Matematisk-fysiske Meddelelser
udgivet af
Det Kongelige Danske Videnskabernes Selskab
Bind **34**, nr. 7

Mat. Fys. Medd. Dan. Vid. Selsk. **34**, no. 7 (1964)

DIE FOURIERKOEFFIZIENTEN DER EISENSTEINREIHEN ZWEITEN GRADES

VON

HANS MAASS

København 1964
Kommissionær: Ejnar Munksgaard

Synopsis

Die Fourierkoeffizienten $a_k(T)$ der Eisensteinreihen zur Modulgruppe n-ten Grades und zur Dimension $-k$ lassen sich, wenn man von einem elementaren Faktor absieht, nach C. L. SIEGEL als Produkt gewisser p-adischer Darstellungsdichten schreiben. Durch Berechnung dieser Dichten gelangt man im Falle $n = 2$ zu einer expliziten Formel für die $a_k(T)$ zu primitiven Matrizen T. Auf diesen speziellen Fall kann die Berechnung beliebiger Fourierkoeffizienten mit Hilfe einer Rekursionsformel zurückgeführt werden, die man aus der verallgemeinerten Heckeschen Operatorentheorie bezieht. Eine eingehende Analyse ergibt nun für die rationalen Zahlen $a_k(T)$ im Falle $n = 2$ bei festem k einen gemeinsamen Nenner, der sich nur aus irregulären Primzahlen (im Sinne Kummers) zusammensetzt. Für $k = 4, 6, 8, 10, 12$ wird insbesondere der größte gemeinsame Teiler aller $a_k(T)$ mitgeteilt.

PRINTED IN DENMARK
BIANCO LUNOS BOGTRYKKERI A/S

Die Fourierkoeffizienten $a_k(T)$ der von C. L. SIEGEL eingeführten Eisensteinreihen n-ten Grades zur Dimension $-k$ $\left(k \equiv 0 \pmod 2,\ k > n+1\right)$:

$$G_{-k}(Z) = \sum_{\{C,D\}} |CZ+D|^{-k}, \tag{1}$$

wobei über ein volles System von n-reihigen nicht-assoziierten teilerfremden symmetrischen Matrizenpaaren C,D summiert wird und Z eine symmetrische komplexe Matrix mit positivem Imaginärteil bezeichnet, sind bisher wenig untersucht worden. Es ist seit langem bekannt [4], daß diese Koeffizienten rational sind und von Fall zu Fall numerisch berechnet werden können. Solche Berechnungen werden aber selbst im Falle $n = 2$ als sehr mühselig angesehen [1]. Eine interessante Entdeckung Siegels, die wesentlich über [4] hinausführt, ist neueren Datums [6]. Sie besagt, daß das Produkt der gekürzten Zähler der k mit Bernoullischen Zahlen gebildeten Quotienten $\frac{B_{2\nu}}{2\nu}$ $(\nu = 1,2,\ldots,k-1)$ und $\frac{B_k}{k}$, von einer Potenz von 2 abgesehen, einen gemeinsamen Nenner aller $a_k(T)$ bei gegebenen k und n bildet. Einem Satz von K. L. JENSEN [2] zufolge setzen sich die gekürzten Nenner der $a_k(T)$ demnach nur aus der Primzahl 2 und gewissen irregulären Primzahlen p zusammen. p heißt irregulär, wenn die Klassenzahl des Körpers der p-ten Einheitzwurseln durch p teilbar ist. Die Bernoullischen Zahlen B_ν werden hier in ihrer Gesamtheit symbolisch $(B^\nu \to B_\nu)$ durch $(B+1)^h - B^h = 0$ für $h \geqq 2$ definiert.

Bei dieser Sachlage hielt ich eine Beschränkung auf den Fall $n = 2$ für gerechtfertigt, um die Analyse der $a_k(T)$ möglichst weit treiben zu können. Wir setzen nun

$$2T = \begin{pmatrix} 2t_0 & t_1 \\ t_1 & 2t_2 \end{pmatrix} \quad \text{und} \quad e(T) = \text{g.g.T.}(t_0,t_1,t_2) \tag{2}$$

mit ganz rationalen t_0,t_1,t_2. Es darf und soll angenommen werden, daß T positiv ist, da $a_k(T)$ im Falle $|T| = 0$ als Fourierkoeffizient einer Eisen-

steinreihe ersten Grades hinreichend bekannt ist. Es gelingt die explizite Berechnung von $a_k(T)$ für primitive, durch $e(T) = 1$ gekennzeichnete T. Der Fall eines beliebigen $T > 0$ wird auf den soeben bezeichneten Spezialfall mit Hilfe einer allgemeinen Koeffizientenrelation aus der Theorie der verallgemeinerten Heckeschen Operatoren [3] rekursiv zurückgeführt. Auf Grund der angegebenen Formeln ist festzustellen, daß $a_k(T)$ bei gegebenem k im Falle $n = 2$ durch $e(T)$ und $|2T|$ eindeutig bestimmt ist. Dieser Satz steht in bemerkenswerter Analogie zu der Aussage, daß die Klassenzahl des Geschlechts von $2T$ nur von den Ordnungsinvarianten, nämlich $e(T)$ und $|2T|$ abhängt, stellt aber wohl eine Besonderheit des Falles $n = 2$ dar. Ferner ergibt sich, daß ein gemeinsamer Nenner der Koeffizienten $a_k(T)$ zu primitiven T bei gegebenem k auch ein Nenner aller $a_k(T)$ ist. Schließlich zeigt sich, daß

$$m_k = \frac{k(2k-2)}{qB_kB_{2k-2}} \tag{3}$$

im Falle $n = 2$ ein gemeinsamer Teiler aller $a_k(T)$ mit $T > 0$ ist. Hierin ist q der größte Teiler von $(k-1)N_{2k-2}$, der sich nur aus Primteilern $p \equiv -1 \pmod 4$ des gekürzten Nenners N_{2k-2} von B_{2k-2} zusammensetzt. Diese Teilbarkeitsaussage stellt eine Verschärfung des Siegelschen Resultats für den Spezialfall $n = 2$ dar. Tatsächlich ist m_k für $k = 4,6,8,10,12$ sogar der größe gemeinsame Teiler der Fourierkoeffizienten $a_k(T)$ mit $T > 0$.

§ 1. Die allgemeine Koeffizientenformel

Für beliebiges n, halbganze symmetrische Matrizen $T > 0$ und gerades $k > n+1$ entnimmt man aus [4] die Darstellung

$$a_k(T) = (-1)^{\frac{nk}{2}} 2^{n\left(k-\frac{n-1}{2}\right)} \prod_{\nu=0}^{n-1} \frac{\pi^{k-\frac{\nu}{2}}}{\Gamma\left(k-\frac{\nu}{2}\right)} |T|^{k-\frac{n+1}{2}} \prod_p S_p, \tag{4}$$

wobei p alle Primzahlen durchläuft und S_p den p-Beitrag zur sogenannten singulären Reihe bezeichnet. Er ist gegeben durch

$$S_p = \sum_{R_p \bmod 1} e^{-2\pi i \sigma(TR_p)} (\nu(R_p))^{-k}. \tag{5}$$

Summiert wird hier über ein vollständiges System mod 1 verschiedener n-reihiger symmetrischer rationaler Matrizen R_p mit einer Potenz von p als

Nenner. $\nu(R_p)$ bezeichnet das Produkt der gekürzten Nenner der Elementarteiler von R_p und allgemein $\sigma(A)$ die Spur von A. Um S_p in gewisser Weise als p-adische Darstellungsdichte zu deuten, empfiehlt sich in der weiteren Behandlung von S_p gegenüber [4] eine geringfügige Modifikation, die auf einem Gedanken von E. WITT [7] beruht. Sie gestattet eine einheitliche Behandlung aller Primzahlen sowie eine Vereinfachung in der Berechnung der benötigten Gaußschen Summen und führt schließlich zu dem Ergebnis in der gewünschten Form. Um $(\nu(R_p))^{-k}$ in geeigneter Weise durch Gaußsche Summen auszudrücken, führen wir

$$G = \sum_{K \bmod q} e^{2\pi i \sigma(FR_p[K])} \qquad (q = p^a) \tag{6}$$

mit

$$F = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$$

ein. a sei so groß gewählt, daß qR_p ganz ist. Summiert wird über ein volles System $\bmod q$ verschiedener ganzer Matrizen $K = K^{(n,2)}$.

Da G nur von $R_p \bmod 1$ abhängt und gegenüber den Transformationen $R_p \to R_p[U]$ mit unimodularen Matrizen U invariant ist, so kann R_p in G durch eine Normalform der folgenden Art ersetzt werden:

$$R_p[U] \equiv \left(\begin{array}{cccc|ccc} a_1 q^{-\mu_1} & & & 0 & & & \\ & a_2 p^{-\mu_2} & & & & 0 & \\ & & \ddots & & & & \\ 0 & & & a_r p^{-\mu_r} & & & \\ \hline & & & & F_1 p^{-\nu_1} & & 0 \\ & & & & & F_2 p^{-\nu_2} & \\ & 0 & & & & & \ddots \\ & & & & 0 & & \\ & & & & & & F_s p^{-\nu_s} \end{array}\right) \pmod 1.$$

Hierin ist

$$F_h = \begin{pmatrix} \alpha_h & \beta_h \\ \beta_h & \gamma_h \end{pmatrix} \quad (h = 1,2,\ldots,s),$$

also $r + 2s = n$, und

$$(a_h, p) = (\beta_h, p) = 1, \quad \alpha_h \equiv \gamma_h \equiv 0 \pmod p.$$

Im Falle $p > 2$ kann überdies $s = 0$ angenommen werden, wovon hier jedoch kein Gebrauch gemacht wird. Offenbar ist

$$\nu(R_p) = \nu(R_p[U]) = p^{\mu_1 + \ldots + \mu_r + 2\nu_1 + \ldots + 2\nu_s}.$$

Mit der angegebenen Normalform an Stelle von R_p in G und der Zerlegung

$$K' = (\mathfrak{l}_1, \ldots, \mathfrak{l}_r, L_1 \ldots, L_s), \quad \mathfrak{l}_h = \mathfrak{l}_h^{(2,1)}, \quad L_h = L_h^{(2)}$$

ergibt sich unmittelbar, wenn unnötige Indices nachträglich gestrichen werden,

$$\begin{aligned} G &= \prod_{h=1}^{r} \sum_{\mathfrak{l} \bmod q} e^{2\pi i a_h p^{-\mu_h} F[\mathfrak{l}]} \prod_{h=1}^{s} \sum_{L \bmod q} e^{2\pi i p^{-\nu_h} \sigma(F[L] F_h)} \\ &= q^{2(r+2s)} p^{-\mu_1 - \ldots - \mu_r - 2\nu_1 - \ldots - 2\nu_s} \end{aligned}$$

oder auch

$$G^k = q^{2nk} (\nu(R_p))^{-k}.$$

Andererseits folgt mit

$$H = H^{(2k)} = \begin{pmatrix} F & & 0 \\ & F & \\ & & \ddots \\ 0 & & F \end{pmatrix},$$

da diese Matrix mit Hilfe einer unimodularen Matrix in

$$S = \begin{pmatrix} 0 & \frac{1}{2}E \\ \frac{1}{2}E & 0 \end{pmatrix} \quad (E = E^{(k)} = \text{Einheitsmatrix})$$

übergeführt werden kann,

$$\begin{aligned} G^k &= \prod_{h=1}^{k} \sum_{K_h \bmod q} e^{2\pi i \sigma(F R_p[K_h])} \\ &= \sum_{K \bmod q} e^{2\pi i \sigma(H R_p[K])} = \sum_{K \bmod q}' e^{2\pi i \sigma(S R_p[K])}, \end{aligned}$$

wobei $K = K^{(n,2k)} = (K_1, K_2, \ldots, K_k)$ gesetzt ist. Nunmehr schließt man wie in [4] und erhält

$$S_p = \lim_{a \to \infty} q^{\frac{n(n+1)}{2} - 2nk} A_q(T), \tag{7}$$

wenn $A_q(T)$ die Anzahl der mod q verschiedenen ganzen Matrizen $C = C^{(2k,n)}$ bezeichnet, für welche $\frac{2}{q}(S[C] - T)$ eine gerade ganze Matrix wird. Die Rationalität von S_p ist eine Folge von

Lemma 1: *Es seien $S = S^{(m)}$ und $T = T^{(n)}$ mit $m \geqq n$ halbganze symmetrische Matrizen, p eine Primzahl und p^b die höchste Potenz von p, welche $|2T|$ teilt. Wir setzen $q = p^a$ und bezeichnen mit $A_q(S,T)$ die Anzahl der* mod q *verschiedenen ganzen Matrizen $C = C^{(m,n)}$, für welche $\frac{2}{q}(S[C] - T)$ eine gerade ganze Matrix wird. Ist $a > 2b$, so ist $q^{\frac{n(n+1)}{2} - mn} A_q(S,T)$ von a unabhängig.*

Für $p > 2$ deckt sich die Aussage dieses Lemmas mit einer Teilaussage von Hilfssatz 13 in [5]. Der Fall $p = 2$ erfordert keine wesentlich neuen Überlegungen und läßt sich in den Beweis entsprechend mit einbeziehen.

Um $A_q(T)$ als Lösungszahl eines Systems von Kongruenzen zu interpretieren, zerlegen wir C in

$$C = \begin{pmatrix} G \\ H \end{pmatrix} \quad \text{mit} \quad G = G^{(k,n)}, \quad H = H^{(k,n)}.$$

$A_q(T)$ ist dann die Anzahl der mod q verschiedenen ganzen Matrizenpaare G,H, für welche

$$\frac{1}{q}(G'H + H'G - 2T) \quad \text{ganz und gerade} \tag{8}$$

ist. Bezeichnen $\mathfrak{g}_1, \mathfrak{g}_2, \ldots \mathfrak{g}_n$ bzw. $\mathfrak{h}_1, \mathfrak{h}_2, \ldots, \mathfrak{h}_n$ die Spalten von G bzw. H und wird $2T = ((1 + \delta_{\mu\nu})t_{\mu\nu})$ mit dem Kroneckersymbol $\delta_{\mu\nu}$ gesetzt, so tritt an Stelle von (8) das gleichwertige Kongruenzensystem

$$\left.\begin{aligned} \mathfrak{g}'_\alpha \mathfrak{h}_\alpha \equiv t_{\alpha\alpha}, \quad \mathfrak{g}'_\alpha \mathfrak{h}_\beta + \mathfrak{g}'_\beta \mathfrak{h}_\alpha \equiv t_{\alpha\beta} \pmod q \\ (1 \leqq \alpha, \beta \leqq n, \quad \alpha \neq \beta) \end{aligned}\right\} \tag{9}$$

Es ist zu beachten, daß sich die Lösungszahl $A_q(T)$ nicht ändert, wenn man T mit einer unimodularen Matrix V transformiert und mit einer zu q primen ganzen Zahl g multipliziert; denn die Forderung (8) bleibt bei einer simultanen Transformation

$$T \to gT[V], \quad H \to UHV, \quad G \to gU^*GV$$

erhalten, wenn neben V auch U eine unimodulare Matrix $\bmod q$ ist, so daß eine ganze Matrix U^* mit $U'U^* \equiv E(q)$ existiert. Wir benutzen diesen Sachverhalt im Falle $n = 2$, um zunächst T geeignet zu normieren. Sodann bestimmen wir die $H \bmod q$, für welche das System (9) Lösungen besitzt. Wegen der angegebenen Invarianz genügt es, wenn aus der Klasse der mit H äquivalenten Matrizen $\{UH \mid U \text{ unimodular } \bmod q\}$ jeweils ein eindeutig bestimmter Repräsentant H ausgewählt wird. Die Anzahl der Lösungen $G \bmod q$ hängt offenbar nur von der Äquivalenzklasse von $H \bmod q$ ab.

§ 2. Die Berechnung von $a_k(T)$ im Falle $e(T) = 1$

Wir befassen uns fortan nur noch mit dem Fall $n = 2$. $d = d(T)$ bezeichne durchweg die Diskriminante des imaginär-quadratischen Zahlkörpers, der von $\sqrt{-|2T|}$ erzeugt wird; sie ist gegenüber den invertierbaren Transformationen $T \to gT[V]$ mit rationalen g und $V = V^{(2)}$ invariant. Es sei p eine vorgegebene Primzahl, p^b die höchste Potenz von p, welche $|2T|$ teilt, und $q = p^a$ mit beliebigem $a > b$. Unter der Voraussetzung $e(T) = 1$ darf angenommen werden, daß T unter die drei Typen fällt, die durch die Kongruenzen

$$t_0 \equiv 1(q)\begin{cases} t_1 \equiv 0 \ (q) & \begin{cases} t_2 \equiv up^b \ (q), & p > 2 \\ t_2 \equiv u2^{b-2} \ (q) \end{cases} \\ t_1 \equiv 1 \ (2), & t_2 \equiv u2^c \ (q) \end{cases} \Bigg\} \begin{matrix} \\ p = 2 \end{matrix} \Bigg\} u \not\equiv 0 \ (p) \qquad (10)$$

definiert werden; denn für $gT[V]$ trifft dies zu, wenn die unimodulare Matrix V und die zu q prime ganze Zahl g geeignet gewählt werden. Wegen $a > b$ erscheint b in (10) in richtiger Bedeutung. Im dritten Fall ist c irgend eine nicht negative ganze Zahl. Entsprechend den drei Fällen (10) gilt

$$-|2T| \equiv \begin{cases} -4up^b \\ -u2^b \\ t_1^2 - u2^{c+2} \end{cases} (\bmod q) \quad \text{für} \begin{cases} p > 2 \\ p = 2 \begin{cases} b \geqq 2 \\ b = 0 \end{cases} \end{cases} \qquad (11)$$

und daher

$$\left(\frac{d}{p}\right) = \begin{cases} \left(\frac{-u}{p}\right) & \text{für } b \equiv 0 \ (2) \\ 0 & \text{für } b \equiv 1 \ (2) \end{cases} \Bigg\} p > 2 \qquad (12)$$

sowie

$$\left(\frac{d}{2}\right) = \left\{\begin{array}{lll} 1 & \text{für} & \left\{\begin{array}{l} b = 0, \quad c > 0 \\ b \equiv 0 \ (2), \quad b > 0, \quad u \equiv 7 \ (8) \end{array}\right. \\ -1 & \text{für} & \left\{\begin{array}{l} b = 0, \quad c = 0 \\ b \equiv 0 \ (2), \quad b > 0, \quad u \equiv 3 \ (8) \end{array}\right. \\ 0 & \text{für} & \left\{\begin{array}{l} b \equiv 1 \ (2) \\ b \equiv 0 \ (2), \quad b > 0, \quad u \equiv 1 \ (4) \end{array}\right. \end{array}\right\} p = 2 \qquad (13)$$

In jeder Äquivalenzklasse $H \bmod q$ gibt es, wie leicht einzusehen ist, einen Repräsentanten $H = H^{(k,2)} = (h_{\alpha\beta})$ der folgenden Art:

$$\left.\begin{array}{c} h_{11} \equiv p^{\mu}, \quad h_{22} \equiv p^{\nu}, \quad h_{\alpha\beta} \equiv 0 \pmod q \\ (0 \leqq \mu,\nu \leqq a; \quad \alpha > \beta) \end{array}\right\} \qquad (14)$$

während $h = h_{12}$ aus einem festen Vertretersystem der Restklassen $\bmod p^{\nu}$ ausgewählt werden kann. Mit diesem speziellen H und $G = (g_{\alpha\beta})$ nimmt das System (9) wegen $t_0 \equiv 1 \pmod q$ die folgende Gestalt an:

$$\left.\begin{array}{c} g_{11}p^{\mu} \equiv 1, \quad g_{12}h + g_{22}p^{\nu} \equiv t_2 \\ g_{12}p^{\mu} + g_{11}h + g_{21}p^{\nu} \equiv t_1 \end{array} \pmod q \right\} \qquad (15)$$

Wir bestimmen sämtliche μ,ν,h, für welche das System (15) Lösungen $g_{\alpha\beta}$ besitzt. Offenbar ist stets $\mu = 0$ und $g_{11} \equiv 1 \pmod q$. Es verbleibt

$$g_{12}h + g_{22}p^{\nu} \equiv t_2, \quad g_{12} \equiv t_1 - h - g_{21}p^{\nu} \pmod q. \qquad (16)$$

Elimination von g_{12} ergibt

$$h(t_1 - h) + (g_{22} - hg_{21})p^{\nu} \equiv t_2 \pmod q,$$

und diese Kongruenz ist genau dann lösbar, wenn

$$h(t_1 - h) \equiv t_2 \pmod{p^{\nu}} \qquad (17)$$

ist. Eine einfache Abzählung ergibt nun für die Anzahl $A(h,p^{\nu})$ der $\bmod q$ verschiedenen ganzen Lösungen $(g_{11},g_{12},g_{21},g_{22})$ von (15) den Wert $p^{\nu}q$ oder 0, je nachdem (17) befriedigt ist oder nicht. Eine vollständige Übersicht über die Lösungen von (17) gibt das folgende Schema. Hierin bezeichnet $A(p^{\nu})$ die Anzahl der $\bmod p^{\nu}$ verschiedenen Lösungen h von (17).

Haupttypus von T:	ν:	$A(p^\nu)$:	Nr.:
$p \neq 2$ oder $b = 0$	$0 \leqq \nu \leqq b$	$p^{\nu - \left[\frac{\nu+1}{2}\right]}$	1
	$b < \nu \leqq a$	$p^{\frac{1}{2}b}\left(1+\left(\frac{d}{p}\right)\right)\left(\frac{d}{p}\right)$	2
$p = 2$ und $b \geqq 2$	$0 \leqq \nu < b-1$	$2^{\nu - \left[\frac{\nu+1}{2}\right]}$	3
	$\nu = b-1$	$2^{\frac{1}{2}b-1}\delta\left(\frac{b}{2}\right)$	4
	$\nu = b$	$2^{\frac{1}{2}b}\left(\frac{d}{2}\right)^2$	5
	$b < \nu \leqq a$	$2^{\frac{1}{2}b}\left(1+\left(\frac{d}{2}\right)\right)\left(\frac{d}{2}\right)$	6

Hierin ist $\delta(x) = 1$ oder 0, je nachdem x ganz rational ist oder nicht. Um die Vollständigkeit der Tabelle zu belegen, hat man die Kongruenz (17) für die drei Haupttypen von T zu diskutieren.

1. $p > 2$: Nach (10) hat man

$$h^2 \equiv -up^b \pmod{p^\nu}$$

zu lösen. Hier mag der Hinweis genügen, daß Lösungen für $\nu > b$ nur dann existieren, wenn $b \equiv 0 \pmod 2$ und $\left(\frac{-u}{p}\right) = 1$ ist, was so viel wie $\left(\frac{d}{p}\right) = 1$ bedeutet. Man findet nun leicht die unter Nr. 1 und 2 angegebenen Werte von $A(p^\nu)$ für $p > 2$.

2. $p = 2$, $b \geqq 2$: Nun ist

$$h^2 \equiv -u2^{b-2} \pmod{2^\nu}$$

zu lösen. Hier ist zu beachten, daß $\nu > b-2$ nur dann Lösungen gestattet, wenn $b \equiv 0 \pmod 2$ ist. $\nu = b-1$ ergibt keine weitere Bedingung. Für $\nu = b$ hat man zusätzlich $-u \equiv 1 \pmod 4$, also $\left(\frac{d}{2}\right) \neq 0$ zu fordern

und im Falle $\nu > b$ darüber hinaus $-u \equiv 1 \pmod 8$ oder $\left(\frac{d}{2}\right) = 1$. Einfache Abzählungen ergeben die unter Nr. 3 bis 6 angegebenen Werte für $A(2^\nu)$.

3. $p = 2$, $b = 0$: Wir multiplizieren (17) mit -4 und erhalten die gleichwertige Kongruenz

$$(2h - t_1)^2 \equiv t_1^2 - u2^{c+2} \pmod{2^{\nu+2}}.$$

Wir konstatieren, daß $\nu = 0$ genau eine Lösung gestattet und daß im Falle $\nu > 0$ notwendig $c > 0$, d. h. $\left(\frac{d}{2}\right) = 1$ ist. Ist diese Bedingung erfüllt, so gibt es genau zwei Lösungen, womit $A(p^\nu)$ unter Nr. 1 und 2 für $p = 2$ verifiziert ist.

Da die Elemente $g_{\alpha\beta}$ für $\alpha > 2$ willkürlich gewählt werden können, so ist die Anzahl $B(h,p^\nu)$ der $\bmod q$ verschiedenen Lösungen G von (9), sofern H den durch h und p^ν gekennzeichneten speziellen Repräsentanten in der Äquivalenzklasse $\bmod q$ von H bezeichnet und (17) erfüllt ist, gleich $q^{2(k-2)}A(h,p^\nu) = q^{2k-3}p^\nu$. Wir brauchen jetzt nur noch die Anzahl $C(h,p^\nu)$ der $\bmod q$ verschiedenen Matrizen UH in der Äquivalenzklasse $\bmod q$ von H zu bestimmen. Dabei ist U eine beliebige unimodulare Matrix $\bmod q$. Sind $\mathfrak{u}_1,\mathfrak{u}_2$ die beiden ersten Spalten von U, so ist

$$UH \equiv (\mathfrak{u}_1, \mathfrak{u}_1 h + \mathfrak{u}_2 p^\nu) \pmod q,$$

woraus hervorgeht, daß $C(h,p^\nu)$ von h unabhängig ist, so daß zur Bestimmung von $C(h,p^\nu)$ das Element h durch 0 ersetzt werden kann. Die $\bmod q$ primitiven Spalten $\mathfrak{u}_1$, die zu einer unimodularen Matrix $\bmod q$ ergänzt werden können, sind dadurch bestimmt, daß nicht alle ihre Elemente durch p teilbar sind. Für die Anzahl der $\bmod q$ verschiedenen $\mathfrak{u}_1$ findet man somit den Ausdruck

$$q^k - p^{(a-1)k} = q^k(1 - p^{-k}).$$

Gefragt wird nun nach der Anzahl der $\bmod p^{a-\nu}$ verschiedenen primitiven Spalten $\mathfrak{u}_2 \bmod q$ derart, daß $(\mathfrak{u}_1,\mathfrak{u}_2)$ zu einer primitiven Matrix $\bmod q$ ergänzbar wird. Diese Anzahl hängt offenbar von der speziellen Wahl von $\mathfrak{u}_1$ nicht ab, so daß für $\mathfrak{u}_1$ auch die erste Spalte der Einheitsmatrix gewählt werden kann. Bezüglich $\mathfrak{u}_2$ ist dann zu fordern, daß die aus den $k-1$ letzten Elementen von $\mathfrak{u}_2$ bestehende Spalte eine primitive Spalte $\bmod q$ ist,

während das erste Element von u_2 willkürlich wählbar ist. Die Anzahl der primitiven $u_2 \bmod p^{a-\nu}$ zu gegebenem u_1 ist also

$$p^{a-\nu}(p^{(k-1)(a-\nu)} - p^{(k-1)(a-\nu-1)}) = p^{(a-\nu)k}(1-p^{1-k}) \quad \text{oder } 1,$$

je nachdem $a < \nu$ oder $a = \nu$ ist. Damit ergibt sich

$$C(h,p^\nu) = \begin{cases} q^{2k}p^{-\nu k}(1-p^{-k})(1-p^{1-k}) & \text{für } \nu < a, \\ q^{2k}p^{-ak}(1-p^{-k}) & \text{für } \nu = a \end{cases}$$

und für die Anzahl $A_q(T)$ der $\bmod q$ verschiedenen Lösungen G,H von (9) schließlich

$$\begin{aligned} A_q(T) &= \sum_{\substack{0 \leqq \nu \leqq a \\ h \bmod p^\nu}} B(h,p^\nu)C(h,p^\nu) \\ &= q^{4k-3}(1-p^{-k}) \sum_{\substack{0 \leqq \nu \leqq a \\ h \bmod p^\nu}} p^{\nu(1-k)}(1-p^{1-k})^* \\ &= q^{4k-3}(1-p^{-k}) \sum_{0 \leqq \nu \leqq a} A(p^\nu)p^{\nu(1-k)}(1-p^{1-k})^*. \end{aligned}$$

Die Summation erfolgt hier über alle Lösungen $h \bmod p^\nu$ von (17). Die mit einem Stern* bezeichnete Klammer ist im Falle $\nu = a$ durch 1 zu ersetzen. Nach kurzer Rechnung erhält man mit Hilfe von

$$\sum_{\nu=0}^{b} p^{\nu-\left[\frac{\nu+1}{2}\right]}p^{\nu(1-k)} = (1+p^{1-k}) \sum_{\mu=0}^{\left[\frac{b-1}{2}\right]} p^{\mu(3-2k)} + \delta\left(\frac{b}{2}\right)p^{\frac{b}{2}(3-2k)}$$

für $a > b$ die Kongruenzlösungsanzahlen

$$\left.\begin{aligned} &A_q(T) = \\ &q^{4k-3}\frac{(1-p^{-k})(1-p^{2-2k})}{1-\left(\frac{d}{p}\right)p^{1-k}}\left\{\left(1-\left(\frac{d}{p}\right)p^{1-k}\right)\sum_{\mu=0}^{j} p^{\mu(3-2k)} + \left(\frac{d}{p}\right)^2 p^{(j+1)(3-2k)}\right\} \end{aligned}\right\} \quad (18)$$

mit

$$j = \begin{cases} \left[\frac{b-1}{2}\right] & \text{für } p > 2, \\ \left[\frac{b-2}{2}\right] & \text{für } p = 2, \end{cases}$$

folglich

$$S_p = q^{3-4k} A_q(T) \quad \text{für } a > b. \tag{19}$$

Es sei $\chi(h)$ der Charakter mod d, der für $h > 0$ mit $\left(\frac{d}{h}\right)$ übereinstimmt. Wir setzen

$$\zeta(s) = \sum_{h=1}^{\infty} h^{-s}, \quad L(s,\chi) = \sum_{h=1}^{\infty} \chi(h) h^{-s}. \tag{20}$$

Aus (4) ergibt sich dann mit Hilfe von (18) und (19) für $n = 2$ und $e(T) = 1$ die Koeffizientenformel

$$\left.\begin{aligned} a_k(T) = {} & \frac{2(2\pi)^{2k-1} L(k-1,\chi)}{(2k-2)!\,\zeta(k)\zeta(2k-2)} \cdot \\ & \cdot |2T|^{k-\frac{3}{2}} \prod_{p \nmid 2|2T|} \left\{ \left(1 - \left(\frac{d}{p}\right) p^{1-k}\right) \sum_{\mu=0}^{j} p^{\mu(3-2k)} + \left(\frac{d}{p}\right)^2 p^{(j+1)(3-2k)} \right\}. \end{aligned}\right\} \tag{21}$$

Bekanntlich ist

$$\zeta(k) = \frac{(-1)^{\frac{k}{2}-1}(2\pi)^k}{2 \cdot k!} B_k, \quad \zeta(2k-2) = \frac{(2\pi)^{2k-2}}{2 \cdot (2k-2)!} B_{2k-2} \tag{22}$$

und

$$L(k-1,\chi) = \frac{1}{\sqrt{|d|}} \sum_{q=1}^{|d|-1} \left(\frac{d}{q}\right) \sum_{m=1}^{\infty} \frac{\sin\left(2\pi \frac{d}{|q|} m\right)}{m^{k-1}} \qquad (d < 0).$$

Die unendliche Reihe über m kann, wenn man von einem elementaren Faktor absieht, als Funktionswert des Bernoullischen Polynoms $(x+B)^{k-1}$ in symbolischer Schreibweise $(B^\nu \to B_\nu)$ einfach dargestellt werden. Man erhält so

$$L(k-1,\chi) = \frac{(-1)^{\frac{k}{2}} (2\pi)^{k-1}}{2(k-1)!\sqrt{|d|}} \sum_{q=1}^{|d|-1} \left(\frac{d}{q}\right) \left(\frac{q}{|d|} + B\right)^{k-1} \tag{23}$$

und schließlich das folgende Resultat:

Satz 1: *Für $n = 2$, $k \equiv 0 \pmod 2$, $k \geq 4$ und $T > 0$, $e(T) = 1$ ist*

$$a_k(T) = -\frac{4k}{B_k B_{2k-2}} \frac{1}{|d|} \sum_{q=1}^{|d|-1} \left(\frac{d}{q}\right) (q + |d|B)^{k-1} b_k(T)$$

mit

$$b_k(T) = \left(\frac{|2T|}{|d|}\right)^{k-\frac{3}{2}} \prod_{p/2|2T|} \left\{\left(1 - \left(\frac{d}{p}\right)p^{1-k}\right)\sum_{\mu=0}^{j} p^{\mu(3-2k)} + \left(\frac{d}{p}\right)^2 p^{(j+1)(3-2k)}\right\}.$$

Hierin ist p^b die höchste Potenz von p, welche $|2T|$ teilt, und $j = \left[\frac{b-1}{2}\right]$ oder $\left[\frac{b-2}{2}\right]$, je nachdem $p > 2$ oder $p = 2$ ist. $b_k(T)$ ist stets ganz rational.

Um auch noch die Ganzzahligkeit von $b_k(T)$ zu beweisen, setzen wir $b = b_p$, $j = j_p$ sowie

$$d = -\prod_{p \geqq 2} p^{\alpha_p}.$$

Aus den Diskriminanteneigenschaften folgt

$$b_p = \alpha_p + 2(j_p + \varepsilon_p) \quad \text{mit } \varepsilon_p = \left(\frac{d}{p}\right)^2 \quad \text{für } p \geqq 2,$$

mithin

$$\left(\frac{|2T|}{|d|}\right)^{k-\frac{3}{2}} = \left(\prod_{p \geqq 2} p^{b_p - \alpha_p}\right)^{k-\frac{3}{2}} = \prod_{p \geqq 2} p^{(j_p + \varepsilon_p)(2k-3)},$$

woraus die behauptete Ganzzahligkeit von $b_k(T)$ erhellt.

§ 3. Die Reduktion auf den Fall $e(T) = 1$

Ist der Rang der halbganzen Matrix $T = T^{(n)} \geqq 0$ kleiner als zwei, so tritt $a_k(T)$ auch als Fourierkoeffizient der Eisensteinreihe ersten Grades auf. Insbesondere ist $a_k(T) = a_k(t)$, wenn alle Elemente von $T = (t_{\mu\nu})$ mit eventueller Ausnahme von $t = t_{11}$ verschwinden. p bezeichne eine beliebige Primzahl. Auf Grund von [3], S. 117 (126) kann festgestellt werden, daß die Fourierkoeffizienten $a_k(T)$ der Eisensteinreihe n-ten Grades der folgenden Beziehung genügen:

$$\left.\begin{aligned} &\prod_{\nu=2}^{n} (1 + p^{\nu-k}) a_k(p) a_k(T) = \\ &p^{k-1} a_k(1) \sum_{\nu=0}^{n} \sum_{U} a_k\left(\frac{1}{p} T[US_{p,\nu}]\right) p^{\frac{1}{2}(n-\nu)(n+1-\nu-2k)}. \end{aligned}\right\} \quad (24)$$

Hierin ist

$$S_{p,\nu} = \begin{pmatrix} E^{(\nu)} & 0 \\ 0 & pE^{(n-\nu)} \end{pmatrix} \quad (25)$$

und bei gegebenem ν durchläuft $U = (Q^{(n,\nu)}, *)$ ein volles System von unimodularen Matrizen, so daß die aus den ν ersten Spalten von U bestehenden Teilmatrizen Q mod$p$ paarweise nicht assoziiert und

$$\frac{1}{p}T[US_{p,\nu}] \quad \text{halbganze Matrizen} \tag{26}$$

sind. Zwei Matrizen Q_1, Q_2 heißen mod$p$ assoziiert, wenn $Q_2 = Q_1 V$ mit einer unimodularen Matrix mod$p$ $V = V^{(\nu)}$ gilt. Auf die Forderung (26) werden wir verzichten und statt dessen $a_k(T) = 0$ für nicht-halbganze T setzen. Da die Eisensteinreihe nicht im Sinne von [3] normiert ist, so erscheint auf der rechten Seite von (24) abweichend von der zitierten Formel der Faktor $a_k(1)$; er fällt wieder heraus, wenn man

$$a_k(t) = a_k(1) \sum_{\substack{g \mid t \\ g > 0}} g^{k-1} \tag{27}$$

berücksichtigt.

Im Falle $n = 2$ nimmt (24) mit

$$U = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} u & 1 \\ 1 & 0 \end{pmatrix} \ (u = 0,1,2,\ldots,p-1) & \text{für } \nu = 1 \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{für } \nu = 0,2 \end{cases}$$

nach einfacher Umformung folgende Gestalt an:

$$\left.\begin{aligned} a_k(pT) = (1+p^{k-1})(1+p^{k-2})a_k(T) - p^{2k-3}a_k\left(\frac{1}{p}T\right) - \\ - p^{k-2}a_k\left(\frac{1}{p}T\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\right) - \sum_{u=0}^{p-1} p^{k-2}a_k\left(\frac{1}{p}T\begin{bmatrix} u & p \\ 1 & 0 \end{bmatrix}\right). \end{aligned}\right\} \tag{28}$$

Diese Formel gestattet, wie sogleich ausgeführt wird, die Berechnung von $a_k(T)$ auf den schon behandelten Fall $e(T) = 1$ zurückzuführen.

Satz 2: *Im Falle $n = 2$ ist $a_k(T)$ für $T > 0$ durch*

$$e = e(T) \quad \textit{und} \quad D = D(T) = |2T|e^{-2} \tag{29}$$

eindeutig bestimmt, so daß

$$a_k(T) = \alpha_k(e,D) \tag{30}$$

gesetzt werden kann. Es gilt

$$\alpha_k(pe,D) = \left\{(1+p^{k-1})(1+p^{k-2}) - \left(1+\left(\frac{-D}{p}\right)\right)p^{k-2}\right\}\alpha_k(e,D) -$$
$$-\left(p-\left(\frac{-D}{p}\right)\right)p^{k-2}\alpha_k(p^{-1}e,p^2D) - p^{2k-3}\alpha_k(p^{-1}e,D)$$

für eine beliebige Primzahl $p \geqq 2$ mit der Maßgabe, daß $\alpha_k(e,D) = 0$ zu setzen ist, wenn e keine natürliche Zahl ist.

Wir rechtfertigen den Ansatz (30) auf Grund von (28) mit vollständiger Induktion nach der Anzahl $h(T)$ der Primzahlen, aus denen sich $e(T)$ zusammensetzt:

$$e(T) = \prod_{p \geqq 2} p^{\nu_p}, \quad h(T) = \sum_{p \geqq 2} \nu_p.$$

Im Falle $h(T) = 0$ ist (30) eine Folge von Satz 1. Wir nehmen an, daß (30) für alle Matrizen S an Stelle von T mit $h(S) \leqq h(T)$ schon gilt, und beweisen dann (30) für pe an Stelle von e, d. h. für $h(T)+1$ an Stelle von $h(T)$. Da $a_k(T)$ gegenüber den unimodularen Transformationen $T \to T[U]$ invariant ist, können wir uns T bezüglich p immer so normiert denken, daß t_0 durch keine höhere Potenz von p teilbar ist wie $e(T)$, so daß $t_0 e^{-1}$ eine zu p prime ganze Zahl ist. $e_p = e_p(T)$ bezeichne die größte Potenz von p, welche $e(T)$ teilt. Neben (2) verwenden wir die Bezeichnung $2S = \begin{pmatrix} 2s_0 & s_1 \\ s_1 & 2s_2 \end{pmatrix}$. Wir diskutieren die in (28) bezeichneten Fälle von S:

1. Für $S = \frac{1}{p}T$ ist ersichtlich $e(S) = p^{-1}e(T)$ und

$$D(S) = |2S|e^{-2}(S) = |2T|e^{-2}(T) = D(T),$$

also

$$a_k\left(\frac{1}{p}T\right) = \alpha_k(p^{-1}e,D).$$

2. Für $S = \frac{1}{p}T\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$ ist $s_0 = p^{-1}t_0$, $s_1 = t_1$, $s_2 = pt_2$. Gemäß unserer Normierung ist also

$$e(S) = \text{g.g.T.}(p^{-1}t_0, t_1, pt_2) = p^{-1}e(T)$$

sowie

$$D(S) = |2S|e^{-2}(S) = |2T|e^{-2}(T)p^2 = p^2D(T),$$

folglich

$$a_k\left(\frac{1}{p}T\begin{bmatrix}1 & 0\\ 0 & p\end{bmatrix}\right) = \alpha_k(p^{-1}e, p^2D).$$

3. Für $S = \frac{1}{p}T\begin{bmatrix}u & p\\ 1 & 0\end{bmatrix}$ hat man

$$s_0 = p^{-1}(t_0u^2 + t_1u + t_2), \quad s_1 = 2t_0u + t_1, \quad s_2 = pt_0,$$

so daß offenbar $|2S| = |2T|$ und

$$e(S) = e(T) \quad \text{oder} \quad p^{-1}e(T)$$

gilt. Der erste Fall ist gleichwertig mit $s_0 \equiv 0 \pmod{e_p}$. Wir haben demnach die Anzahl der mod p verschiedenen Lösungen von

$$t_0u^2 + t_1u + t_2 \equiv 0 \pmod{pe_p} \tag{31}$$

zu bestimmen. Gemäß der Bedeutung von e_p sind die durch $t_\nu = r_\nu e_p$ bestimmten Zahlen r_ν ganz; gemäß unserer Normierung ist p kein Teiler von r_0. Außerdem unterscheidet sich

$$D_p = 4r_0r_2 - r_1^2 = |2T|e_p^{-2}(T)$$

von $D = |2T|e^{-2}(T)$ nur um das Quadrat einer ganzen durch p nicht teilbaren Zahl, so daß $\left(\frac{-D_p}{p}\right) = \left(\frac{-D}{p}\right)$ ist. An Stelle von (31) erhalten wir nun

$$r_0u^2 + r_1u + r_2 \equiv 0 \pmod{p}. \tag{32}$$

Eine gleichwertige Kongruenz ergibt sich nach Multiplikation mit $4r_0$ in der Gestalt

$$(2r_0u + r_1)^2 \equiv -D_p \pmod{p^\alpha} \quad \text{mit } \alpha = \begin{cases}1 \text{ für } p > 2,\\ 3 \text{ für } p = 2,\end{cases} \tag{33}$$

woraus erhellt, daß die Anzahl der mod p verschiedenen Lösungen u in jedem Fall gleich $1 + \left(\frac{-D}{p}\right)$ ist. Es ist demnach

$$a_k\left(\frac{1}{p}T\begin{bmatrix}u & p\\ 1 & 0\end{bmatrix}\right) = \begin{cases}\alpha_k(e, D) & \text{in } 1 + \left(\frac{-D}{p}\right) \text{ Fällen,}\\ \alpha_k(p^{-1}e, p^2D) & \text{in } p - 1 - \left(\frac{-D}{p}\right) \text{ Fällen.}\end{cases}$$

Insgesamt kann (28) damit in

$$a_k(pT) = \left\{(1+p^{k-1})(1+p^{k-2}) - \left(1+\left(\frac{-D}{p}\right)\right)p^{k-2}\right\}\alpha_k(e,D) -$$

$$- p^{2k-3}\alpha_k(p^{-1}e,D) - \left(p - \left(\frac{-D}{p}\right)\right)p^{k-2}\alpha_k(p^{-1}e,p^2D)$$

übergeführt werden. $\alpha_k(pT)$ ist also auch durch

$$e(pT) = pe, \quad D(pT) = |2pT|e^{-2}(pT) = D$$

eindeutig bestimmt. Damit ist (30), zugleich auch die Rekursionsformel von Satz 2 bewiesen.

Mit vollständiger Induktion nach $h(T)$ beweist man schließlich noch die Gültigkeit einer Darstellung

$$\alpha_k(e,D) = \sum_{\substack{t^2|e \\ t>0}} c_k(e,D,t)\alpha_k(1,t^2D) \tag{34}$$

mit gewissen ganz rationalen Koeffizienten $c_k(e,D,t)$, die allerdings von recht komplizierter Struktur sind.

§ 4. Teilerprobleme

Es ist im Fall $n = 2$ leicht einzusehen, daß die Diskriminanten aller imaginär-quadratischen Körper in der Gestalt $d = -|2T|$ durch halbganze $T > 0$ mit $e(T) = 1$ realisiert werden können. Der in Satz 1 definierte ganz rationale Faktor $b_k(T)$ ist dann gleich 1. Im Hinblick auf (34) ist nun festzustellen, daß eine Bestimmung des größten gemeinsamen Teilers aller $a_k(T)$ mit $T > 0$ zu gegebenem k darauf hinausläuft, den größten gemeinsamen Teiler der Summen

$$W_{k-1}(d) = \frac{1}{|d|}\sum_{q=1}^{|d|-1}\left(\frac{d}{q}\right)(q+|d|B)^{k-1} \tag{35}$$

zu berechnen. Wir werden das Problem nicht in dieser Allgemeinheit lösen, sondern nur einen gemeinsamen, im allgemeinen gebrochenen Teiler aller $a_k(T)$ mit $T > 0$ zu gegebenem k bestimmen, der sich vom größten gemeinsamen Teiler vermutlich „nicht wesentlich" unterscheidet. Jedenfalls stimmt er mit diesem für $k = 4, 6, 8, 10, 12$ überein.

Im folgenden sei N_{2v} der gekürzte positive Nenner der Bernoullischen Zahl B_{2v}, mithin $Z_{2v} = B_{2v}N_{2v}$ ihr Zähler. N_{2v} setzt sich aus den verschiedenen Primzahlen p zusammen, für die $p-1$ ein Teiler von $2v$ ist:

$$N_{2v} = \prod_{p-1|2v} p. \tag{36}$$

Bestimmt man sämtliche Primteiler der gekürzten Zähler sämtlicher Quotienten $\frac{B_{2v}}{2v}$ ($v = 1,2,3,\ldots$), so erhält man nach einem Satz von K. L. JENSEN [2] genau alle irregulären Primzahlen, d. h. diejenigen Primzahlen p, für welche die Klassenzahl des Körpers der p-ten Einheitswurzeln durch p teilbar ist. Schließlich machen wir noch Gebrauch von der folgenden Identität (in symbolischer Schreibweise):

$$\sum_{a=1}^{m-1} a^h = \frac{1}{h+1}\{(m+B)^{h+1} - B^{h+1}\},$$

wobei h,m beliebige natürliche Zahlen sind. Speziell für $k = h+2$ folgt

$$(m+B)^{k-1} \equiv 0 \pmod{k-1}. \tag{37}$$

Mit dieser Kongruenz beweisen wir

Lemma 2: *Es sei t der größte Teiler von $k-1$, der mit der Diskriminante d keinen echten Teiler gemeinsam hat. Dann ist*

$$W_{k-1}(d) \equiv 0 \left(\mathrm{mod}\frac{t}{d}\right). \tag{38}$$

Ist w das Produkt aller Primzahlen $p < k$, die nicht in d aufgehen, so ist wd eine gemeinsamer Nenner aller Bernoullischen Zahlen auf der linken Seite der Kongruenz (37). Wir multiplizieren diese mit $|d|$ und erhalten

$$(|d|m + |d|B)^{k-1} \equiv 0 \pmod{t}.$$

Wegen $(d,wt) = 1$ kann m so bestimmt werden, daß

$$|d|m \equiv q \pmod{wt},$$

also $|d|m = q + gwt$ mit ganzem g wird. Es folgt

$$
\begin{aligned}
0 &\equiv (q + gwt + |d|B)^{k-1} \\
&\equiv (q + gwt)^{k-1} - \frac{k-1}{2}(q + gwt)^{k-2}|d| + \\
&\quad + \sum_{\nu=0}^{\frac{k}{2}-1} \binom{k-1}{2\nu} (q + gwt)^{k-1-2\nu} |d|^{2\nu} B_{2\nu} \\
&\equiv q^{k-1} - \frac{k-1}{2} q^{k-2} + \sum_{\nu=0}^{\frac{k}{2}-1} \binom{k-1}{2\nu} q^{k-1-2\nu} |d|^{2\nu} B_{2\nu} \\
&\equiv (q + |d|B)^{k-1} \pmod{t},
\end{aligned}
$$

damit auch die Behauptung von Lemma 2.

Wir bestimmen analoge Teilbarkeitseigenschaften von $W_{k-1}(d)$ bezüglich der Primteiler von d. Die folgenden Aussagen über die Summen

$$S_h(d) = \sum_{q=1}^{|d|-1} \left(\frac{d}{q}\right) q^h \tag{39}$$

dienen zur Vorbereitung.

Lemma 3: *Es sei s der größte Teiler von $k-1$, der sich nur aus Primteilern der Diskriminante d zusammensetzt. Dann ist*

$$S_{k-1}(d) \equiv 0 \pmod{sd} \tag{40}$$

mit Ausnahme der folgenden Fälle:

1. $d = -4$:

$$S_{k-1}(d) \equiv 2 \pmod 4. \tag{41}$$

2. $d = -p$ (*Primzahl*), p/N_{2k-2}:

$$S_{k-1}(d) \equiv p - 1 \pmod p. \tag{42}$$

Zum Beweis führen wir den Charakter $\chi(h) \bmod d$ ein, der für $h > 0$ mit $\left(\frac{d}{h}\right)$ übereinstimmt. Es sei p^ϱ bzw. p^α die höchste Potenz eines gegebenen Primteilers p von d, welche $k-1$ bzw. d teilt, insbesondere also $\alpha = 2$ oder 3 für $p = 2$ und $\alpha = 1$ für $p > 2$. Es ist dann

$$S_{k-1}(d) \equiv \sum_{q \bmod d} \chi(q) q^{k-1} \pmod{p^{\varrho+\alpha}}; \tag{43}$$

denn $q^{k-1} \bmod p^{\varrho+\alpha}$ hängt nur von $q \bmod d$ ab, wie aus

$$(q+gd)^{k-1} = \sum_{\nu=0}^{k-1} \binom{k-1}{\nu} q^{k-1-\nu}(gd)^{\nu} \quad (g \text{ ganz})$$

unmittelbar hervorgeht, da $\binom{k-1}{\nu} d^{\nu}$ für $\nu > 0$ durch $p^{\varrho+\alpha}$ teilbar ist. Die Fälle $p > 2$ und $p = 2$ werden nun getrennt behandelt.

1. $p > 2$: Sind a und d teilerfremd, so durchläuft aq mit q auch alle Restklassen $\bmod d$. Aus (43) folgt dann

$$S_{k-1}(d) \equiv \chi(a) a^{k-1} S_{k-1}(d) \pmod{p^{\varrho+\alpha}}. \tag{44}$$

Gibt es ein a mit

$$\chi(a) a^{k-1} \not\equiv 1 \pmod{p},$$

so folgt aus (44) sofort $S_{k-1}(d) \equiv 0 \pmod{p^{\varrho+\alpha}}$. Diese Teilbarkeit wird in (40) bezüglich p behauptet. Wir brauchen also nur noch den Fall zu diskutieren, daß $\chi(a) \equiv a^{k-1} \pmod{p}$ für alle zu d primen a gilt. Hieraus folgt $d = -p$; denn wenn p ein echter Teiler von d ist, dann läßt sich, weil χ ein eigentlicher Charakter $\bmod d$ ist, ein zu d primes $a \equiv 1 \pmod{p}$ mit $\chi(a) = -1$ bestimmen. Das würde einen Widerspruch ergeben. Da χ die Ordnung zwei hat, so folgt $p-1 \mid 2k-2$, was so viel wie $p \mid N_{2k-2}$ bedeutet, wegen $\alpha = 1$ schließlich auch $S_{k-1}(-p) \equiv p-1 \pmod{p}$. Es liegt also der zweite Ausnahmefall vor.

2. $p = 2$: Wegen $\varrho = 0$, $\alpha \leqq 3$, $k \equiv 0 \pmod 2$ ist nach (43)

$$S_{k-1}(d) \equiv \sum_{q=1}^{|d|-1} \chi(q) q \pmod{2^{\varrho+\alpha}}.$$

Bekanntlich ist diese Summe durch d teilbar, wenn wir den Fall $d = -4$ ausnehmen. Unter dieser Voraussetzung folgt dann wieder $S_{k-1}(d) \equiv 0 \pmod{2^{\varrho+\alpha}}$, d. h. die Teilbarkeitsaussage (40) bezüglich $p = 2$. Der Fall $d = -4$ ist der erste Ausnahmefall. Hier ist $S_{k-1}(-4) \equiv 2 \pmod 4$ evident. Die Kongruenz (40) ist also immer gültig, wenn für d nicht die Ausnahmefälle gelten. Lemma 3 ist damit bewiesen.

Wir merken noch an

$$S_{2k}(d) \equiv 0 \pmod 8 \quad \text{für } d \equiv 0 \pmod 2, \tag{45}$$

was evident ist, da $q^2 \equiv 1 \pmod 8$ für ungerade q gilt.

Mit dem oben eingeführten w erhalten wir ausführlich

$$\left.\begin{aligned} wW_{k-1}(d) &= \frac{w}{|d|}S_{k-1}(d) - \frac{k-1}{2}wS_{k-2}(d) + \\ &+ \frac{w|d|}{2\cdot 3}(k-1)\left(\frac{k}{2}-1\right)S_{k-3}(d) + \sum_{\nu=0}^{\frac{k}{2}-1}\binom{k-1}{2\nu}|d|^{2\nu-2}S_{k-1-2\nu}(d)(w|d|B_{\nu 2}). \end{aligned}\right\} \quad (46)$$

Für einen Primteiler p von d sei

$$k-1 = p^{\varrho}u, \quad 2\nu = p^{\beta}v, \quad uv \not\equiv 0 \pmod{p}.$$

In geläufiger Weise zeigt man, daß $\binom{k-1}{2\nu}|d|^{2\nu-2}$ für $\nu \geqq 2$ durch p^{σ} teilbar ist, wenn $\sigma = \varrho - \beta + 2\nu - 2$ gesetzt wird. Aus der Abschätzung $2\nu \geqq 2^{\beta}$ und $\nu \geqq 2$ folgt $2\nu \geqq \beta + 2$, also $\sigma \geqq \varrho$. Beachtet man ferner, daß $wS_{k-2}(d)$ nach (45) gerade und $w|d|$ durch 6 teilbar ist, so ergibt sich schließlich

$$W_{k-1}(d) \equiv \frac{1}{|d|}S_{k-1}(d) \left(\mathrm{mod}\frac{s}{w}\right); \quad (47)$$

denn jeder Term auf der rechten Seite von (46) mit Ausnahme des ersten ist durch $s = \prod_{p|d} p^{\varrho}$ teilbar.

Aus Lemma 3 folgt in Verbindung mit (47) sofort

Lemma 4: *Es sei w das Produkt aller Primzahlen $p < k$, welche die Diskriminante d nicht teilen, und s der größte Teiler von $k-1$, der sich nur aus Primteilern von d zusammensetzt. Dann ist*

$$W_{k-1}(d) \equiv 0 \left(\mathrm{mod}\frac{s}{w}\right)$$

mit Ausnahme der folgenden Fälle:

1. $d = -4$:

$$W_{k-1}(d) \equiv -\frac{1}{2}\left(\mathrm{mod}\frac{1}{w}\right) \quad \textit{mit } s = 1.$$

2. $d = -p$ *(Primzahl)*, p/N_{2k-2}:

$$W_{k-1}(d) \equiv -\frac{1}{p}\left(\mathrm{mod}\frac{1}{w}\right) \quad \textit{mit } s = p^{\varrho}.$$

Dieses Ergebnis liefert mit Lemma 2 das folgende Resultat

Lemma 5: *Es ist*

$$W_{k-1}(d) \equiv 0 \pmod{k-1}$$

mit Ausnahme der folgenden Fälle:

1. $d = -4$:

$$2W_{k-1}(d) \equiv 0 \pmod{k-1}, \quad 2W_{k-1}(d) \equiv -1 \pmod{2}$$

2. $d = -p$ *(Primzahl)*, p/N_{2k-2}:

$$pW_{k-1}(d) \equiv 0 \left(\mathrm{mod}\frac{k-1}{p^{\varrho}}\right), \quad pW_{k-1}(d) \equiv -1 \pmod{p}$$

Dabei ist p^{ϱ} die größte Potenz von p, welche $k-1$ teilt.

Da die Fourierkoeffizienten $\alpha_k(1,t^2D)$ in (34) bei gegebenem D alle zur selben Diskriminante d gehören, so können wir auf Grund von Satz 1

$$a_k(T) \equiv 0 \left(\mathrm{mod}\frac{4k}{B_kB_{2k-2}}W_{k-1}(d)\right) \quad \text{für } T > 0$$

schließen. Unter Berücksichtigung von Lemma 5 folgt hieraus

Satz 3: *Für $n = 2$, $k \equiv 0 \pmod 2$, $k > 3$ und $T > 0$ ist*

$$a_k(T) \equiv 0 \left(\mathrm{mod}\frac{4k(k-1)}{B_kB_{2k-2}}\right)$$

mit Ausnahme der Fälle:

1. $d = -4$:

$$a_k(T) \equiv 0 \left(\mathrm{mod}\frac{2k(k-1)}{B_kB_{2k-2}}\right)$$

2. $d = -p$ *(Primzahl)*, p/N_{2k-2}:

$$a_k(T) \equiv 0 \left(\mathrm{mod}\frac{4k(k-1)}{B_kB_{2k-2}p^{\varrho+1}}\right)$$

Dabei ist p^{ϱ} die höchste Potenz von p, welche $k-1$ teilt. In den Ausnahmefällen ist der Primteiler p von d in optimaler Potenz in dem jeweiligen Modul enthalten, sofern $d = -|2T|$ ist.

Da jeder Primteiler $p \equiv -1 \pmod 4$ von N_{2k-2} eine Ausnahmediskriminante $d = -p$ ergibt, so gelangen wir zu einem von T unabhängigen Modul, indem wir gewisse Kürzungen gemäß den Angaben von Satz 3 vornehmen. Wir erreichen damit das Ziel unserer Betrachtungen:

Satz 4: *Es sei $n = 2$, $k \equiv 0 \pmod 2$, $k > 3$, $T > 0$ und q der größte Teiler von $(k-1)N_{2k-2}$, der sich nur aus Primteilern $p \equiv -1 \pmod 4$ von N_{2k-2} zusammensetzt. Dann ist*

$$a_k(T) \equiv 0 \left(\mathrm{mod}\frac{k(2k-2)}{qB_kB_{2k-2}}\right).$$

Der gekürzte Nenner des Moduls setzt sich nur aus irregulären Primteilern der Zähler von B_k und B_{2k-2} zusammen.

Die letzte Aussage bezüglich des Modulnenners folgt aus dem zitierten Satz von K. L. JENSEN, wenn man beachtet, daß q mit dem Zähler Z_{2k-2} von B_{2k-2} keinen echten Teiler gemeinsam hat.

Wir teilen noch einige schon von IGUSA [1] berechnete Koeffizienten mit. Auf Grund dieser Zahlenangaben sowie der Feststellungen in Satz 3 ist der größte gemeinsame Teiler t_k aller $a_k(T)$ mit $T > 0$ für die fünf ersten Werte von k zu berechnen. Man entnimmt die Werte der folgenden Aufstellung.

k	$a_k\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$
4	$2^5 3^3 5 \cdot 7$
6	$2^4 3^3 5 \cdot 7 \cdot 11$
8	$2^6 3^2 5 \cdot 61$
10	$2^4 3^4 5 \cdot 7 \cdot 11 \cdot 19 \cdot 277 \cdot 43867^{-1}$
12	$2^5 3^3 5 \cdot 7 \cdot 13 \cdot 19 \cdot 23 \cdot 2659 \cdot 131^{-1} \cdot 593^{-1} \cdot 691^{-1}$

k	$a_k\begin{pmatrix}1 & \frac{1}{2}\\ \frac{1}{2} & 1\end{pmatrix}$
4	$2^7 3 \cdot 5 \cdot 7$
6	$2^6 3^2 7 \cdot 11$
8	$2^8 3 \cdot 5 \cdot 7$
10	$2^6 3 \cdot 7 \cdot 11 \cdot 19 \cdot 809 \cdot 43867^{-1}$
12	$2^7 3^2 5 \cdot 7 \cdot 13 \cdot 23 \cdot 1847 \cdot 131^{-1} \cdot 593^{-1} \cdot 691^{-1}$

k	t_k
4	$2^5 3 \cdot 5$
6	$2^4 3^2 7$
8	$2^6 3 \cdot 5$
10	$2^4 3 \cdot 11 \cdot 43867^{-1}$
12	$2^5 3^2 5 \cdot 7 \cdot 13 \cdot 131^{-1} \cdot 593^{-1} \cdot 691^{-1}$

Weitere Fourierkoeffizienten können mit den von H. ZASSENHAUS [8] angegebenen L-Reihenwerten berechnet werden.

Literatur

[1] J.-I. IGUSA: On Siegel modular forms of genus two. Amer. J. Math. **84** (1962), 175–200.

[2] K. L. JENSEN: Om talteoretiske Egenskaber ved de Bernoulliske Tal. Nyt Tidsskr. for Mat. B **26** (1915), 73–83.

[3] H. MAASS: Die Primzahlen in der Theorie der Siegelschen Modulfunktionen. Math. Ann. **124** (1951), 87–122.

[4] C. L. SIEGEL: Einführung in die Theorie der Modulfunktionen n-ten Grades. Math. Ann. **116** (1939), 617–657.

[5] C. L. SIEGEL: Über die analytische Theorie der quadratischen Formen. Ann. of Math. **36** (1935), 527–606.

[6] C. L. SIEGEL: Über die Fourierschen Koeffizienten der Eisensteinschen Reihen. Mat. Fys. Medd. Dan. Vid. Selsk. **34**, Nr. 6, (1964).

[7] E. WITT: Eine Identität zwischen Modulformen zweiten Grades. Abh. Math. Sem. Hansische Univ. **14** (1941), 323–337.

[8] H. ZASSENHAUS: Tabelle der Absolutglieder der Eisensteinreihen $E_2(\tau)$ für die ersten Primzahlen und Dimensionen. Abh. Math. Sem. Hansische Univ. 14 (1941), 285–288.

Indleveret til Selskabet den 15. april 1964.
Færdig fra trykkeriet den 24. november 1964.