_{n-l} = e_l - \sum_{i=0}^{l} s_i d_{l-i}$ auswerten, welche mit l Multiplikationen und l Additionen zu Buche schlägt. Insgesamt kostet der l-te Rekursionsschritt also nur $2l$ Multiplikationen und $2l$ Additionen. Alle Rekursionschritte zusammen bringen es daher nur auf etwa n^2 viele Multiplikationen und ebenso viele Additionen.

Insgesamt steckt die Rechenzeit bei dem ganzen Prozess also in den Vorbereitungen, insbesondere in der Berechnung der j^i (und bei der Berechnung mehrerer ϕ_k auch in den Δ^i). Die Laufzeit bleibt aber wie bei der alten Methode bei dem wenig befriedigenden Wert $O(n^3)$.

... bei wachsenden Koeffizienten

Wir waren natürlich wieder zu optimistisch. Ich habe bereits zuvor angedeutet, dass die Koeffizienten aller beteiligten Potenzreihen und Polynome sehr rasch explodieren. Wir wollen hier den Versuch unternehmen, dies in unsere Berechnungen zu integrieren. Dazu werden wir davon ausgehen, dass sich die Koeffizienten der auftretenden Modulformen in Anlehnung an die Ramanujan-Petersson-Vermutung etwa wie $\Theta(n^{\frac{k}{2}})$ verhalten (Satz 3.1.7). Diese Annahme scheint zumindest für die Δ-Funktion eine brauchbare Näherung zu liefern, und die durchgeführten Berechnungen legen nahe, dass auch die Koeffizineten der Eisensteinreihen ein vergleichbares Wachstum an den Tag legen (obwohl sie keine Spitzenformen sind, und die Ramanujan-Petersson-Vermutung deshalb gar nichts über sie aussagt).
Um zwei Zahlen der Größe $n^{\frac{k}{2}}$ miteinander zu multiplizieren, muss man mit der Laufzeit $O(k^2)$ rechnen (da die Stellenzahl der Zahlen in $O(k)$ liegt). Wir schauen uns daher den aufwändigsten Teil, die Berechnung der j^i an, wobei wir auch für j^i davon ausgehen, dass die Koeffizienten die Größe n^{ik} haben. Ein wenig Glück hat man dabei, denn die „schlimmsten" Ergebnisse muss man gar nicht erst ausrechnen, da man ja nur die ersten n Terme von j^i benötigt. Multipliziert man aber zwei Koeffizienten, die weit hinten in der Entwicklung von j liegen (und damit tendenziell groß sind), so liegt das Ergebnis außerhalb des benötigten Bereiches. Jedenfalls benötigen die Multiplikationen bei der Berechnung von $j^{i+1} = j^i \cdot j$ etwa die Zeit $O(i)$. Da man $O(n^2)$ viele Multiplikationen hat, kommt man im i-ten Schritt auf eine Zeit von $O(in^2)$, und für alle Schritte zusammen auf $O(n^4)$.
Eine Analyse der Berechnung von Δ^n zeigt, dass auch hier etwa der Faktor n hinzukommt. Man hat also die Laufzeit $O(\log(n)n^3)$ für die Berechnung von Δ^n oder $O(n^4)$ für die Berechnung aller Potenzen von Δ.
Man sieht also, dass auch diese Art der Berechnung schon nach recht kurzer

Zeit an ihre Grenzen stoßen muss. In der Praxis liegt diese Grenze zwischen $k = 500$ und $k = 1000$.
Es gibt jedoch einen Aspekt, der die neue Methode gegenüber der alten doch in einen Vorteil versetzt. Es zeigt sich nämlich, dass die Koeffizienten der Eisensteinpolynome noch sehr viel stärker wachsen als die Koeffizienten der auftretenden Reihen. Nun bringt es die Swinnerton-Dyer-Methode aber mit sich, dass man die Eisensteinpolynome miteinander multiplizieren muss, ein Vorgang, der sehr kostspielig ist. Dagegen müssen die Koeffizienten dieser Polynome bei der neuen Methode nie untereinander, sondern „nur" mit den Koeffizienten der j^i sowie den Koeffizienten von D multipliziert werden. Tatsächlich scheint sich die Grenze der Berechenbarkeit durch die neue Methode ein wenig nach hinten zu verschieben. Man kann aber leider nicht davon sprechen, dass ein großer Durchbruch erzielt wäre.

Kapitel 5

Eigenschaften der Eisensteinpolynome

Man sucht natürlich nicht nur zum Spaß nach einer effizienten Methode, die Eisensteinpolynome zu berechnen. Hat man erst einmal ein genügend großes Beispielmaterial zusammen, so sucht man in diesem Material nach Auffälligkeiten und Regelmäßigkeiten. Wenn man Glück hat, so bemerkt man Strukturen, die sich in allgemeine Vermutungen ummünzen lassen. Diese Vermutungen können sich als einfache Eigenschaften herausstellen. So stammt zum Beispiel die Einsicht über die Nenner der Eisensteinpolynome (vgl. Korollar 3.2.4) aus den Berechnungen, die Bernd Kremling im Rahmen seiner Diplomarbeit ([Kre]) angestellt hat. Andererseits ist es auch möglich, dass diese Vermutungen über längere Zeit allen Versuchen widerstehen, sie zu beweisen oder zu widerlegen. Ich werde in Abschnitt 5.2 einige Beispiele dafür angeben.

5.1 Tatsachen über die Eisensteinpolynome

Zunächst einige der Eigenschaften, die sich auch tatsächlich beweisen lassen:

5.1.1 Die Nullstellen

Die erste Frage, die auftritt, wenn man es mit Polynomen zu tun hat, ist natürlich: Wie sieht die Faktorisierung aus? Oder anders ausgedrückt: Wo liegen die Nullstellen des Polynoms? Für die Eisensteinpolynome kann man diese Frage mit bemerkenswerter Genauigkeit beantworten. Zunächst schauen wir uns dazu an, wie die Nullstellen der Eisensteinreihen aussehen:

5.1.1 Satz. *Sei $k \geq 4$ gerade und sei D der übliche Fundamentalbereich der modularen Gruppe. Mit I bezeichnen wir die Menge $\{z = e^{i\theta} \in \mathbb{C} | \ \theta \in (\frac{\pi}{2}, \frac{2\pi}{3})\}$, also der Kreisbogenabschnitt des Einheitskreises zwischen i und ρ.*

(i) Die Eisensteinreihe E_k hat genau $n(k)$ viele Nullstellen in I, eine $\alpha(k)$-fache Nullstelle in ρ und eine $\beta(k)$-fache Nullstelle in i. Sonst hat E_k keine weiteren Nullstellen in D, mit Ausnahme der Translate der schon angegebenen Nullstellen unter G. (Mit anderen Worten, E_k hat in $\mathbb{C}/G$ keine weiteren Nullstellen.)

(ii) Bezeichnet man die Nullstellen $\neq i, \rho$ mit $\{\tau_r | \ r = 1, \ldots, n(k)\}$, so gilt: In jedem der $n(k)$ gleich langen, offenen Kreisbogenteilabschnitte von I (d.h. in jeder der Mengen $\{e^{i\theta} | \ \theta \in (\frac{\pi}{2} + \frac{r}{n(k)} \cdot \frac{\pi}{6}, \frac{\pi}{2} + \frac{r+1}{n(k)} \cdot \frac{\pi}{6})\}$, wobei $r = 0, \ldots, n(k) - 1$) liegt genau eine Nullstelle von E_k.
Diese Nullstellen sind alle einfach.

Beweis. Diese Aussage wurde 1969 von Rankin und Swinnerton-Dyer in [Ran] bewiesen. Da der Beweis sehr hübsch die Symmetrie der Eisensteinreihen ausnutzt, möchte ich ihn hier (mit nur einigen kleineren Anpassungen) wiedergeben.
Von der Residuenformel

$$\frac{1}{2}v_i(E_k) + \frac{1}{3}v_\rho(E_k) + \sum_{\text{sonstige } p \in (\mathbb{H}_\infty/G)} v_p(E_k) = \frac{k}{12}$$

kann man sofort deduzieren, dass

- E_k mindestens eine $\alpha(k)$-fache Nullstelle in ρ und eine $\beta(k)$-fache Nullstelle in i haben muss, und dass

- E_k höchstens $n(k)$ weitere Nullstellen haben kann.

So waren $n(k)$, $\alpha(k)$ und $\beta(k)$ nämlich gerade definiert.
Außerdem sehen wir daran Folgendes: Wenn wir zeigen können, dass in jedem der in (ii) definierten Kreisbogenteilabschnitte eine Nullstelle liegt, dann haben wir damit schon alle Nullstellen gefunden. Insbesondere müssen diese Nullstellen dann alle einfach sein, und die Nullstellen in ρ und i können nicht mit höherer Ordnung als $\alpha(k)$ bzw. $\beta(k)$ auftreten. Kurz gesagt: Dann ist unser Beweis schon komplett.
Um nun noch nachzuweisen, dass tatsächlich in jedem Abschnitt eine Nullstelle liegt, definieren wir uns erst eine Hilfsfunktion

$$F_k(\theta) := e^{i\pi k \frac{\theta}{2}} E_k(e^{\pi i\theta}).$$

Die Variablentransformation $\theta \mapsto e^{\pi i\theta}$ transformiert das Intervall $[\frac{1}{2}, \frac{2}{3}]$ zum Kreisbogenabschnitt zwischen i und ρ, was uns vor allem die Rechnung etwas vereinfacht. Wichtiger dagegen ist die Tatsache, dass der Vorfaktor $e^{i\pi k\frac{\theta}{2}}$ aus F_k eine reellwertige Funktion macht (zumindest für $\theta \in \mathbb{R}$). Es gilt nämlich

$$\begin{aligned} F_k(\theta) &= e^{i\pi k\frac{\theta}{2}} \sum_{c\in\mathbb{Z}} \sum_{d\in\mathbb{Z}}{}' \frac{1}{(ce^{\pi i\theta}+d)^k} \\ &= \sum_{c\in\mathbb{Z}} \sum_{d\in\mathbb{Z}}{}' \frac{1}{\left(ce^{\pi i\frac{\theta}{2}}+de^{-\pi i\frac{\theta}{2}}\right)^k}. \end{aligned}$$

Zunächst sehen wir, dass die Summanden mit Indizes (c, d), für die $c = d$ gilt, reell sind, denn es ist dann

$$\begin{aligned} ce^{\pi i\frac{\theta}{2}}+de^{-\pi i\frac{\theta}{2}} &= 2c \cdot \left(\frac{e^{\pi i\frac{\theta}{2}}+e^{-\pi i\frac{\theta}{2}}}{2}\right) \\ &= 2c \cdot \cos\left(\frac{\theta}{2}\right) \in \mathbb{R}. \end{aligned}$$

Wenden wir uns nun also den Paaren (c, d) mit $c \neq d$ zu.
In diesem Fall fassen wir den Summanden für (c, d) mit dem Summanden für (d, c) zusammen, und erhalten insgesamt

$$\begin{aligned} &\frac{1}{\left(ce^{\pi i\frac{\theta}{2}}+de^{-\pi i\frac{\theta}{2}}\right)^k} + \frac{1}{\left(de^{\pi i\frac{\theta}{2}}+ce^{-\pi i\frac{\theta}{2}}\right)^k} \\ =&\frac{1}{\left(ce^{\pi i\frac{\theta}{2}}+de^{-\pi i\frac{\theta}{2}}\right)^k} + \frac{1}{\left(c\frac{1}{e^{\pi i\frac{\theta}{2}}}+d\frac{1}{e^{-\pi i\frac{\theta}{2}}}\right)^k}. \end{aligned}$$

Schauen wir uns einmal an, was passiert, wenn wir von diesem Ausdruck das Konjugiert-Komplexe bilden (zu $z \in \mathbb{C}$ sei $\overline{z}$ das Konjugiert-Komplexe): Wegen $\left|e^{i\pi\frac{\theta}{2}}\right| = 1$ ist $\overline{e^{i\pi\frac{\theta}{2}}} = \frac{1}{e^{i\pi\frac{\theta}{2}}}$. Also ist auch

$$\overline{ce^{\pi i\frac{\theta}{2}}+de^{-\pi i\frac{\theta}{2}}} = c\frac{1}{e^{\pi i\frac{\theta}{2}}}+d\frac{1}{e^{-\pi i\frac{\theta}{2}}},$$

und daran ändert auch das Erheben in die k-te Potenz nichts. Der Ausdruck

$$\frac{1}{\left(ce^{\pi i\frac{\theta}{2}}+de^{-\pi i\frac{\theta}{2}}\right)^k} + \frac{1}{\left(c\frac{1}{e^{\pi i\frac{\theta}{2}}}+d\frac{1}{e^{-\pi i\frac{\theta}{2}}}\right)^k}$$

wird also durch komplexe Konjugation in sich selbst überführt, er muss also aus $\mathbb{R}$ gewesen sein.
Damit haben wir gezeigt, dass für $\theta \in \mathbb{R}$ auch $F_k(\theta) \in \mathbb{R}$ ist.

Nun sortieren wir die Summe etwas um. Als erstes fassen wir die Terme für $(c,d) \in \{(0,1),(1,0),(0,-1),(-1,0)\}$ zusammen (man beachte, dass dies genau die Paare sind mit $c^2+d^2=1$) und erhalten

$$\begin{aligned} F_k(\theta) &= e^{-i\pi k\frac{\theta}{2}} + e^{-i\pi k\frac{\theta}{2}} - e^{-i\pi k\frac{\theta}{2}} - e^{-i\pi k\frac{\theta}{2}} + R_k(\theta) \\ &= 4\cos\left(\pi k\frac{\theta}{2}\right) + R_k(\theta), \end{aligned}$$

wobei $R_k(\theta)$ die verbleibenden Summanden (mit $c^2+d^2>1$) enthält.
Wir zeigen nun, dass für $\theta \in [\frac{1}{2}, \frac{2}{3}]$ immer $|R_k(\theta)| < 4$ gilt. Dann muss F_k nämlich an den Stellen $\frac{2m}{k}$ dasselbe Vorzeichen haben wie $\cos\left(\pi k\frac{\theta}{2}\right)$, also immer abwechselnd ein positives und ein negatives Vorzeichen (für $m \in [\frac{k}{4}, \frac{k}{3}] \cap \mathbb{Z}$). Zwischen jedem Vorzeichenwechsel muss aber eine Nullstelle liegen, und da es im Intervall $[\frac{k}{4}, \frac{k}{3}]$ genau $n(k)+1$ verschiedene ganze Zahlen gibt (dies überprüft man durch Fallunterscheidung nach k mod 12), hat man seine $n(k)$ vielen Nullstellen gefunden.
Es bleibt also nur noch die Ungleichung $|R_k(\theta)| < 4$ zu verifizieren. Zunächst schätzen wir die beiden Summanden für $(c,d) \in \{(1,-1),(-1,1)\}$ ab: Ist $\theta \in [\frac{\pi}{2}, \frac{2\pi}{3}]$, so ist $|\sin(\pi\frac{\theta}{2})| \geq \sqrt{\frac{1}{2}}$, und daher

$$\left|\frac{1}{\left(e^{\pi i\frac{\theta}{2}} - e^{-\pi i\frac{\theta}{2}}\right)^k}\right| = \frac{1}{|2\sin\pi\frac{\theta}{2}|^k} \leq 2^{-\frac{k}{2}}.$$

Alle anderen Summanden können wir pauschal abschätzen. Dazu stellen wir fest, dass für $\theta \in [\frac{1}{2}, \frac{2}{3}]$ immer $|\cos\pi\theta| \leq \frac{1}{2}$ ist. Wir haben daher:

$$\begin{aligned} \left|ce^{\pi i\frac{\theta}{2}} + de^{-\pi i\frac{\theta}{2}}\right|^2 &= c^2 + 2cd\cos(\pi\theta) + d^2 \\ &\geq \frac{1}{2}(c^2+d^2) + \underbrace{\frac{1}{2}(c^2+d^2-2|cd|)}_{=(|c|-|d|)^2\geq 0} \\ &\geq \frac{1}{2}(c^2+d^2), \end{aligned}$$

oder

$$\frac{1}{\left(ce^{\pi i\frac{\theta}{2}} + de^{-\pi i\frac{\theta}{2}}\right)^k} \leq \left(\frac{c^2+d^2}{2}\right)^{-\frac{k}{2}}.$$

Nun sortieren wir die Summe R_k wieder nach der Größe von $c^2 + d^2$ und schätzen sie mit obiger Ungleichung ab (die 4 Summanden mit $c^2 + d^2 = 2$ werden gesondert behandelt):

$$\begin{aligned} |R_k(\theta)| &= \left| \sum_{(c,d)\in\left\{\substack{(1,-1),(-1,1),\\ (1,1),(-1,-1)}\right\}} \frac{1}{\left(ce^{\pi i\frac{\theta}{2}} + de^{-\pi i\frac{\theta}{2}}\right)^k} + \right. \\ &\qquad \left. + \sum_{N=3}^{\infty} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ c^2+d^2=N}} \frac{1}{\left(ce^{\pi i\frac{\theta}{2}} + de^{-\pi i\frac{\theta}{2}}\right)^k} \right| \\ &\leq 2\cdot 2^{-\frac{k}{2}} + 2\left(\frac{2}{2}\right)^{-\frac{k}{2}} + \sum_{N=3}^{\infty} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ c^2+d^2=N}} \left(\frac{N}{2}\right)^{-\frac{k}{2}} \\ &= 2 + 2^{-\frac{k}{2}+1} + \sum_{N=3}^{\infty} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ c^2+d^2=N}} \left(\frac{N}{2}\right)^{-\frac{k}{2}} \end{aligned}$$

Als nächsten Schritt schätzen wir ab, wie viele Paare (c, d) die Bedingung $c^2 + d^2 = N$ für eine gegebenes $N > 2$ erfüllen: Für $N = 4$ sind es genau 4 Paare und für $N = 3$ ist die Gleichung unlösbar. Für $N \geq 5$ überlegen wir uns, dass $|c|^2 \leq \sqrt{N}$ sein muss, und es zu jedem c nur maximal zwei d geben kann, die die Gleichung erfüllen. Es gibt daher höchstens $2(2\sqrt{N}+1) \leq 5\sqrt{N}$ viele Paare, die die Gleichung erfüllen. Damit können wir den Rest weiter abschätzen:

$$\begin{aligned} R_k(\theta) &\leq 2 + 2^{-\frac{k}{2}+1} + \sum_{N>2}^{\infty} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ c^2+d^2=N}} \left(\frac{N}{2}\right)^{-\frac{k}{2}} \\ &\leq 2 + 2^{-\frac{k}{2}+1} + 4\cdot 2^{-\frac{k}{2}} + \sum_{N=5}^{\infty} 5\sqrt{N}\left(\frac{N}{2}\right)^{-\frac{k}{2}} \\ &= 2 + 2^{-\frac{k}{2}+1} + 4\cdot 2^{-\frac{k}{2}} + 5\sum_{N=5}^{\infty} \left(\frac{N}{2}\right)^{-\frac{k}{2}+1} \end{aligned}$$

Da die Funktion, über die summiert wird, monoton in N fällt, kann man die Summe

$$\sum_{N=5}^{\infty} \left(\frac{N}{2}\right)^{-\frac{k}{2}+1}$$

gegen das uneigentliche Integral

$$\begin{aligned}\int_4^\infty \left(\frac{x}{2}\right)^{-\frac{k}{2}+1} dx &= \left(\frac{2}{-\frac{k}{2}+2}\left(\frac{x}{2}\right)^{-\frac{k}{2}+2}\right)\Bigg|_{x=4}^{x=\infty} \\ &= \frac{4}{k-4}\cdot 2^{-\frac{k-4}{2}}\end{aligned}$$

abschätzen. Für $k \geq 8$ ergibt sich tatsächlich die gewünschte Abschätzung

$$R_k(\theta) < 2 + \frac{1}{8} + \frac{1}{4} + 5 \cdot 2^{-2} < 4.$$

(Für $k = 4$ und $k = 6$ ist die Aussage sowieso trivial.) Damit ist der Restterm abgeschätzt und unser Beweis vollendet. $\square$

Nun kommen wir zu den Nullstellen der Eisensteinpolynome. Dazu schauen wir uns an, wie der Zusammenhang zwischen den Nullstellen der ϕ_k und der Nullstellen der E_k ist.

5.1.2 Satz. *Es ist*

$$\phi_k(X) = \prod_{x_i}(X - x_i),$$

wobei x_i die Menge $\{j(z) \mid z \in \mathbb{H}/G,\ E_k(z) = 0,\ z \neq i, z \neq \rho\}$ durchläuft. ϕ_k kodiert also in gewisser Weise die Nullstellen von E_k.

Beweis. Da ϕ_k normiert ist, genügt es, sich zu überlegen, dass es dieselben Nullstellen hat wie das angegebene Produkt.
Betrachte dazu wieder die Gleichung

$$E_k(z) = \phi_k(j(z))\Delta^{n(k)}(z)E_4^{\alpha(k)}(z)E_6^{\beta(k)}(z).$$

Den Faktor $\Delta^{n(k)}(z)$ können wir ignorieren, denn Δ hat nur die einfache Nullstelle in ∞ (Korollar 2.2.7), $\Delta^{n(k)}$ also eine $n(k)$-fache Nullstelle. Diese wird aber durch die $n(k)$-fache Polstelle von $\phi_k(j)$ in ∞ wieder aufgehoben. In $E_4^{\alpha(k)}(z)$ und $E_6^{\beta(k)}(z)$ stecken genau die Nullstellen von E_k an den Stellen ρ bzw. i.
Es gibt noch $n(k)$ weitere Punkte z mit $E_k(z) = 0$. Für jeden dieser Punkte muss auch $\phi_k(j(z))$ verschwinden (da die anderen Faktoren der rechten Seite an diesen Stellen $\neq 0$ sind). Also ist $j(z)$ für jeden dieser Punkte eine Nullstelle von ϕ_k.
Damit haben wir aber schon $n(k)$ verschiedene Nullstellen von ϕ_k gefunden. Da ϕ_k vom Grad $n(k)$ ist, kann es keine weiteren Nullstellen mehr geben. $\square$

5.1.3 Korollar.

- *Alle Nullstellen von ϕ_k sind einfach.*
- *Alle Nullstellen von ϕ_k sind reell und liegen im Intervall* $[0, 1728]$.

Beweis. Dies folgt aus dem Beweis des vorhergenden Satzes sowie der Tatsache, dass der Kreisbogenabschnitt I, auf dem die Nullstellen von E_k liegen, von j auf das Intervall $[0, 1728]$ abgebildet wird. □

5.1.4 Bemerkung. *Wir wissen bereits, dass die Nullstellen der E_k in gewisser Hinsicht im Kreisbogenabschnitt zwischen i und ρ gleichverteilt sind. Nun bildet j diesen Abschnitt bijektiv auf das Intervall* $(0, 1728)$ *ab, daher überträgt sich natürlich auch die Gleichverteilung im folgenden Sinne: Man kann das Intervall* $(0, 1728)$ *in $n(k)$ Intervalle unterteilen, und man weiß a priori, dass in jedem dieser Intervalle genau eine Nullstelle von ϕ_k liegt.*
Unglücklicherweise sind diese Intervalle jedoch weit davon entfernt, gleich groß zu sein. Es zeigt sich, dass die Intervalle am Rand von $(0, 1728)$ *sehr klein sind, während die Intervalle in der Mitte recht groß sind. Das bedeutet, dass viele Nullstellen der ϕ_k dicht beisammen liegen (nämlich in der Nähe von* 0 *und in der Nähe von* 1728*). Das ist von einem approximativen Standpunkt natürlich ungünstig, denn will man diese Nullstellen numerisch approximieren, muss man dies mit entsprechend großer Genauigkeit tun.*

5.2 Vermutungen über die Eisensteinpolynome

Es gibt noch weitere Auffälligkeiten der Eisensteinreihen, die empirisch beobachtet wurden. Da für diese Eigenschaften keine Beweise vorliegen, sind es natürlich nichts weiter als Vermutungen. Der folgende Punkt fasst einige davon zusammen.

5.2.1 Beobachtungen. *Die folgenden Aussagen haben sich für alle Eisensteinpolynome, die bisher überprüft wurden, als zutreffend erwiesen; sie sind aber bislang unbewiesen:*

(i) Jedes Eisensteinpolynom hat volle Galoisgruppe.

(ii) Die Nullstellen von ϕ_k separieren die Nullstellen von ϕ_{k+12}. Das heißt, dass zwischen je zwei Nullstellen von ϕ_{k+12} eine Nullstelle von ϕ_k zu finden ist.
Man kann die Aussage etwas präzisieren, wenn man berücksichtigt, dass

der Grad von ϕ_{k+12} genau um 1 größer ist als der von ϕ_k: Die Nullstellen von ϕ_k zerteilen das Intervall $(0, 1728)$ in $n(k)+1$ Teilintervalle. In jedem dieser Teilintervalle befindet sich nun genau eine Nullstelle von ϕ_{k+12}.

5.2.2 Bemerkung. *Es ist nicht ganz trivial, Begriffe wie „beliebig“ oder „zufällig ausgewählt“ für Polynome zu erklären. Insbesondere sind Serien wie die Eisensteinpolynome natürlich per Definition nicht zufällig ausgewählt, weil sie einer Definition genügen. Trotzdem kann man sagen, dass es für ein „beliebiges“ Polynom in einem gewissen Sinne sehr wahrscheinlich ist, dass es die volle Galoisgruppe hat. Es ist also nicht unbedingt überraschend, dass alle bislang überprüften Eisensteinpolynome diese Eigenschaft haben. Es könnte sich durchaus um einen Zufall handeln, und die Überraschung würde sich in Grenzen halten, wenn man hierzu irgendwann Gegenbeispiele finden würde, wenn es sich also um keine strukturelle Eigenschaft handelt.*
Die zweite Eigenschaft hat dagegen einen ganz anderen Charakter. Hat man zwei „zufällig ausgewählte“ Polynome, wobei der Grad des einen Polynoms um 1 größer ist als der des anderen Polynoms, so kann man nicht damit rechnen, dass die Nullstellen des zweiten Polynoms von denen des ersten separiert werden. Da sich diese Eigenschaft aber bei den Eisensteinpolynomen gleich auf ganze Serien erstreckt, muss hier wohl tatsächlich ein prinzipieller Grund vorliegen.
Allerdings gibt es auch hier ein Argument, das gegen eine Allgemeingültigkeit spricht. Betrachten wir statt des Eisensteinpolynoms hierzu wieder die Eisensteinreihen (für die diese Eigenschaft natürlich ganz analog gilt). Von diesen wissen wir aus dem Beweis von Satz 5.1.1, dass sich $E_k(e^{2\pi i\theta})$ in der Nähe des relevanten Kreisbogenabschnitts so ähnlich wie die Funktion $C \cdot \cos\left(\pi k \frac{\theta}{2}\right)$ verhält. Das heißt, dass die Nullstellen von E_k nahe bei den Nullstellen $\theta_{m,k} = \frac{2m+1}{k}$, $\left(\frac{k-6}{12} < m < \frac{k-4}{8}\right)$ der entsprechenden cos-Funktion liegen. Nun separieren die $\theta_{m,k+12}$ aber die $\theta_{m,k}$. Wenn man also davon ausgeht, dass die Nullstellen von E_k „nahe genug“ an den $\theta_{m,k}$ liegen, dann überträgt sich die Separierungseigenschaft auf die Nullstellen der E_k. Nun liegen die $\theta_{m,k}$ mit wachsendem k aber immer dichter beisammen, sodass die Nullstellen von E_k und der cos-Funktion immer weniger voneinander abweichen dürfen, damit sich die Eigenschaft noch überträgt. Es könnte also durchaus sein, dass die Separierungseigenschaft nur für kleine k gilt, und ab einer gewissen Grenze verloren geht.

Kapitel 6

Übertragung auf $\mathbb{Z}_p$

Die verblüffende Eigenschaft, dass die bislang untersuchten Reihen (oder zumindest ihre q-Entwicklungen) rationale Koeffizienten haben, zieht weitere Fragen nach sich: Erfüllen die Koeffizienten vielleicht besondere Teilbarkeits- oder doch doch zumindest Kongruenzeigenschaften? Die Antwort hierauf lautet: Ja, und zwar sehr viel stärkere Eigenschaften, als man zunächst vielleicht vermuten würde.
Um dem Leser einen Eindruck von der Vielfalt der auftretenden Kongruenzen zu geben, zitiere ich hier einige ausgewählte Sätze aus der Literatur:

6.0.3 Beispiele.

- *Ist $p \in \mathbb{P}$, $p > 5$, so sind die Nenner von E_{p-1} und E_{p+1} nicht durch p teilbar und es gilt:*

$$\begin{array}{rcll} E_{p-1} & \equiv & 1 & \mod p, \\ E_{p+1} & \equiv & E_4 & \mod p, \\ \frac{d}{dq}E_{p-1} & \equiv & E_{p+1} & \mod p, \\ \frac{d}{dq}E_{p+1} & \equiv & -E_6E_{p-1} & \mod p. \end{array}$$

  [Lan, Ch. X, Th. 7.1]

- *Sei $p \in \{2,3,5,7,13\}$, $N := 2^7 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 13$ und $k \geq 4$ gerade. Dann sind die Nenner von E_k und E_{k+12} nicht durch p teilbar und es gilt*

$$E_{k+12} \equiv E_k \mod N.$$

  [Gek, Th 3.1]

- *Seien $h, k \geq 4$ gerade. Sei p prim mit der Eigenschaft, dass die Nenner von E_k, E_h und E_{k+h} nicht durch p teilbar sind. Sei $r \geq 1$ und seien* *schließlich $q, a \in \mathbb{N}$. Die Gleichung*

$$E_{k+h} \equiv E_k \cdot E_h \bmod p^r \text{ für alle } k \equiv a \bmod q$$

ist zum Beispiel für die folgenden Tupel $T := (h, p, a, q, r)$ erfüllt:

$$\begin{aligned} T &= (4, 2, 10, 16, 10) \\ T &= (4, 2, 10, 32, 11) \\ T &= (4, 3, 6, 9, 5) \\ T &= (6, 2, 136, 256, 13) \\ T &= (8, 3, 0, 3, 5) \\ T &= (12, 13, 0, 12, 2) \end{aligned}$$

Dies ist nur ein kleiner Ausschnitt aus einer sehr viel umfangreicheren (und leicht erweiterbaren) Tabelle für T, die von Ernst-Ulrich Gekeler in [Ge2, Cor. 5.8] aufgestellt wurde. (Insbesondere impliziert sie auch das vorangegangene Beispiel).

Einige der obigen Aussagen lassen sich relativ leicht mit elementaren Mitteln beweisen. Will man jedoch ernsthafter an solche Fragestellungen herangehen, so empfiehlt es sich, die gesamte Theorie nicht mehr über $\mathbb{C}$, sondern vielmehr über $\mathbb{Z}_p$ auszuführen. Es stellt sich in der Tat heraus, dass sich die wesentlichen Resultate und Sätze in analoger Form übertragen, und dass man etwa aus den p-adischen Eisensteinreihen Rückschlüsse über die gewöhnlichen Eisensteinreihen ziehen kann. (So wird etwa die im letzten Beispiel zitierte Tabelle mit solchen Methoden gewonnen).
Unglücklicherweise ist die Übertragung der Theorie zwar kein sehr schwieriger (zumindest wenn man Grundkenntnisse in p-adischer Funktionentheorie voraussetzt), aber ein recht länglicher Prozess, weshalb ich hier nur die wesentlichen Ergebnisse ohne Beweise vorstellen werde.
Darüber hinaus werde ich in diesem Kapitel auch gewisse Grundkenntnisse p-adischer Zahlen und p-adischer Funktionentheorie voraussetzen. Der Leser kann sich in vielen Lehrbüchern mit dem Thema vertraut machen, zum Beispiel in [Mah] oder online in [Bak].

6.1 Eisensteinreihen über $\mathbb{Z}_p$

Wir wissen bereits, dass der Nenner der klassischen Eisensteinreihe E_k gerade der Zähler von $\frac{B_k}{2k}$ ist. Ist nun p ein Primteiler dieser Zahl, so ist es nicht verwunderlich, dass technische Probleme auftreten, wenn man die Reihe E_k

nach $\mathbb{Z}_p$ übertragen will. Deshalb werden wir solche Fälle hier ausschließen (Man beachte, dass uns dabei zu jedem k nur endlich viele Primzahlen p Probleme machen):

6.1.1 Definition/Vereinbarung. *Sei $p \in \mathbb{P}$ und $k \in \mathbb{Z}$. Das Paar (k,p) heißt* REGULÄR, *falls p kein Teiler des Zählers von $\frac{B_k}{2k}$ ist.*
Wir werden im Folgenden in diesem Kapitel immer davon ausgehen, dass die auftretenden Paare (k,p) regulär sind, sofern nichts anderes gesagt wird.

6.1.2 Bemerkung. *Reguläre Paare (k,p) haben vor allem einen großen Vorteil: Da der Nenner von E_k nicht durch p teilbar ist, ist er automatisch in $\mathbb{F}_{p^r}$ invertierbar (f ür alle $r \geq 1$). Die Koeffizienten von E_k lassen sich somit als Elemente von $\mathbb{F}_{p^r}$ auffassen, und es macht Sinn, von „$E_k \mod p^r$" zu sprechen.*

Um die Eisensteinreihen auf $\mathbb{Z}_p$ zu übertragen, modifizieren wir sie erst nach dem Vorbild von Serre [Se2] und Gekeler [Ge2]:

6.1.3 Definition. *Sei $p \in \mathbb{P}$, $k \geq 4$ gerade. Wir definieren*

$$\begin{aligned} B_k^* &:= \left(1 - p^{k-1}\right) B_k, \\ C_k^* &:= -\frac{2k}{B_k^*} = \frac{2k}{(1-p^{k-1})B_k}, \\ \sigma_l^*(n) &:= \sum_{d|n,(d,p)=1} d^l, \\ E_k^* &:= 1 + C_k^* \sum_{n=1}^{\infty} \sigma_{k-1}^*(n) q^n. \end{aligned}$$

*Wir nennen die E_k^* auch die p-*ADISCHEN EISENSTEINREIHEN.

Zunächst überzeugen wir uns davon, dass diese Abweichungen keine wesentliche Verfälschung darstellen:

6.1.4 Lemma. *Für alle geraden $k \geq 4$ (mit regulärem (k,p)) gilt:*

$$E_k \equiv E_k^* \mod p^{k-1}.$$

Beweis. Es ist sofort offensichtlich, dass $B_k^* \equiv B_k \mod p^{k-1}$ und $C_k^* \equiv C_k \mod p^{k-1}$ ist. Auch bei der Summe $\sigma_l^*(n)$ sieht man sofort, dass jeder weggelassene Summand (also jedes d^l mit $p|d|n$) durch p^{k-1} teilbar ist, sofern nur $l \geq k-1$ ist. Also stimmen auch $\sigma_l^*(n)$ und $\sigma_l(n)$ modulo p^{k-1} überein. Die Definition der Eisensteinreihen ist ansonsten identisch. ☐

Wieso gibt man sich nun die Mühe, die Eisensteinreihen in dieser Weise zu modifizieren?
Um das zu verstehen, sehe man sich die Funktion $a_n(k)$ an. Diese soll einem Index k den n-ten Koeffizienten der Eisensteinreihe E_k zuordnen. Entsprechend sei $a_n^*(k)$ der n-te Koeffizient der p-adischen Eisensteinreihe E_k^*. Dabei ist a_n zunächst einmal eine Funktion mit Werten in $\mathbb{Q}$. Man kann sie aber auch, ebenso wie a_n^*, als Funktion mit Werten in $\mathbb{Z}_p$ auffassen. Betrachtet man die beiden Funktionen in diesem Licht, so wird man feststellen, dass a_n^* gewissermaßen eine „geglättete" Version von a_n ist. Präzise ausgedrückt handelt es sich um eine Iwasawa-Funktion (sofern man den Definitionsbereich richtig wählt, siehe Satz 6.1.7). Sollte der Leser diesem Begriff noch nicht begegnet sein, so mag es hilfreich sein, sich solche Funktionen als p-adisches Pendant zu holomorphen Funktionen vorzustellen. Sie lassen insbesondere in mehrfacher Hinsicht eine Potenzreihenentwicklung zu. Detailliertere Anweisungen sind zum Beispiel in [Mah] zu finden.

Für uns ist vor allem eine Eigenschaft von Iwasawa-Funktionen wichtig (die den Leser kaum überraschen wird, wenn er an holomorphe Funktionen oder an Potenzreihen als Vergleich denkt): Wenn eine Funktion an „genügend vielen" Stellen verschwindet, so ist sie schon identisch 0. Es gilt außerdem die Verschärfung, dass eine Funktion, die an den richtigen (diesmal endlich vielen) Stellen modulo p^r verschwindet, schon modulo p^r identisch 0 sein muss. Technisch korrekt ausgedrückt liest sich dies als:

6.1.5 Satz. *Sei $p > 2$ prim. Sei $f : X \to \mathbb{Z}_p$ eine Iwasawa-Funktion, wobei X ein Intervall der Länge p^{-t} sei, d.h. $X = k + p^t\mathbb{Z}_p$ für ein $k \in \mathbb{Z}_p$ und ein $t \geq 0$.*
Sei $k_1, k_2, ..., k_r$ eine arithmetische Folge der Länge r in X gegeben, deren Schrittweite nicht durch p^{t+1} teilbar ist (durch p^t ist die Schrittweite schon automatisch teilbar, wenn die Folge in X liegen soll).
Gilt

$$f(k_i) \equiv 0 \mod p^r \text{ für alle } i \in \{1, \ldots, r\},$$

so ist schon $f \equiv 0 \mod p^r$ auf ganz X.

6.1.6 Bemerkung. *In obigem Satz wurde die Primzahl $p = 2$ ausgeschlossen. Der Satz gilt aber sinngemäß auch für diese Zahl, nur unterscheidet sich die Zahl der benötigten Nullstellen $\bmod 2^r$. (Man benötigt $\left\lfloor \frac{r+1}{2} \right\rfloor$ solche Stellen.) Dies liegt letztendlich daran, dass die Einheitengruppe in $\mathbb{Z}_2$ anders aussieht als in den anderen $\mathbb{Z}_p$. Dadurch wird es meistens nötig, diese beiden Fälle zu unterscheiden. Allerdings ist es in sehr vielen Fällen so, dass man (ähnlich wie beim obigen Satz) analoge Aussagen erhält, die sich nur durch minimale technische Feinheiten unterscheiden.*

Nun wollen wir diese Aussage natürlich auf unsere Situation übertragen. Dazu müssen wir erst die etwas schlampige Aussage, dass a_n^* eine Iwasawa-Funktion sei, präzisieren. Der folgende Satz geht auf Serre zurück und findet sich (leicht abgewandelt) mitsamt einer Beweisskizze in [Se2, S. 245].

6.1.7 Satz. *Sei (k_0, p) regulär. Sei $\mathcal{C} := \{k \in \{4, 6, 8, 10, ...\} | k \equiv k_0 \mod p-1\}$.*
Dann ist für jedes $n \geq 0$ die Funktion $a_n^* : \mathcal{C} \to \mathbb{Z}_p; k \mapsto a_n^*(k)$ eine Iwasawa-Funktion auf $\mathcal{C}$.

Nun können wir die Ergebnisse kombinieren, und erhalten:

6.1.8 Satz. *Sei $p > 2$ prim, k_0 und $\mathcal{C}$ wie im vorangegangen Satz, und sei $k_1, ..., k_r$ eine arithmetische Folge in $\mathcal{C}$, deren Schrittlänge von p^r, nicht aber von p^{r+1} geteilt wird. Außerdem sollen alle Folgenglieder $\geq r+1$ sein.*
Wenn für jedes k aus dieser Folge jeweils die beiden Reihen E_{k+k_0} und $E_k \cdot E_{k_0}$ modulo p^r übereinstimmen, dann ist schon generell

$$E_{k+k_0} \equiv E_k \cdot E_{k_0} \mod p^r \quad \textbf{\textit{für alle}}\ k \geq r+1. \tag{6.1}$$

6.1.9 Bemerkung.

- *Der Beweis besteht aus dem Zusammenführen der bisher festgehaltenen Tatsachen. Die einzige Ingredienz, die bislang noch nicht erwähnt wurde, ist die Tatsache, dass nicht nur die Koeffizienten der E_k^* eine (bzw. mehrere) Iwasawafunktion ergeben, sondern auch die Koeffizienten des Produktes $E_k^* \cdot E_{k_0}$.*
  Die Einschränkungen $k \geq r+1$ kommen übrigens jeweils daher, dass für kleinere k die Reihen E_k und E_k^* nicht unbedingt modulo p^r übereinstimmen müssen.
  Einen ausführlichen Beweis findet der Leser in [Ge2, Satz 5.4]. In der selben Arbeit findet sich außerdem eine umfangreiche Tabelle von konkreten Äquivalenzen, die aus dem obigen Satz abgeleitet wurden.

- *Ich möchte dem Leser nochmals daran erinnern, dass implizit in diesem Kapitel vorausgesetzt wird, dass die auftretenden Paare (k, p) regulär sind. In diesem Fall heißt das, dass der Satz nur dann gilt, wenn das Paar (k_0, p) und alle Paare (k, p) und $(k + k_0, p)$ regulär sind ($k \in \mathcal{C}$).*

- *Die Einschränkung $p > 2$ ist wieder rein technisch. Der einzige Unterschied im Falle $p = 2$ ist, dass die Länge der arithmetischen Folge anders ist. (siehe wiederum [Ge2, Satz 5.4] für eine genaue Formulierung).*

- *Der Leser mag einwenden, dass man vom Regen in die Traufe komme: Um zu überprüfen, dass die Modulformen E_{k+k_0} und $E_k \cdot E_{k_0}$ modulo p^r übereinstimmen, muss man ja vermeintlich immer noch unendlich viele Koeffizienten untersuchen.*
  Es stellt sich aber glücklicherweise heraus, dass man hierfür nur endlich viele Werte überprüfen muss. Stimmen nämlich zwei Modulformen vom Gewicht k in den ersten $\left\lfloor \frac{k}{12} + 1 \right\rfloor$ Koeffizienten (mod p^r) überein, so sind sie schon (mod p^r) identisch. (Dies folgt zum Beispiel aus [Gek, Lemma 2.3])
  Benutzt man dieses Prinzip, kann man also tasächlich eine allgemeine Regel wie in Gleichung 6.1 durch endlich viele Rechnungen testen.

Teil III

Kapitel 7

Anhänge

7.1 Anhang A: Konvergenz der Eisensteinreihen

Die Eisensteinreihe wird bekanntlich über die Potenzreihe

$$E_k(z) := \frac{1}{2\zeta(k)} \sum_{m,n}{}' \frac{1}{(mz+n)^k}$$

definiert.
Wir wollen beweisen, dass diese Potenzreihe für $k > 2$ konvergiert.
Sei dazu $z \in \mathbb{H}$ und $c > 0$ eine Konstante mit $\Im(z) \geq c$.
Um das Argument etwas zu vereinfachen, werden wir die absolute (bzw. gleichmäßige) Konvergenz bezüglich der Norm $\|z\| := \max\{|\Re(z)|, \frac{1}{c}|\Im(z)|\}$ nachrechnen. Da auf $\mathbb{R}^n$ und somit auf $\mathbb{C}$ alle Normen äquivalent sind, genügt es, die Konvergenz für eine beliebige Norm nachzuweisen.
Sehen wir uns an, für wie viele Paare (m, n) die Ungleichung $\|mz + n\| < n_0$ gilt (für eine Konstante $n_0 \in \mathbb{N}$):
Dazu muss erstens $|\frac{1}{c}\Im(mz + n)| = m\frac{|\Im(z)|}{c} < n_0$ gelten. Dies ist höchstens für $m \in]-n_0, n_0[$ erfüllt.
Zusätzlich muss außerdem noch $|\Re(mz + n)| < n_0$ sein, was bei fixiertem m nur $2n_0$ viele n erfüllen können.
Insgesamt gibt es also weniger als $4n_0^2$ Paare (m, n), für die der Summand $||\frac{1}{mz+n}|| > n_0$ ist. Wir erhalten also die Abschätzung

$$\sum_{m,n}{}' \left\| \frac{1}{(mz+n)^k} \right\| < \sum_{n_0=1}^{\infty} (4(n_0+1)^2 - 4n_0^2) \cdot \frac{1}{n_0^k} = \sum_{n_0=1}^{\infty} \frac{8n_0+4}{n_0^k} < \infty$$

für $k > 2$.

7.1.1 Bemerkung. *Anschaulich ist die Konvergenz auch relativ klar: Hat man im $\mathbb{R}^n$ ein $(n-1)$-dimensionales Gitter, so hat eine Fundamentalmasche ein bestimmtes, festes Volumen. In einer Kugel vom Radius R können daher nur $O(R^n)$ viele Fundamentalmaschen liegen. Die Anzahl der Gitterpunkte in der Kugel entspricht aber (von den Rändern abgesehen) exakt der Anzahl der Maschen in dieser Kugel (man nehme im $\mathbb{R}^2$ beispielsweise die Bijektion, die jeder Masche die linke untere Ecke zuordnet). Also ist die Anzahl der Gitterpunkte in dieser Kugel ebenfalls in $O(R^n)$.*
Vergrößert man den Radius der Kugel nun von R auf $R+1$, so vergrößert sich das Volumen (und damit die Anzahl der Gitterpunkte) um $O(R^{n-1})$. Man bekommt daher die Überschlagsrechnung

$$\sum_{w \text{ Gitterpunkt}} \frac{1}{\|w\|^k} \approx \sum_{R=1}^{\infty} R^{n-1} \cdot \frac{1}{R^k} = \sum_{R=1}^{\infty} R^{n-k-1},$$

wobei das Zeichen $\approx$ im Sinne der O-Notation zu verstehen ist.
Die vereinfachte Reihe konvergiert bekanntlich für $n-k-1 < -1$, also für $k > n$. Insbesondere ergibt sich für $\mathbb{C} = \mathbb{R}^2$ die Bedingung $k > 2$. Man beachte auch, dass der Exponent k nicht notwendig aus $\mathbb{Z}$ stammen muss.

7.2 Anhang B: Bernoullizahlen

7.2.1 Definition. *Die* Bernoullizahlen *B_k sind die eindeutig bestimmten Zahlen, die die Potenzreihenidentität*

$$\frac{X}{e^X - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} X^k$$

erfüllen.

7.2.2 Bemerkung.

- *Ab $k = 3$ verschwinden alle Bernoullizahlen mit ungeradem Index.*
- *Die ersten Bernoullizahlen sind $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = -\frac{691}{2730}$.*
  Es gibt außerdem explizite Rekursionsformeln für die Berechnung der Bernoullizahlen. Die Berechnung dieser Zahlen ist zudem in den gängigen Computeralgebra-Programmen implementiert.
- *Die Vorzeichen der Bernoullizahlen mit geradem Index alternieren ab $k = 2$.*

- *Ist* $p \in \mathbb{P}$, $l, m, n \geq 0$ *mit* $m \equiv n \bmod (p-1)p^l$ *und mit* $n \not\equiv 0 \bmod p-1$, *so gelten die* Kummer-Kongruenzen*:*

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} \bmod p^{l+1}.$$

  Insbesondere für $l=0$*: Ist* $m \equiv n \not\equiv 0 \bmod p-1$*, so ist*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \bmod p.$$

- *(*von Staudt-Clausen:*) Die Zahl*

$$B_{2n} + \sum_{p\in\mathbb{P},\ (p-1)|2n} \frac{1}{p}$$

  liegt in $\mathbb{Z}$*.*

  Dieser Satz zeigt insbesondere, dass im Nenner von B_{2n} *höchstens Primteiler p auftauchen können, die die Bedingung* $(p-1)|2n$ *erfüllen. Man kann die Nenner der Bernoullizahlen also schon a priori sehr gut kontrollieren.*

Über die Bernoullizahlen sind buchstablich unzählige Identitäten bekannt. Ich habe hier nur eine winzige Auswahl davon wiedergeben. In praktisch jedem mathematischen Übersichtsbuch findet sich ein ausführlicher Abschnitt über diese Zahlen, wie z.B. [Spa, Ch. 4: „The Bernoulli Numbers“]. Sollte der Leser Interesse an Beweisen zu den oben angeführten Aussagen haben, so wird er keine Schwierigkeiten haben, sie in der Literatur zu finden.
Ein wenig muss man aber aufpassen, da die Bernoullizahlen vor allem in älteren Büchern oft etwas anders definiert sind. Diese oft mit B_k^* bezeichneten Zahlen erfüllen dann $B_k^* = (-1)^{k-1}B_{2k}$.

7.2.3 Proposition. *Die Werte der Riemannschen Zeta-Funktion an geraden Stellen lassen sich mit Hilfe der Bernoullizahlen wie folgt berechnen:*

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

Beweis. siehe z.B. [Lan, 4.1: „The Bernoulli Numbers B_k“]
(Vorsicht, denn Lang benutzt die andere Definition der Bernoullizahlen!) □

7.3 Anhang C: asymptotisches Wachstum

Bei Fragen, die die Laufzeit von Computerprogrammen betreffen, hat es sich eingebürgert, diese Laufzeit aus Gründen der Einfachheit nur asymptotisch genau anzugeben. Dabei stehen einem die folgenden Symbole zur Verfügung:

$f \in O(g)$	f wächst asymptotisch höchstens so schnell wie g, d.h. $\frac{f(x)}{g(x)}$ bleibt beschränkt, wenn $x \to \infty$.
$f \in o(g)$	f wächst asymptotisch langsamer als g, d.h. $\frac{f(x)}{g(x)} \to 0$, wenn $x \to \infty$.
$f \in \Omega(g)$	f wächst asymptotisch mindestens so schnell wie g, d.h. $\frac{g(x)}{f(x)}$ bleibt beschränkt, wenn $x \to \infty$.
$f \in \omega(g)$	f wächst asymptotisch schneller als g, d.h. $\frac{g(x)}{f(x)} \to 0$, wenn $x \to \infty$.
$f \in \Theta(g)$	f und g wachsen asymptotisch gleich schnell, d.h es gilt $f \in O(g)$ und $g \in O(f)$.

Die Bezeichnungen „langsamer als" usw. können hier ganz intuitiv behandelt werden; so implizieren beispielsweise die Aussagen „f wächst langsamer als g" und „g wächst langsamer als h" die Aussage „f wächst langsamer als h". (Präzise ausgedrückt: Man hat hier eine partielle Ordnungsrelation vorliegen).
Die wichtigsten Vergleichsfunktionen für Laufzeiten stellen dabei exponentielle ($\Theta(a^n)$, für ein $a > 1$) und polynomiale ($\Theta(n^k)$, für ein $k > 0$) Funktionen dar. (Wobei mit den angegebenen Einschränkungen an a und k jedes exponentielle Wachstum schneller ist als jedes polynomielle Wachstum).

Folgende Faustregeln lassen sich für die Praxis formulieren:

- Ist die Laufzeit eines Programmes exponentiell, so ist das Programm unbrauchbar.

- Ist die Laufzeit in $O(n)$ oder unwesentlich schlechter (z.B. $O(n \log(n))$), so ist das Programm gut.

- Hat ein Programm polynomielle Laufzeit mit Exponenten $k \geq 2$, so ist es in der Regel nur sehr eingeschränkt brauchbar. Teilweise lassen sich kleinere Beispiele noch durchrechnen, aber das Programm wird vermutlich sehr schnell an seine Grenzen stoßen.

Literaturverzeichnis

[Mat] http://mathworld.wolfram.com/

[Bak] A.J.Baker, An Introduction to p-adic Numbers and p-adic Analysis, 2004, http://www.maths.gla.ac.uk/∼ajb/dvi-ps/padicnotes.pdf

[Car] H. Cartan, Thorie lmentaire des fonctions analytiques d'une ou plusieurs variables complexes, Hermann, Paris, 1961

[Fre] Freitag-Busam, Funktionentheorie, Springer, Heidelberg, 2000 http://www.rzuser.uni-heidelberg.de/ t91/

[Gek] Ernst-Ulrich Gekeler, Some Observations on the Arithmetic of Eisenstein Series for the Modular Group $SL(2, \mathbb{Z})$, Archiv der Mathematik, Vol.77, Nr.1, Seite 5ff., 2001

[Ge2] Ernst-Ulrich Gekeler, A Series of New Congruences for Bernoulli Numbers an Eisenstein Series, Journal of Number Theory 97, Seite 132ff., 2002

[Jef] Alan Jeffrey, Handbook of Mathematical Formulas and Integrals, Academic Press, 2000

[Hur] Adolf Hurwitz, Mathematische Werke, Birkhäuser, Band I, 1932

[Kre] Bernd Kremling, Diskriminanten und Resultanten einer arithmetisch definierten Folge von Polynomen über $\mathcal{F}_q(T)$, Diplomarbeit an der Universität des Saarlandes, Saarbrücken, 1999

[Lan] Serge Lang, Introduction to Modular Forms, Springer Berlin Heidelberg New York, A Series of Comprehensive Studies in Mathematics 222, 1976

[La2] Serge Lang, Elliptic Functions, Addison Wesley, 1973

[LEDA] C++ Library of Efficient Data Structures and Algorithms, `http://www.algorithmic-solutions.com`

[Mah] K. Mahler, Introduction to p-adic Numbers and their Function, Second Edition, Cambridge University Press, 1981

[Meh] Kurt Mehlhorn, Data Structures and Efficient Algorithms, Vol. 2, Springer Verlag, 1986, teilweise online unter `http://www.mpi-sb.mpg.de/~mehlhorn/DatAlgbooks.html`

[Ram] S. Ramanujan, On Certain Arithmetical Functions, Trans. Cambridge phil. Soc., 22, 1916

[Ran] F.K.C. Rankin und H.P.F. Swinnerton-Dyer, On the Zeros of Eisenstein Series, Bull. London Math. Soc. 2, Seite 169f., 1970

[Ser] Jean Pierre Serre, A Course in Arithmetic, Springer, New York, 1973

[Se2] Jean Pierre Serre, Formes modulaires et fonctions zta p-adiques, Lecture Notes in Mathematics, Vol. 350, Springer-Verlag, Berlin, 1973

[Sil] Joseph H. Silverman, The Arithmetic of Elliptic Curves. Springer-Verlag, New York, 1986

[Spa] J. Spanier und K. B. Oldham, An Atlas of Functions, Springer Berlin, 1987

[Swi] H.P.F. Swinnerton-Dyer, On l-adic Representations and Congruences for Coefficients of Modular Forms, Lecture Notes in Mathematics, Bd. 350, Springer Berlin Heidelberg New York, 1972