Weil, A.
Math. Annalen 168, 149—156 (1967)

Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen

Carl Ludwig Siegel zu seinem 70. Geburtstag freundlichst zugeeignet

André Weil

Angesichts der Gelegenheit, für welche die vorliegende Note bestimmt ist, ist der Versuch gewiß nicht unangebracht, einen berühmten Heckeschen Ansatz weiterzuführen; daran soll auch der obige Titel erinnern. Grundlegend bei diesem Ansatz ist das folgende Lemma:

Lemma 1. *Es seien* $(a_1, a_2, \ldots)$ *und* $(b_1, b_2, \ldots)$ *zwei Folgen komplexer Zahlen; für irgendein* $\sigma > 0$ *sei* $a_n = O(n^\sigma)$ *und* $b_n = O(n^\sigma)$. *Die Funktionen* φ, ψ, Φ, Ψ, F, G *seien durch*

$$\varphi(s) = \sum_1^\infty a_n n^{-s}, \qquad \psi(s) = \sum_1^\infty b_n n^{-s},$$

$$\Phi(s) = (2\pi)^{-s}\,\Gamma(s)\,\varphi(s), \quad \Psi(s) = (2\pi)^{-s}\,\Gamma(s)\,\psi(s),$$

$$F(\tau) = \sum_1^\infty a_n e^{2\pi i n\tau}, \qquad G(\tau) = \sum_1^\infty b_n e^{2\pi i n\tau}$$

in der Halbebene $\mathrm{Re}(s) > \sigma$ *bzw. in der oberen Halbebene* $\mathrm{Im}(\tau) > 0$ *definiert. Es sei* $C \neq 0$, $A > 0$, $k > 0$. *Dann sind die folgenden Aussagen* (A) *und* (B) *gleichwertig:*

(A) Φ *und* Ψ *lassen sich in der ganzen s-Ebene holomorph fortsetzen und bleiben dabei in jedem Vertikalstreifen* $\sigma' \leqq \mathrm{Re}(s) \leqq \sigma''$ *beschränkt, und es ist*

$$\Phi(s) = C A^{\frac{k}{2}-s}\,\Psi(k-s).$$

(B) *In der oberen Halbebene ist*

$$F(\tau) = C A^{\frac{k}{2}} \left(\frac{A\tau}{i}\right)^{-k} G\left(\frac{-1}{A\tau}\right).$$

Zwar behandelt Hecke ([1]) nur den Fall $(a_n) = (b_n)$, allerdings unter Zulassung einfacher Pole bei $s = 0$, $s = k$ für $\Phi = \Psi$; der Beweis bleibt aber für den Fall zweier Folgen (a_n), (b_n) Wort für Wort derselbe.

Weiterhin sei k eine positive *ganze* Zahl; $GL_+(2, \mathbf{R})$ sei die Gruppe der reellen Matrizen $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit positiver Determinante. Es sei $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ein Element dieser Gruppe, und F sei irgendeine holomorphe Funktion in der oberen Halbebene $\mathrm{Im}(\tau)>0$. In Anlehnung an HECKE definieren wir

$$(F|\alpha)(\tau)=F\left(\frac{a\tau+b}{c\tau+d}\right)(c\tau+d)^{-k}(ad-bc)^{\frac{k}{2}};$$

dann ist ebenfalls $F|\alpha$ eine in der oberen Halbebene holomorphe Funktion. Für $\alpha=\begin{pmatrix}a&0\\0&a\end{pmatrix}$ ist $F|\alpha=(\operatorname{sgn}a)^k F$.

Für $b\in\mathbf{R}$ bzw. $B>0$ definieren wir

$$\alpha(b)=\begin{pmatrix}1&b\\0&1\end{pmatrix},\quad \omega(B)=\begin{pmatrix}0&-1\\B&0\end{pmatrix}.$$

Die rechte Seite der letzten Formel in Lemma 1 läßt sich dann in der Form $Ci^k(G|\omega(A))$ schreiben. Ferner sei ω ein Element des Gruppenringes der Gruppe $GL_+(2,\mathbf{R})$, also eine lineare Kombination $\omega=\sum u_i\alpha_i$ von Elementen α_i dieser Gruppe mit komplexen Koeffizienten u_i; wir definieren dann

$$F|\omega=\sum u_i(F|\alpha_i).$$

Für ein gegebenes F bezeichnen wir durch Ω_F die Gesamtheit der Elemente ω des Gruppenringes von $GL_+(2,\mathbf{R})$ mit der Eigenschaft $F|\omega=0$; das ist offensichtlich ein Rechtsideal im Gruppenring.

Nun sei $(c_1,c_2,\ldots)$ eine Folge komplexer Zahlen, nicht alle 0; es sei $c_n=O(n^\sigma)$ mit irgendeinem $\sigma>0$. Für jeden Modul m und jeden *primitiven* Charakter χ der ganzen Zahlen modulo m setzen wir

$$L_\chi(s)=\sum_1^\infty c_n\chi(n)n^{-s},$$

$$\Lambda_\chi(s)=\left(\frac{m}{2\pi}\right)^s\Gamma(s)L_\chi(s),$$

$$F_\chi(\tau)=\sum_1^\infty c_n\chi(n)e^{2\pi in\tau};$$

für $m=1$, also für den Hauptcharakter $\chi=1$, schreiben wir einfach L, Λ, F statt L_1, Λ_1, F_1. Für $m>1$ sei $g(\chi)$ die Gaußsche Summe

$$g(\chi)=\sum_{x\bmod m}\chi(x)e^{2\pi i\frac{x}{m}}.$$

Dann ist bekanntlich für alle n:

$$\chi(n)=\frac{g(\chi)}{m}\sum_{a\bmod m}\bar\chi(a)e^{2\pi i\frac{na}{m}},$$

und daher mit den oben erklärten Bezeichnungen

$$F_\chi=F\left|\frac{g(\chi)}{m}\sum_{a\bmod m}\bar\chi(a)\,\alpha\left(\frac{a}{m}\right).\right.$$

Fortan sei A eine positive *ganze* Zahl; $C=C_1$, C_χ seien komplexe Konstanten. Als unmittelbare Folge des Heckeschen Lemmas haben wir:

Lemma 2. *Folgende Aussagen sind gleichwertig:* (A2) *Λ ist eine ganze Funktion, beschränkt in jedem Vertikalstreifen, und genügt der Funktionalgleichung*

$$\Lambda(s)=C A^{\frac{k}{2}-s}\Lambda(k-s)\,;$$

(B2) *es ist*

$$1\equiv C i^k\omega(A)\quad(\operatorname{mod}\Omega_F)\,.$$

(B2) ist nämlich nur eine Umschreibung für (B) in Lemma 1, falls Λ statt Φ und Ψ gesetzt ist. Selbstverständlich muß hierbei $C=\pm 1$ sein, was wir auch weiterhin benutzen werden.

Lemma 3. *Für $m>1$ sind folgende Aussagen gleichwertig:* (A3) *Λ_χ, $\Lambda_{\bar\chi}$ sind ganze Funktionen, beschränkt in jedem Vertikalstreifen, und genügen der Gleichung*

$$\Lambda_\chi(s)=C_\chi A^{\frac{k}{2}-s}\Lambda_{\bar\chi}(k-s)\,;$$

(B3) *es ist*

$$g(\chi)\sum_{a \bmod m}\bar\chi(a)\,\alpha\left(\frac{a}{m}\right)\equiv C_\chi i^k g(\bar\chi)\sum_{a \bmod m}\chi(a)\,\alpha\left(\frac{a}{m}\right)\omega(Am^2)\quad(\operatorname{mod}\Omega_F)\,.$$

Falls die c_n reell sind, sieht man sofort, durch Übergang zum komplexkonjugierten, daß $|C_\chi|=1$ sein muß.

Für $(a,m)\neq 1$ ist $\chi(a)=0$; in der Summation auf beiden Seiten von (B3) kommen also nur solche a in Betracht, die zu m teilerfremd sind. Es werde nun angenommen, daß $(A,m)=1$, also daß *m zu A teilerfremd sei.* Dann gibt es zu jedem a mit $(a,m)=1$ eine ganze Zahl b derart, daß $Aab\equiv -1\ (\operatorname{mod} m)$, also $1=mn-Aab$ mit ganzzahligem n. Die Matrix

$$\gamma(a,b)=\begin{pmatrix} m & -b\\ -Aa & n\end{pmatrix}$$

gehört alsdann zur Modulgruppe; genauer gesagt gehört sie zur Untergruppe $\Gamma_0(A)$ der Modulgruppe, die aus allen ganzzahligen Matrizen $\begin{pmatrix} r & s\\ t & u\end{pmatrix}$ mit $1=ru-st$, $t\equiv 0(\operatorname{mod} A)$ besteht. Eine leichte Rechnung ergibt nun

$$\alpha\left(\frac{a}{m}\right)\omega(Am^2)=\omega(A)\,\gamma(a,b)\,\alpha\left(\frac{b}{m}\right)\begin{pmatrix} m & 0\\ 0 & m\end{pmatrix}.$$

Jedem b mit $(b,m)=1$ werde ein a so zugeordnet, daß $Aab\equiv -1(\operatorname{mod} m)$; dann sei $1=mn-Aab$, und es werde $\gamma(b)$ statt $\gamma(a,b)$ geschrieben. Wenn b ein volles System von zu m teilerfremden und modulo m inkongruenten Zahlen durchläuft, so tut a dasselbe. Da aus $Aab\equiv -1(\operatorname{mod} m)$ folgt, daß $\chi(a)=\bar\chi(-Ab)$, so läßt sich nun (B3) durch folgende äquivalente Formel ersetzen:

$$\text{(B3')}\qquad \sum_{b \bmod m}\bar\chi(b)\left[1-\frac{C_\chi i^k g(\bar\chi)\bar\chi(-A)}{g(\chi)}\,\omega(A)\,\gamma(b)\right]\alpha\left(\frac{b}{m}\right)\equiv 0\quad(\operatorname{mod}\Omega_F)\,.$$

Es sei nun ε ein (nicht notwendig primitiver) Charakter modulo A. Wir erinnern daran, daß F eine Modulform vom Heckeschen Typus $(-k, A, \varepsilon)$ heißt, falls für jede Matrix $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ aus $\Gamma_0(A)$ die Gleichung $F|\gamma = \varepsilon(r)^{-1} F$ besteht und außerdem F gewissen Regularitätsbedingungen an den Spitzen von $\Gamma_0(A)$ genügt. Für $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ folgt daraus, daß $\varepsilon(-1) = (-1)^k$. Wenn noch angenommen wird, daß F die Eigenschaft (B2) hat, also der Bedingung $F|\omega(A) = C^{-1} i^{-k} F$ genügt, so ergibt sich aus der Gleichung

$$\omega(A) \begin{pmatrix} r & s \\ At & u \end{pmatrix} \omega(A)^{-1} = \begin{pmatrix} u & -t \\ -As & r \end{pmatrix},$$

daß $\varepsilon(r) = \varepsilon(u)$ für $ru \equiv 1 \pmod{A}$, also $\varepsilon(r)^2 = 1$, $\varepsilon(r) = \pm 1$. Unter diesen Umständen muß also der Charakter ε reell sein.

Satz 1. *Es sei ε ein Charakter modulo A. Die Bezeichnungen und Voraussetzungen seien wie oben, also insbesondere $F(\tau) = \sum_1^\infty c_n e^{2\pi i n \tau}$ und $c_n = O(n^\sigma)$ mit einem $\sigma > 0$; F sei eine Modulform vom Heckeschen Typus $(-k, A, \varepsilon)$, und es sei $F|\omega(A) = C^{-1} i^{-k} F$. Dann genügt Λ der Bedingung* (A2) *in Lemma 2, und für jeden primitiven Charakter χ mit einem zu A teilerfremden Führer $m = f_\chi$ genügen Λ_χ, $\Lambda_{\bar\chi}$ der Bedingung* (A3) *von Lemma 3, mit der Konstanten*

$$C_\chi = C\varepsilon(f_\chi) \frac{g(\chi)}{g(\bar\chi)} \chi(-A).$$

Die erste Behauptung ist nämlich in Lemma 2 enthalten; die zweite folgt unmittelbar aus Lemma 3, wenn man darin (B3) durch (B3′) ersetzt, was wegen $(A, m) = 1$ erlaubt ist.

Jetzt handelt es sich um die Umkehrung von Satz 1. Es sei $\mathfrak{M}$ die Menge, die aus der Zahl 4 und allen ungeraden Primzahlen besteht. Für $m \in \mathfrak{M}$ sind sämtliche Charaktere modulo m primitiv, mit der einzigen Ausnahme des Hauptcharakters $\chi = 1$.

Lemma 4. *Es sei $m \in \mathfrak{M}$, $(A, m) = 1$; C'_m sei eine komplexe Zahl $\neq 0$. Folgende Aussagen sind gleichwertig:* (A4) *die Bedingung* (A3) *in Lemma 3 ist für jeden primitiven Charakter χ modulo m erfüllt, mit*

$$C_\chi = C'_m i^{-k} \frac{g(\chi)}{g(\bar\chi)} \chi(-A);$$

(B4) *es ist, für alle b, b' mit $(b, m) = (b', m) = 1$:*

$$[1 - C'_m\, \omega(A)\, \gamma(b)]\, \alpha\left(\frac{b}{m}\right) \equiv [1 - C'_m\, \omega(A)\, \gamma(b')]\, \alpha\left(\frac{b'}{m}\right) \quad (\operatorname{mod} \Omega_F).$$

Bezeichnen wir nämlich mit $\lambda(b)$ die linke Seite der Gleichung in (B4). Wenn man in Lemma 3 (B3) durch (B3′) ersetzt, so sieht man, daß (A4) mit der folgenden Bedingung gleichwertig ist:

(B4′) $$\sum_{b \bmod m} \bar\chi(b)\, \lambda(b) \equiv 0 \quad (\operatorname{mod} \Omega_F),$$

wenn man darin für χ alle primitiven Charaktere modulo m, d. h. alle Charaktere modulo m mit Ausnahme von $\chi = 1$, einsetzt. Falls (B 4) erfüllt ist, ist offensichtlich auch (B 4') erfüllt. Umgekehrt bekommt man (B 4), indem man (B 4') mit $\chi(b') - \chi(b'')$ multipliziert und über alle primitiven Charaktere χ summiert.

Lemma 5. *Es sei* $\gamma = \begin{pmatrix} m & -b \\ -Aa & n \end{pmatrix}$ *ein Element von* $\Gamma_0(A)$ *mit* $m \in \mathfrak{M}$, $n \in \mathfrak{M}$. *Die Bedingung* (A 4) *von Lemma 4 sei sowohl für den Führer m wie für den Führer n erfüllt, und es sei* $C'_m C'_n = (-1)^k$. *Außerdem genüge F der Bedingung* (A 2) *von Lemma 2. Dann ist* $F|\gamma = C'^{-1}_m C i^k F$.

Wir setzen noch $\gamma' = \begin{pmatrix} m & b \\ Aa & n \end{pmatrix}$. In (B 4) ersetzen wir b, b' durch b, $-b$; da $b \not\equiv -b (\operatorname{mod} m)$, können wir dabei annehmen, daß $\gamma(b) = \gamma$, $\gamma(-b) = \gamma'$. Wegen Lemma 2 ergibt sich dann aus Lemma 4:

$$(1 - \xi\gamma)\,\alpha\left(\frac{b}{m}\right) \equiv (1 - \xi\gamma')\,\alpha\left(\frac{-b}{m}\right) \quad (\operatorname{mod} \Omega_F)$$

mit $\xi = C'_m C^{-1} i^{-k}$, oder auch, da Ω_F Rechtsideal ist:

$$1 - \xi\gamma' \equiv (1 - \xi\gamma)\,\alpha\left(\frac{2b}{m}\right) \quad (\operatorname{mod} \Omega_F).$$

Andererseits hat man

$$\gamma^{-1} = \begin{pmatrix} n & b \\ Aa & m \end{pmatrix}, \quad \gamma'^{-1} = \begin{pmatrix} n & -b \\ -Aa & m \end{pmatrix}.$$

Da (B 4) auch für den Führer n gilt, ergibt sich genau wie oben

$$(1 - \xi'\gamma^{-1})\,\alpha\left(\frac{-b}{n}\right) \equiv (1 - \xi'\gamma'^{-1})\,\alpha\left(\frac{b}{n}\right) \quad (\operatorname{mod} \Omega_F)$$

mit $\xi' = C'_n C^{-1} i^{-k}$. Wegen $C'_m C'_n = (-1)^k$, $C = \pm 1$ ist $\xi' = \xi^{-1}$, also

$$1 - \xi'\gamma'^{-1} = -(1 - \xi\gamma')\xi^{-1}\gamma'^{-1}.$$

Da Ω_F Rechtsideal ist, hat man also

$$\begin{aligned} 1 - \xi\gamma' &\equiv -\xi(1 - \xi^{-1}\gamma^{-1})\,\alpha\left(\frac{-2b}{n}\right)\gamma' \\ &\equiv (1 - \xi\gamma)\gamma^{-1}\alpha\left(\frac{-2b}{n}\right)\gamma' \quad (\operatorname{mod} \Omega_F). \end{aligned}$$

Durch Vergleich mit der oben erhaltenen Kongruenz für $1 - \xi\gamma'$ ergibt sich

$$(1 - \xi\gamma)(1 - \mu)\,\alpha\left(\frac{2b}{m}\right) \equiv 0 \quad (\operatorname{mod} \Omega_F),$$

wo man gesetzt hat

$$\mu = \gamma^{-1}\alpha\left(\frac{-2b}{n}\right)\gamma'\alpha\left(\frac{-2b}{m}\right) = \begin{pmatrix} 1 & -\dfrac{2b}{m} \\ \dfrac{2Aa}{n} & \dfrac{4}{mn} - 3 \end{pmatrix}.$$

Es sei nun $G=F|(1-\xi\gamma)=F-\xi(F|\gamma)$. Dann ist die zuletzt erhaltene Gleichung gleichbedeutend mit $G|(1-\mu)=0$, d. h. $G=G|\mu$. Die Eigenwerte der Matrix μ sind aber die Wurzeln der Gleichung

$$T^2+2\left(1-\frac{2}{mn}\right)T+1=0;$$

sie sind imaginär und sind keine Einheitswurzeln; also ist μ elliptisch von unendlicher Ordnung. Dann ist aber bekanntlich $G=0$ die einzige in der oberen Halbebene holomorphe Lösung der Gleichung $G=G|\mu$. Aus $G=0$ folgt nun $F=\xi(F|\gamma)$, w. z. b. w.

Satz 2. *Es sei $\mathfrak{M}'$ eine Untermenge von $\mathfrak{M}$ mit nicht-leerem Durchschnitt mit jeder arithmetischen Progression vom Teiler* 1 (d. h. mit jeder Folge ganzer Zahlen a, $a+b$, $a+2b, \ldots$ für welche $(a,b)=1$, $b>0$); *außerdem sei* $(A,m)=1$ *für alle $m\in\mathfrak{M}'$. Es sei ε ein Charakter modulo A. Mit denselben Bezeichnungen wie oben erfülle F die Bedingung* (A 2) *von Lemma 2; weiter sei die Bedingung* (A 3) *von Lemma 3 für jeden primitiven Charakter χ mit einem Führer $f_\chi\in\mathfrak{M}'$ erfüllt, und es sei*

$$C_\chi=C\varepsilon(f_\chi)\frac{g(\chi)}{g(\overline{\chi})}\chi(-A).$$

Dann ist F eine ganze Modulform vom Typus $(-k,A,\varepsilon)$, und es ist $F|\omega(A)=Ci^{-k}F$. Ist die Dirichletsche Reihe $L(s)$ für $s=k-\delta$ mit irgendeinem $\delta>0$ absolut konvergent, so ist F sogar eine Spitzenform.

Es sei $\gamma=\begin{pmatrix}a & b\\ Ac & d\end{pmatrix}$ ein Element von $\Gamma_0(A)$; wir müssen zuerst beweisen, daß $F|\gamma=\varepsilon(a)^{-1}F$. Für $b=0$, $a=d=1$ ist das klar wegen Lemma 2 und der Gleichung

$$\begin{pmatrix}1 & 0\\ Ac & 1\end{pmatrix}=\omega(A)\cdot\begin{pmatrix}1 & -c\\ 0 & 1\end{pmatrix}\cdot\omega(A)^{-1}.$$

Es sei $b\neq 0$. Da $1=ad-Abc$, ist $(a,Ab)=1$, $(d,Ab)=1$; wegen der Annahme über $\mathfrak{M}'$ gibt es also Zahlen

$$m=a+Abs\in\mathfrak{M}',\quad n=d+Abt\in\mathfrak{M}'$$

mit ganzzahligen s, t. Schreiben wir

$$b'=c+mt+ns-bst,\quad \gamma'=\begin{pmatrix}m & b\\ Ab' & n\end{pmatrix}.$$

Die Voraussetzungen von Lemma 5 sind für m und n erfüllt mit $C'_m=Ci^k\varepsilon(m)$, $C'_n=Ci^k\varepsilon(n)$; da $mn\equiv ad\equiv 1 \pmod A$, ist $\varepsilon(m)\,\varepsilon(n)=1$, also $C'_m\,C'_n=1$ wegen $C=\pm 1$. Lemma 5 zeigt, daß $F|\gamma'=\varepsilon(m)^{-1}F$; nun ist aber

$$\gamma=\begin{pmatrix}1 & 0\\ -At & 1\end{pmatrix}\gamma'\begin{pmatrix}1 & 0\\ -As & 1\end{pmatrix},$$

woraus die Behauptung für γ folgt, weil sie für alle drei Matrizen auf der rechten Seite zutrifft. Schließlich, falls $b=0$, $a=d=-1$, kann man das eben Bewiesene auf $\gamma\alpha(u)$ anwenden, mit u ganz und $\neq 0$.

Um den Beweis zu Ende zu führen, muß noch das Verhalten von F bei Annäherung an die reelle Achse untersucht werden. Anfangs wurde angenommen, daß $c_n = O(n^\sigma)$ mit einem gewissen $\sigma > 0$. Wegen der Stirlingschen Formel gibt es also ein $C > 0$, so daß

$$|c_n| \leqq C \frac{\Gamma(\sigma+n+1)}{\Gamma(\sigma)\,\Gamma(n+1)}.$$

Daraus ergibt sich, für $y > 0$:

$$|F(x+iy)| \leqq C(1-e^{-2\pi y})^{-1-\sigma},$$

also $F(x+iy) = O(y^{-1-\sigma})$ für $y \to 0$. Daraus folgt bekanntlich, daß F eine ganze Modulform ist. Nun sei $L(s)$ für $s = k - \delta$ mit $0 < \delta < k$ absolut konvergent. Dann ist

$$s_n = \sum_{\nu=1}^{n} |c_\nu| \leqq n^{k-\delta} \sum_{\nu=1}^{\infty} |c_\nu|\, \nu^{-k+\delta},$$

also $s_n = O(n^{k-\delta})$. Andererseits bekommt man, durch „partielle Summation“[1]

$$|F(x+iy)| \leqq (1-e^{-2\pi y}) \sum_{1}^{\infty} s_n e^{-2\pi n y},$$

also, genau wie oben, $F(x+iy) = O(y^{-k+\delta})$ für $y \to 0$. Daher ist F eine Spitzenform.

An die obigen Resultate lassen sich noch Überlegungen über Zetafunktionen elliptischer Kurven anknüpfen, die vielleicht auch einige Aufmerksamkeit verdienen.

Es sei C eine elliptische Kurve, definiert über dem rationalen Zahlkörper $\mathbf{Q}$, etwa durch eine Weierstraßsche Gleichung $y^2 = x^3 - ax - b$ mit rationalen Koeffizienten. Bekanntlich (vgl. NÉRON [2]) läßt sich für jede Primzahl p ein (im wesentlichen eindeutig bestimmtes) „Néronsches Modell“ C_p für C angeben, welches mit C über dem p-adischen Körper $\mathbf{Q}_p$ birational äquivalent ist; C_p ist durch eine Gleichung

$$Y^2 + \lambda XY + \mu Y = X^3 + \alpha X^2 + \beta X + \gamma$$

mit ganzen p-adischen Koeffizienten gegeben; wenn man diese Gleichung modulo p reduziert, bekommt man die Gleichung einer *irreduziblen* Kurve $\bar{C}_p$ über dem Primkörper $\mathbf{F}_p$. Wir unterscheiden nun drei Fälle:

(I) $\bar{C}_p$ ist vom Geschlecht 1 und hat also eine Zetafunktion mit einem Zähler von der Form $1 - c_p T + pT^2$; dabei ist $1 - c_p + p$ die Anzahl der über $\mathbf{F}_p$ rationalen Punkte auf der Kurve $\bar{C}_p$, und es ist $|c_p| \leqq 2\sqrt{p}$. Wir setzen dann

$$L_p(s) = (1 - c_p p^{-s} + p^{1-2s})^{-1}.$$

(II) $\bar{C}_p$ hat einen gewöhnlichen Doppelpunkt. Wir setzen $\varepsilon_p = +1$ oder -1, je nachdem die Tangenten am Doppelpunkt rational über $\mathbf{F}_p$ sind oder nicht, und schreiben

$$L_p(s) = (1 - \varepsilon_p p^{-s})^{-1}.$$

---

[1] Diesen Schluß verdanke ich einem freundlichen Hinweis von A. SELBERG.

Dieser Fall kann übrigens nur dann eintreten, wenn entweder $p=2$ oder 3 oder die absolute Invariante j von C nicht p-ganz ist.

(III) $\bar{C}_p$ hat eine Spitze. Dann setzen wir $L_p(s)=1$.

Ferner sei Δ_p die Diskriminante der Gleichung der Kurve C_p; setzen wir $\delta_p=\mathrm{ord}(\Delta_p)$; dann ist $\delta_p=0$ im Fall (I); sonst ist $\delta_p>0$. Die auf p bezügliche Faser des Néronschen singularitätenfreien Minimalmodells für C_p ist im Fall (I) nichts anderes als $\bar{C}_p$; sonst ist sie ein Zyklus; in allen Fällen sei μ_p die Anzahl ihrer Komponenten. Nach einer Angabe von OGG (vgl. [3]) setzen wir $A_p=p^a$ mit $a=\delta_p-\mu_p+1$. Nach NÉRON [2] ist $a=0$ im Fall (I), $a\geqq 1$ im Fall (II), $a\geqq 2$ im Fall (III); es ist immer $a=1$ im Fall (II) und $a=2$ im Fall (III), falls $p\neq 2, 3$.

Wir schreiben nun

$$A=\prod_p A_p, \quad L(s)=\prod_p L_p(s)=\sum_1^\infty c_n n^{-s}$$

und nennen A den *Führer* und L die *Zetafunktion* der Kurve C. Mit den Koeffizienten c_n von L bilden wir dann die Funktionen Λ, F, L_χ, Λ_χ, genau wie oben.

Aus gewissen theoretischen Gründen darf man mit ziemlicher Sicherheit vermuten, daß Λ eine Funktionalgleichung besitzt, oder, genauer gesagt, daß sie die Bedingung (A 2) von Lemma 2 mit $k=2$ erfüllt. Weiter läßt sich vermuten, daß für jeden primitiven Charakter χ mit einem zu A teilerfremden Führer die Bedingung (A 3) von Lemma 3 ebenfalls erfüllt ist, wieder mit $k=2$. In allen mir zugänglichen Sonderfällen habe ich nun gefunden, daß C_χ dabei die in den Sätzen 1 und 2 vorgesehene Form hat, sogar mit $\varepsilon=1$. Nach Satz 2 ist dann F eine Spitzenform vom Heckeschen Haupttypus $(-2, A)$, und $F(\tau)\,d\tau$ ist ein Differential 1. Gattung auf der durch $\Gamma_0(A)$ bestimmten Riemannschen Fläche R; nach einer Mitteilung von G. SHIMURA muß sogar dieses Differential zu einer über $\mathbf{Q}$ definierten elliptischen Kurve C' gehören, die in der Jacobischen Mannigfaltigkeit von R enthalten ist; der Periodenmodul von $F(\tau)\,d\tau$ ist also mit demjenigen von C' kommensurabel. Es ist natürlich naheliegend zu erwarten, daß unter diesen Umständen C' mit C isogen ist; das bestätigt sich tatsächlich in einigen Fällen. Ob die Dinge immer, d. h. für jede über $\mathbf{Q}$ definierte Kurve C, sich so verhalten, scheint im Moment noch problematisch zu sein und mag dem interessierten Leser als Übungsaufgabe empfohlen werden.

Literatur

[1] HECKE, E.: Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung. Math. Ann. **112**, 664—699 (1936); Mathematische Werke, Göttingen 1959 (Nr. 33, S. 591—626).

[2] NÉRON, A.: Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. Publ. Math. I.H.E.S. **21**, 1—128 (1964).

[3] OGG, A. P.: Elliptic curves and wild ramification. Erscheint im Am. J. Math.

Professor ANDRÉ WEIL
Institute for Advanced Study
Princeton, N.J.

(Eingegangen am 10. Januar 1966)