Reduktion modulo ℓ von Thetareihen zu positiven quadratischen Formen der Stufe ℓ^n für Primzahlen $\ell \geqq 5$. (N.-P. Skoruppa)

1. Zusammenfassung

Sei $Q = Q(x_1, \ldots, x_r)$ eine positive quadratische Form mit ganz rationalen Koeffizienten in r Variablen, sei F die (symetrische) Matrix zu Q, also

$$Q(x) = \frac{1}{2}\, x^t F x \quad \text{für } x \in \mathbb{Z}^r$$

($\mathbb{Z}^r$ ist die Menge der r-zeiligen Spaltenvektoren mit Komponenten in $\mathbb{Z}$, x^t bezeichnet den zu x transponierten Zeilenvektor).

Der Form Q ordnen wir folgende Größen zu:

$r(Q)$ = Anzahl der Variablen von Q,

$d(Q)$ = Determinante von F,

$s(Q)$ = Stufe von Q, d.h. die kleinste positive ganze Zahl s, sodaß sF^{-1} ganzzahlige Komponenten und gerade Diagonalelemente hat,

$e(Q) = \frac{1}{2}\,\{$Summe der positiv zu nehmenden Elementarteiler von $F\}$,

$$\Theta_Q = \Theta_F = \sum_{x \in \mathbb{Z}^r} q^{Q(x)} \in \mathbb{Z}[\![q]\!].$$

Sei nun ℓ eine Primzahl, $\ell \geqq 5$, und sei Q eine Form mit $s(Q) = \ell^n$ für ein $n \geqq 0$. Es ist dann auch $d(Q)$ eine Potenz von ℓ und nach dem Elementarteilersatz erhalten wir mit $r = r(Q)$:

$$SFT = \begin{bmatrix} \ell^{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & \ell^{\alpha_r} \end{bmatrix}$$

für geeignete $S, T \in GL_r(\mathbb{Z})$ und $\alpha_1, \ldots, \alpha_r \geqq 0$, insbesondere

$$e(Q) = \frac{1}{2}\left\{ \ell^{d_1} + \dots + \ell^{d_r} \right\}.$$

Man rechnet leicht nach, daß $r(Q)$ eine gerade Zahl ist (denn die Determinante einer symetrischen Matrix mit ganzzahligen Komponenten, geraden Diagonalelementen und einer ungeraden Anzahl von Zeilen und Spalten ist stets eine gerade Zahl), und daß

$$e(Q) \equiv \begin{cases} \dfrac{r(Q)}{2} \mod \ell-1 & \text{— falls } d(Q) \text{ eine Quadratzahl ist} \\[2ex] \dfrac{r(Q)+\ell-1}{2} \mod \ell-1 & \text{— falls } d(Q) \text{ keine Quadratzahl ist} \end{cases}.$$

Es ist bekannt, daß $(-1)^{r/2} d(Q) \equiv 1 \mod 4$ ist, also $r \equiv 0 \mod 4$, falls $d(Q)$ eine Quadratzahl ist, und $r \equiv 2 \mod 4$, $\ell \equiv 3 \mod 4$ bzw. $r \equiv 0 \mod 4$, $\ell \equiv 1 \mod 4$ anderenfalls, sodaß in jedem Fall $e(Q)$ eine gerade Zahl ist.

Ist $f(z)$ eine Modulform der Stufe 1, so fassen wir $f(z)$ wahlweise als formale Potenzreihe in $q = e^{2\pi i z}$ auf, sodaß Aussagen wie „$\Theta_Q \equiv f \mod \ell^n$" einen Sinn erhalten (in diesem Fall also: $\Theta_Q - f \in \ell R[[q]]$, wenn R den von den Fourierkoeffizienten von f über $\mathbb{Z}$ erzeugten Ring bezeichnet).

Es gilt nun

Satz

Es gilt eine Modulform f der Stufe 1, vom Gewicht $e(Q)$ und mit ganzen rationalen Fourierkoeffizienten, sodaß

$$\Theta_Q \equiv f \mod \ell$$

gilt.

Vor dem Beweis dieses Satzes geben wir einige Folgerungen und Beispiele.

Sei $\mathbb{Z}_\ell$ der Ring der ℓ-ganzen Zahlen in $\mathbb{Q}$, $F_\ell = \mathbb{Z}_\ell / \ell\mathbb{Z}_\ell$; wir können jeder Teilmenge $A \subseteq \mathbb{Z}_\ell[[q]]$ eine Teilmenge $\tilde{A} \subseteq F_\ell[[q]]$ zuordnen, indem wir $f = \sum a_n q^n \in A$ das Element $\tilde{f} = \sum (a_n \bmod \ell)\, q^n$ zuordnen.

Es bezeichne M_k den $\mathbb{Z}_\ell$-Modul der Modulformen der Stufe 1 vom Gewicht k mit Fourierkoeffizienten in $\mathbb{Z}_\ell$.

Nach dem Satz erhalten wir in Übereinstimmung mit einem früheren Ergebnis

$$\tilde{\Theta}_Q \in \tilde{M}_{\frac{\ell+1}{2}}$$

für jede binäre Form Q der Diskriminante $-\ell$.

Für jede quaternäre Form Q der Stufe ℓ mit $d(Q) = \ell^2$ erhalten wir mit dem Satz:

$$\tilde{\Theta}_Q \in \tilde{M}_{\ell+1},$$

in Übereinstimmung mit einem Ergebnis von Serre wonach

$$\tilde{M}_{\ell+1} = \left(\widetilde{\mathbb{Z}_\ell\text{-Modul der Modulformen für } \Gamma_0(\ell) \text{ vom Gewicht 2 mit Fourierkoeffizienten in } \mathbb{Z}_\ell} \right).$$

(Nach Serre ist überhaupt jede Modulform für $\Gamma_0(\ell)$ mit rationalen Koeffizienten eine "ℓ-adische Modulform", insbesondere ist jede Form für $\Gamma_0(\ell)$ mit Fourierkoeffizienten in $\mathbb{Z}_\ell$ kongruent modulo ℓ zu einer Modulform der Stufe 1 mit Koeffizienten in $\mathbb{Z}_\ell$.)

Sei nun $M \subseteq \mathbb{Z}_\ell[[q]]$ die von allen Modulformen der Stufe 1 mit Fourierkoeffizienten in $\mathbb{Z}_\ell$ erzeugte $\mathbb{Z}_\ell$-Algebra, und sei $\Theta(\ell^n)$ die von allen Θ_Q mit $s(Q) \mid \ell^n$ und von 1 erzeugte Teilalgebra von $\mathbb{Z}_\ell[[q]]$, schließlich $\Theta(\ell^\infty) = \bigcup_{n \geq 0} \Theta(\ell^n)$.

Mit diesen Bezeichnungen gilt

Korollar 1

Es gilt

$$\widetilde{\Theta(1)} = \widetilde{\Theta(\ell)} = \widetilde{\Theta(\ell^2)} = \dots = \widetilde{\Theta(\ell^\infty)} = \widetilde{\mathcal{M}} \quad - \text{ für } \ell \equiv 3\,(4),$$

und

$$\widetilde{\Theta(1)} \subsetneqq \widetilde{\Theta(\ell)} \subseteq \widetilde{\Theta(\ell^2)} = \dots = \widetilde{\Theta(\ell^\infty)} = \widetilde{\mathcal{M}} \quad - \text{ für } \ell \equiv 1\,(4).$$

Insbesondere ist $\widetilde{\Theta(\ell^\infty)}$ *eine endlich erzeugte* F_ℓ*-Algebra.*

Beweis:

Es ist bekannt, daß $\mathcal{M} = \mathbb{Z}_\ell[E_4, E_6]$, wo $E_k = 1 - \frac{2k}{B_k}\sum_{n>0}\sigma_{k-1}(n)q^n$ für gerades k und wo B_k die k-te Bernoullische Zahl ist $\left(\frac{q}{e^q-1} = \sum \frac{B_k}{k!} q^k\right)$, und daß $E_4 = \Theta_{\Gamma_8}$, wo Γ_8 die bis auf Äquivalenz über $\mathbb{Z}$ eindeutig bestimmte positive Form in 8 Variablen mit Determinante 1 ist.

Nach dem Satz genügt es daher zum Nachweis von $\widetilde{\Theta(1)} = \widetilde{\mathcal{M}}$ bzw. $\widetilde{\Theta(\ell^2)} = \widetilde{\mathcal{M}}$ zu zeigen, daß $\widetilde{E}_6 \in \widetilde{\Theta(1)}$ für $\ell \equiv 3\,(4)$ bzw. $\widetilde{E}_6 \in \widetilde{\Theta(\ell^2)}$ für $\ell \equiv 1\,(4)$.

Sei zunächst $\ell \equiv 3\,(4)$:

Nach der Staudt-Kongruenz ist $E_{\ell-1} \equiv 1 \bmod \ell$, daher $E_6 \equiv E_6 E_{\ell-1} \bmod \ell$; insbesondere ist also $\widetilde{E}_6 \in \widetilde{\mathcal{M}}_{\ell+5}$, und $\ell+5 \equiv 0 \bmod 4$. Es ist aber für $k \equiv 0 \bmod 4$ jede Form aus $\mathcal{M}_k$ eine $\mathbb{Z}_\ell$-Linearkombination von Reihen Θ_Q mit $r(Q) = 2k$, $d(Q) = +1$. (Ein Beweis hierfür ergibt sich etwa durch Induktion über k unter Beachtung von $\Delta = q\prod_{n>0}(1-q^n)^{24} = \frac{\Theta_{\Gamma_8}^3 - \Theta_{Leech}}{2^4 \times 3^2 \times 5}$), wo Θ_{Leech} die zum Leech-Gitter gehörige Thetareihe bezeichnet (d.h. $\Theta_{Leech} = \Theta_Q$, wo Q für die bis auf Äquivalenz über $\mathbb{Z}$ eindeutig bestimmte positive Form in 24 Variablen mit $d(Q) = +1$ und $Q(x) \neq 1$ für alle $x \in \mathbb{Z}^{24}$ steht)

Sei nun allgemein $\ell \equiv 1, 3 \bmod 4$:

Ist Q eine positive Form in 12 Variablen der Stufe ℓ, sodaß $d(Q)$ eine Quadratzahl ist, so ist Θ_Q – vermöge $q = e^{2\pi i z}$ aufgefasst als Funktion von z mit $\operatorname{Im} z > 0$ – bekanntlich eine Modulform vom Gewicht 6 für $\Gamma_0(\ell)$; bilden wir bzgl. Θ_Q die Spur von $\Gamma_0(\ell)$ nach $SL_2(\mathbb{Z})$, so erhalten wir eine Modulform der Stufe 1, d.h.

$$\Theta_Q + \sum_{t=1}^{\ell} \frac{\Theta_Q\left(\frac{-1}{z+t}\right)}{(z+t)^6} = \Theta_Q - \frac{\ell}{\sqrt{d(Q)}} \sum_{\substack{x \in \mathbb{Z}^{12} \\ Q^*(x) \equiv 0 \bmod \ell}} q^{\frac{Q^*(x)}{\ell}}$$

$$= \left(1 - \frac{\ell}{\sqrt{d(Q)}}\right) E_6 ,$$

wo $Q^*(x) = \frac{1}{2} x^t \ell F^{-1} x$ ist, wenn F die zu Q gehörige Matrix bezeichnet; wählen wir etwa $\Theta_Q = \Theta_{Q_1}^3$ für eine quaternäre Form Q_1 der Stufe ℓ und Determinante ℓ^2 (solch ein Q_1 existiert bekanntlich), so erhalten wir

$$E_6 \equiv \sum_{\substack{x \in \mathbb{Z}^{12} \\ Q^*(x) \equiv 0 \bmod \ell}} q^{\frac{Q^*(x)}{\ell}} \bmod \ell .$$

Ist $P_{11}(F_\ell) = {}^{\textstyle\{(\mathbb{Z}/\ell\mathbb{Z})^{12} - \{0\}\}} \big/ {}_{\textstyle(\mathbb{Z}/\ell\mathbb{Z})^*}$, $u \mapsto [u]$ die kanonische Abbildung von $(\mathbb{Z}/\ell\mathbb{Z})^{12} - \{0\} \to P_{11}(F_\ell)$, so können wir schreiben:

$$\sum_{\substack{x \in \mathbb{Z}^{12} \\ Q^*(x) \equiv 0 \bmod \ell}} q^{\frac{Q^*(x)}{\ell}} = \sum_{\substack{[u] \in P_{11}(F_\ell) \\ Q^*(u) = 0}} \; \sum_{\substack{x \in \mathbb{Z}^{12} \\ x \bmod \ell = \lambda u \\ \text{für ein} \\ \lambda \in \mathbb{Z}/\ell\mathbb{Z}}} q^{\frac{Q^*(x)}{\ell}}$$

$$- \left(\# \{ [u] \in P_{11}(F_\ell) \mid Q^*(u) = 0 \} - 1 \right) \sum_{\substack{x \in \mathbb{Z}^{12} \\ x \equiv 0 \bmod \ell}} q^{\frac{Q^*(x)}{\ell}} .$$

Setzen wir für $[u] \in P_{11}(F_\ell)$

$$L_{[u]} = \{ x \in \mathbb{Z}^{12} \mid x \bmod \ell = \lambda u \text{ für ein } \lambda \in \mathbb{Z}/\ell\mathbb{Z} \},$$

so ist $L_{[u]}$ ein Teilmodul von $\mathbb{Z}^{12}$ mit $\ell\mathbb{Z}^{12} \subseteq L_{[u]}$; ist daher $y_1, \dots, y_{12}$ eine $\mathbb{Z}$-Basis von $L_{[u]}$, $T = (y_1, \dots, y_{12})$ die aus den Spaltenvektoren $y_1, \dots, y_{12}$ gebildete Matrix, so ist für $Q^*(u) = 0$ die Form $Q_{[u]}(x) = \frac{1}{\ell} Q^*(Tx)$ eine positive Form mit ganzzahligen Koeffizienten der Stufe ℓ oder ℓ^2 (man kann leicht einsehen, daß die Stufe ℓ^2 ist), und es gilt

$$\sum_{\substack{x \in \mathbb{Z}^{12} \\ x \bmod \ell = \lambda u \\ \text{für ein } \lambda \in \mathbb{Z}/\ell\mathbb{Z}}} q^{Q^*(x)/\ell} = \Theta_{Q_{[u]}}$$

Ähnlich sieht man, daß $\sum\limits_{\substack{x \in \mathbb{Z}^{12} \\ x \equiv 0 \bmod \ell}} q^{Q^*(x)/\ell} \in \Theta(\ell^2)$

(oder man benützt, daß $\#\{[u] \in P_{11}(F_\ell) \mid Q^*(u) = 0\} \equiv 1 \bmod \ell$ gilt), sodaß jedenfalls $\widetilde{E}_6 \in \widetilde{\Theta(\ell^2)}$.

Zum Nachweis von $\widetilde{\Theta(1)} \subsetneqq \widetilde{\Theta(\ell)}$ für $\ell \equiv 1 \bmod 4$, beachten wir, daß nach einem Ergebnis von Swinnerton-Dyer $\widetilde{M} = \bigoplus\limits_{t \bmod \ell-1} \widetilde{M}^t$, wo $\widetilde{M}^t = \bigcup\limits_{k \equiv t \bmod \ell-1} \widetilde{M}_k$, daß ferner die Anzahl der Variablen einer positiven Form mit ganzzahligen Koeffizienten der Determinante 1 durch 8 teilbar ist; damit ~~so~~ erhalten wir für $\ell \equiv 1 \bmod 4$, daß $\widetilde{\Theta(1)} \cap \widetilde{M}_{\ell+1} = \{0\}$; dagegen ist aber $\widetilde{\Theta}_Q \in \widetilde{M}_{\ell+1} \cap \widetilde{\Theta(\ell)}$, wenn Q eine quaternäre Form mit $s(Q) = \ell$, $d(Q) = \ell^2$ bezeichnet. $\square$

Anmerkung

Korollar 1 gilt sinngemäß, wenn statt $\mathbb{Z}_\ell$ der Ring der ℓ-ganzen Zahlen in einem beliebigen algebraischen Zahlkörper betrachtet wird.

Für die ersten in Frage kommenden Primzahlen $\ell = 5, 7, 11$ erhält man z. B.:

– für $\ell = 5$

Es ist $E_4 \equiv 1 \bmod 5$; ist Q eine quaternäre Form der Stufe 5, Determinante 25, so ist $e(Q) = 6$, also $\Theta_Q \equiv E_6 \bmod 5$;

Also:

$$\tilde{M} = \widetilde{\Theta(5^\infty)} = F_5 [\tilde{\Theta}_Q].$$

– für $\ell = 7$

$E_6 \equiv 1 \bmod 7$, $E_4 \equiv \Theta_{\left[\begin{smallmatrix} 2 & 1 \\ 1 & 4 \end{smallmatrix}\right]} \bmod 7$,

also

$$\tilde{M} = \widetilde{\Theta(7^\infty)} = F_7 [\widetilde{\Theta_{\left[\begin{smallmatrix} 2 & 1 \\ 1 & 4 \end{smallmatrix}\right]}}].$$

– für $\ell = 11$

$E_6 \equiv \Theta_{\left[\begin{smallmatrix} 2 & 1 \\ 1 & 6 \end{smallmatrix}\right]} \bmod 11$; $E_4 E_6 = E_{10} \equiv 1 \bmod 11$,

daher $E_4 \equiv E_6^{-1} \equiv \Theta^{-1}_{\left[\begin{smallmatrix} 2 & 1 \\ 1 & 6 \end{smallmatrix}\right]} \bmod 11$,

also

$$\tilde{M} = \widetilde{\Theta(11^\infty)} = F_7 \left[\widetilde{\Theta_{\left[\begin{smallmatrix} 2 & 1 \\ 1 & 6 \end{smallmatrix}\right]}}, \frac{1}{\widetilde{\Theta_{\left[\begin{smallmatrix} 2 & 1 \\ 1 & 6 \end{smallmatrix}\right]}}} \right].$$

Unmittelbar mit dem oben schon erwähnten Ergebnis von Swinnerton-Dyer:

$$\tilde{M} = \bigoplus_{t \bmod \ell-1} \tilde{M}^t, \quad \tilde{M}^t = \bigcup_{k \equiv t \bmod \ell-1} \widetilde{M_k}.$$

erhalten wir noch das

<u>Korollar 2</u>

<u>$\widetilde{\Theta(\ell^\infty)}$ ist eine $\mathbb{Z}/(\ell-1)\mathbb{Z}$ – graduierte Algebra:</u>

$$\widetilde{\Theta(\ell^\infty)} = \bigoplus_{e \bmod \ell-1} \widetilde{\Theta(\ell^\infty)}^e,$$

<u>wo</u> $\widetilde{\Theta(\ell^\infty)}^e$ <u>den von allen</u> $\tilde{\Theta}_Q$ <u>mit</u> $e(Q) \equiv e \bmod \ell-1$ <u>erzeugten F_ℓ-Modul bezeichnet.</u>

Zum Beweis des Satzes werden wir Q über $\mathbb{Z}_\ell$ diagonalisieren:

$$Q(x) = x^t T^t \begin{bmatrix} a_1 \ell^{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & a_r \ell^{\alpha_r} \end{bmatrix} Tx \quad, T \in GL_r(\mathbb{Z}_\ell),\ a_1,\dots,a_r \in \mathbb{Z}_\ell^*;$$

wir können dabei annehmen, daß T ganzzahlige Komponenten hat.

Mit $d = \det(T) \times \{\text{Hauptnenner der } a_1,\dots,a_r\}$, $y = \begin{bmatrix} y_1 \\ \vdots \\ y_r \end{bmatrix}$ haben wir dann:

$$\Theta_Q = \sum_{y \in T\mathbb{Z}^r} q^{\sum a_i \ell^{\alpha_i} y_i^2} = \sum_{\substack{y \in \mathbb{Z}^r \\ dT^{-1}y \equiv 0 \bmod d}} q^{\sum a_i \ell^{\alpha_i} y_i^2}$$

$$= \sum_{\substack{y \in \mathbb{Z}^r \\ y \bmod d \\ dT^{-1}y \equiv 0 \bmod d}} \prod_{i=1}^{r} \sum_{n \equiv y_i \bmod d} q^{a_i \ell^{\alpha_i} n^2}$$

$$\equiv \sum_{\substack{y \in \mathbb{Z}^r \\ y \bmod d \\ dT^{-1}y \equiv 0 \bmod d}} \prod_{i=1}^{r} \Big(\sum_{n \equiv y_i \bmod d} q^{a_i n^2} \Big)^{\ell^{\alpha_i}} \bmod \ell \ .$$

Die zuletzt auftrende Reihe ist nun ein $\Theta_{\hat{Q}}$ für eine Form $\hat{Q}$ in $2e(Q) = \{\ell^{\alpha_1} + \dots + \ell^{\alpha_r}\}$ Variablen, mit ganzzahligen Koeffizienten und mit $d(\hat{Q}) \big| 2^{2e(Q)} d^{2e(Q)} \times a_1^{\ell^{\alpha_1}} \times \dots \times a_r^{\ell^{\alpha_r}}$, also $s(\hat{Q}) \not\equiv 0 \bmod \ell$.

Wegen $s(\hat{Q}) \not\equiv 0 \bmod \ell$ hat nach bekannten Sätzen über das Transformationsverhalten von Thetareihen

$$\Theta_{\hat{Q}}|_A = \Theta_{\hat{Q}}\left(\frac{az+b}{cz+d}\right) \Big/ (cz+d)^{e(Q)} \qquad (q = e^{2\pi i z})$$

für jedes $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ ℓ-ganze Fourierkoeffizienten, und wir werden zeigen, daß stets

$$\Theta_{\hat{Q}}|_A \equiv \Theta_{\hat{Q}} \bmod \ell,$$

$\Theta_{\hat{Q}}$ ist nun bekanntlich eine Modulform für $\Gamma_0(s(\hat{Q}))$; aus der letzten Gleichung ergibt sich, daß $\Theta_{\hat{Q}}$ vom Haupttyp ist; hieraus und nochmals mit der letzten Gleichung erhält man sofort vermöge einer Spurbildung, daß

$$\widetilde{\Theta_{\hat{Q}}} \in [Sl_2(\mathbb{Z}) : \Gamma_0(s(\hat{Q}))] \cdot \widetilde{\mathcal{M}_{e(Q)}} .$$

Der angekündigte Satz wäre bewiesen, wenn nur

$$[Sl_2(\mathbb{Z}) : \Gamma_0(s(\hat{Q}))] \not\equiv 0 \bmod \ell ,$$

d.h. – wegen $[Sl_2(\mathbb{Z}) : \Gamma_0(s(\hat{Q}))] = s(\hat{Q}) \prod_{p \mid s(\hat{Q})} (1 + \frac{1}{p})$ – wenn nur

$$s(\hat{Q}) \in \bigcap_{p \equiv 0, -1 \bmod \ell} \mathbb{Z}_p^*$$

wäre.

Diese letzte Bedingung wäre nun sicherlich erfüllt, falls wir Q über $\bigcap_{p \equiv 0,-1 \bmod \ell} \mathbb{Z}_p$ statt nur über $\mathbb{Z}_\ell$ diagonalisiert hätten.

In 2.) werden wir zeigen, daß wir jede Form über $\bigcap_{p \equiv 0,-1(\ell)} \mathbb{Z}_p$ diagonalisieren können, in 3.), 4.) wird im Wesentlichen die Kongruenz $\Theta_{\hat{Q}}|_A \equiv \Theta_{\hat{Q}} \bmod \ell$ bewiesen.

2. In diesem Abschnitt sei

$$Q(x) = \sum_{1 \leq i \leq j \leq r} a_{ij} x_i x_j \qquad \left(x = \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \right)$$

eine quadratische Form mit ganzzahligen Koeffizienten a_{ij}; Q sei positiv, d.h. $Q(x) > 0$ für alle $x \in \mathbb{Z}^r$. Q heißt primitiv, falls der größte gemeinsame Teiler der a_{ij} $(1 \leq i \leq j \leq n)$ die Zahl 1 ist.

Mit ℓ bezeichnen wir weiterhin eine Primzahl mit $\ell \geq 5$; es sei

$$R = \bigcap_{p \equiv 0,-1 \bmod \ell} \mathbb{Z}_p \quad ,$$

d.h. R ist der Durchschnitt der bei p lokalisierten rationalen Zahlen $\mathbb{Z}_p$, wo p sämtliche Primzahlen mit der Eigenschaft $p = \ell$ oder $p \equiv -1 \bmod \ell$ durchläuft.
R ist ein Hauptidealring; mit R^* sei wie üblich die Gruppe der Einheiten von R bezeichnet.

<u>Lemma 1</u>

<u>Ist</u> Q <u>primitiv</u>, <u>so gibt es ein</u> $y \in \mathbb{Z}^r$, <u>so daß</u> $Q(y) \in R^*$.

(Das Lemma 1 ist für $\ell = 3$ i.A. falsch; ein Gegenbeispiel ist $Q = 2x_1^2 + 3x_2^2$) -

<u>Beweis</u>

Ist $Q(x)$ Form in einer Variablen, so folgt der Satz aus der Existenz von Primzahlen p mit $p \not\equiv 0,-1 \bmod \ell$.
Wir nehmen daher an, daß $Q(x)$ von mehr als einer

Variablen abhängt.

Zunächst zeigen wir, daß man sich auf den Fall einer binären Form beschränken kann:

Sei $y \in \mathbb{Z}^r$ mit $Q(y) \neq 0$. Da Q primitiv ist, gibt es keine Primzahl p, sodaß $p \mid Q(x)$ für alle $x \in \mathbb{Z}^r$; insbesondere gibt es also zu jedem $p \mid Q(y)$ ein $y_p \in \mathbb{Z}^r$ mit $Q(y_p) \not\equiv 0 \bmod p$. Mit dem chinesischen Restsatz konstruiert man aus den y_p leicht ein $z \in \mathbb{Z}^r$, sodaß $Q(z) \equiv Q(y_p) \bmod p$, d.h. $Q(z) \not\equiv 0 \bmod p$ für alle $p \mid Q(y)$. Dann ist aber $Q(my + nz)$ eine primitive binäre Form in m und n, und das Lemma würde folgen, falls es für binäre Formen bewiesen wäre.

Sei also

$$Q = a x_1^2 + b x_1 x_2 + c x_2^2$$

eine (positive) primitive Form.

Wir haben dann

$$b^2 - 4ac = f^2 d$$

für die Diskriminante d des (imaginär) quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{b^2-4ac})$ und eine geeignete ganze Zahl $f > 0$.

Sei $\mathcal{O}_f$ die Ordnung von $\mathbb{Q}(\sqrt{d})$ mit Führer f; sei I_f die Halbgruppe der in $\mathcal{O}_f$ gelegenen vollständigen Moduln von $\mathbb{Q}(\sqrt{d})$ mit Multiplikatorenring $\mathcal{O}_f$, P_f die Halbgruppe der von 0 verschiedenen Hauptideale von $\mathcal{O}_f$. Es gibt dann bekanntlich ein $A \in I_f / P_f$, sodaß für jedes $m > 0$ die Gleichung $m = Q(x)$ in $x \in \mathbb{Z}^2$ genau dann lösbar ist, wenn ein $\mathfrak{a} \in A$ mit $N(\mathfrak{a}) = m$ existiert (wobei $N(\mathfrak{a}) = [\mathcal{O}_f : \mathfrak{a}]$ gilt).

Sei I die Halbgruppe der ganzen Ideale $\mathfrak{a}$ der Hauptordnung $\mathcal{O}$ von $\mathbb{Q}(\sqrt{d})$, die zu $b \cdot f$ teilerfremd sind, sei $\mathfrak{P}$ die Halbgruppe der (ganzen) Hauptideale $\alpha\mathcal{O}$, wo $\alpha \equiv 1 \bmod \ell f$ gilt.

Wir haben dann einen surjektiven Homomorphismus

$$\Phi := I/_{\mathfrak{P}} \longrightarrow I_f/_{\mathfrak{P}_f},$$

der durch $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}_f$ induziert wird.

Da $N(\mathfrak{a}) = N(\mathfrak{a} \cap \mathcal{O}_f)$ (und $N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$) gilt, genügt es somit, die folgende Aussage zu beweisen:

Zu jedem $A \in \Phi$ gibt es ein $\mathfrak{a} \in A$ mit $N(\mathfrak{a}) \in R^{\times}$.

Wir unterscheiden zwei Fälle.

<u>Fall 1</u> $d = -\ell$, $\ell \equiv 3 \bmod 4$

Sei $A \in \Phi$, dann enthält A nach allgemeinen Sätzen über die Verteilung der Primideale auf „verallgemeinerte Idealklassen" ein Primideal $\mathfrak{p}$ ersten Grades; für $p = N(\mathfrak{p})$ ist dann bekanntlich $\left(\frac{p}{\ell}\right) = +1$, insbesondere $p \not\equiv -1 \bmod \ell$, also $N(\mathfrak{p}) \in R^*$.

<u>Fall 2</u> d enthält mindestens einen von ℓ verschiedenen Primteiler.

Ist $\alpha\mathcal{O} \in \mathfrak{P}$, so ist $N(\alpha\mathcal{O}) \equiv 1 \bmod \ell$, sodaß die Abbildung $\mathfrak{a} \mapsto \left(\frac{N(\mathfrak{a})}{\ell}\right)$ ($\mathfrak{a} \in I$; $\left(\frac{\cdot}{\ell}\right)$ ist das Legendre-Symbol) einen Charakter von Φ induziert. Sei $\Sigma \leq \Phi$ der Kern dieses Homomorphismus; Σ besteht also aus der Menge der $A \in \Phi$, die ein $\mathfrak{a}$ mit $\left(\frac{N(\mathfrak{a})}{\ell}\right) = +1$ enthalten.

Daneben betrachten wir die Menge $\Gamma \subseteq \Phi$ der Klassen A, die ein $\mathfrak{a}$ mit $N(\mathfrak{a}) \in R^*$ enthalten; Γ ist offenbar eine Untergruppe von Φ.

Es gilt

$$\Sigma \subseteq \Gamma \quad \text{falls } \ell \equiv 3 \bmod 4$$

$$\Phi - \Sigma \subseteq \Gamma \quad \text{falls } \ell \equiv 1 \bmod 4.$$

Ist nämlich $A \in \Sigma$ - falls $\ell \equiv 3 \bmod 4$, bzw. $A \in \Phi - \Sigma$ - falls $\ell \equiv 1 \bmod 4$, so enthält A ein Primideal $\mathfrak{p}$ ersten Grades; für dieses Primideal gilt dann $\left(\frac{N(\mathfrak{p})}{\ell}\right) = +1$ - für $\ell \equiv 3 \bmod 4$ - bzw $\left(\frac{N(\mathfrak{p})}{\ell}\right) = -1$ für $\ell \equiv 1 \bmod 4$, in jedem Fall $N(\mathfrak{p}) \not\equiv 0, -1 \bmod \ell$, daher - da $N(\mathfrak{p})$ eine Primzahl ist - $N(\mathfrak{p}) \in R^*$.

Da d mindestens einen von ℓ verschiedenen Primfaktor enthält, gibt es nach bekannten Schlüssen eine Primzahl p mit

$$\left(\frac{d}{p}\right) = +1 \quad , \quad \left(\frac{p}{\ell}\right) = -1 \quad , \quad p \not\equiv 0, -1 \bmod \ell$$

(hier wird zum ersten Mal benutzt, daß $\ell \geqq 5$ ist); ist daher $p = N(\mathfrak{p})$ für ein geeignetes Primideal $\mathfrak{p}$, A die zu $\mathfrak{p}$ gehörende (verallgemeinerte) Idealklasse, so ist

$$A \in (\Phi - \Sigma) \cap \Gamma .$$

Fassen wir zusammen, so haben wir

$$[\Phi : \Sigma] = 2$$

und

$$\Sigma \subsetneqq \Gamma \quad \text{für } \ell \equiv 3 \bmod 4,$$

$$\emptyset \neq \Phi - \Sigma \subseteq \Gamma \quad \text{für } \ell \equiv 1 \bmod 4,$$

in jedem Fall also $\Gamma = \Phi$. $\square$

<u>Lemma 2</u>

<u>Es gibt ein</u> $T \in GL_r(R)$, <u>sodaß</u>

$$Q(Tx) = a_1 x_1^2 + a_2 x_2^2 + \dots + a_r x_r^2$$

<u>für geeignete Zahlen</u> $a_1, a_2, \dots, a_r \in R$.

Beweis

Wir zeigen die Behauptung (scheinbar) allgemeiner für (positive) Formen Q mit Koeffizienten in R. Zur Abkürzung setzen wir

$$x \cdot y = Q(x+y) - Q(x) - Q(y)$$

für Spaltenvektoren $x, y \in R^r$.
Sei dR das von den Koeffizienten von Q erzeugte Ideal; es gibt dann ein $\alpha \in R^*$, sodaß $\frac{\alpha}{d} \cdot Q(x)$ eine Form mit ganzrationalen Koeffizienten, positiv und primitiv ist; nach Lemma 1 gibt es ein $y \in \mathbb{Z}^r$, sodaß $\frac{\alpha}{d} Q(y) \in R^*$, d.h. $\frac{1}{d}\, y \cdot y \in R^\times$ gilt. Das von den Komponenten von y erzeugte Ideal in R ist dann offenbar gerade R, sodaß eine R-Basis $y = y_1, \ldots, y_r$ von R^r existiert.
Nach Definition von d ist aber $y_i \cdot y_j \in dR$ für alle i,j, daher $\frac{y_i \cdot y_j}{y_1 \cdot y_1} \in R$ für alle i,j; dann ist aber auch
$y_1' = y_1$, $y_2' = y_2 - \frac{y_2 \cdot y_1}{y_1 \cdot y_1} y_1, \ldots, y_r' = y_r - \frac{y_r \cdot y_1}{y_1 \cdot y_1} y_1$ eine Basis von R^r.
Ist nun T die aus den Vektoren $y_1', y_2', \ldots, y_r'$ als Spalten gebildete Matrix, so gilt

$$Q(Tx) = Q(y_1')\, x_1^2 + Q_0(x_2, \ldots, x_r) \qquad \left(x = \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \right),$$

für eine positive Form Q_0 in $(r-1)$ Variablen.
Die Behauptung folgt hieraus leicht durch Induktion über die Anzahl der Variablen von Q. $\square$

3. Ist Q eine quadratische Form in r Variablen, ist A ein Automorphismus von Q, d.h. $A \in GL_r(\mathbb{Z})$ mit $Q(Ax) = Q(x)$ für alle $x \in \mathbb{Z}^r$, so können wir eine Form Q^A folgendermaßen definieren: sei $M = \{x \in \mathbb{Z}^r \mid Ax = x\}$; dann ist M ein freier $\mathbb{Z}$-Modul – etwa vom Rang t; sei $x_1, \dots, x_t$ eine Basis von M, $\{x_1, \dots, x_t\}$ die aus den Spalten $x_1, \dots, x_t$ gebildete Matrix; wir setzen $Q^A(y) = Q(\{x_1, \dots, x_t\} y)$ für $y \in \mathbb{Z}^t$.
Ist Q' eine weitere Form, so schreiben wir $Q' = Q^A$, falls Q' unimodular äquivalent ist zu einer der bis auf unimodulare Äquivalenz eindeutig bestimmten Formen Q^A.

Sei nun wieder Q eine positive quadratische Form in r Variablen mit ganzzahligen Koeffizienten und $d(Q) = \ell^n$ für eine Primzahl $\ell \geqq 5$. Es ist dann $e(Q) = \frac{1}{2}\{\ell^{\alpha_1} + \dots + \ell^{\alpha_r}\}$ für geeignete Zahlen $\alpha_1, \dots, \alpha_r$. Wir beweisen:

Lemma 3

Es gibt eine positive quadratische Form $\hat{Q}$ mit ganzzahligen Koeffizienten und einen Automorphismus A von $\hat{Q}$, dessen Ordnung eine Potenz von ℓ ist, sodaß $Q = \hat{Q}^A$ und $d(\hat{Q}) \in \bigcap_{p \not\equiv 0,-1 \bmod \ell} \mathbb{Z}_p^*$ gilt. Dabei kann $\hat{Q}$ so gewählt werden, daß $r(\hat{Q}) = 2e(Q)$.

Beweis

Nach Lemma 3 gibt es ein $T \in GL_r\left(\bigcap_{p \not\equiv 0,-1(\ell)} \mathbb{Z}_p^*\right)$, sodaß

$$Q(x) = Q_1(Tx),$$

wo

$$Q_1(x) = a_1 \ell^{\alpha_1} x_1^2 + \dots + a_r \ell^{\alpha_r} x_r^2 \qquad \left(x = \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \right)$$

für Zahlen $a_1, \dots, a_r \in \bigcap_{p \not\equiv 0,-1(\ell)} \mathbb{Z}_p^*$.

Wir setzen für $y = \begin{bmatrix} y_1 \\ \vdots \\ y_{\hat{r}} \end{bmatrix}$, wo $\hat{r} = 2e(Q)$;

$$Q_2(y) = \alpha_1 (y_1^2 + \dots + y_{\ell^{d_1}}^2) + \alpha_2 (y_{\ell^{d_1}+1}^2 + \dots + y_{\ell^{d_1}+\ell^{d_2}}^2) + \dots$$
$$\dots + \alpha_r (y_{\ell^{d_1}+\dots+\ell^{d_{r-1}}+1}^2 + \dots + y_{\hat{r}}^2).$$

sei $d = \det(T) \times \{$Hauptnenner von $\alpha_1, \dots, \alpha_r\}$, sei

$$M = \left\{ y = \begin{bmatrix} y_1 \\ \vdots \\ y_{\hat{r}} \end{bmatrix} \in \mathbb{Z}^{\hat{r}} \;\middle|\; y_1 \equiv \dots \equiv y_{\ell^{d_1}} \bmod d,\ y_{\ell^{d_1}+1} \equiv \dots \equiv y_{\ell^{d_1}+\ell^{d_2}} \bmod d, \dots, y_{\ell^{d_1}+\dots+\ell^{d_{r-1}}+1} \equiv \dots \equiv y_{\hat{r}} \bmod d \text{ und } \begin{bmatrix} y_1 \\ y_{\ell^{d_1}+1} \\ \vdots \\ y_{\ell^{d_1}+\dots+\ell^{d_{r-1}}+1} \end{bmatrix} \in T\mathbb{Z}^r \right\};$$

M ist ein freier $\mathbb{Z}$-Modul vom Rang $\hat{r}$; wir wählen eine Basis $z_1, \dots, z_{\hat{r}}$ von M und setzen

$$\hat{Q}(y) = Q_2(\{z_1, \dots, z_{\hat{r}}\} y), \text{ für } y \in \mathbb{Z}^{\hat{r}}$$

wo $\{z_1, \dots, z_{\hat{r}}\}$ für die aus den Spalten $z_1, \dots, z_{\hat{r}}$ gebildete Matrix steht.

Wir definieren eine $\mathbb{Z}$-lineare Abbildung $M \to M$ durch

$$y_1 \mapsto y_2 \mapsto y_3 \dots \mapsto y_{\ell^{d_1}} \mapsto y_1,$$
$$y_{\ell^{d_1}+1} \mapsto y_{\ell^{d_1}+2} \dots \mapsto y_{\ell^{d_1}+\ell^{d_2}} \mapsto y_{\ell^{d_1}+1},$$
$$- \quad - \quad - \quad -$$
$$y_{\ell^{d_1}+\dots+\ell^{d_{r-1}}+1} \mapsto \dots \mapsto y_{\hat{r}} \mapsto y_{\ell^{d_1}+\dots+\ell^{d_{r-1}}+1};$$

sei A die Matrix dieser Abbildung bzgl. der Basis $z_1, \dots, z_{\hat{r}}$. Offenbar ist A ein Automorphismus von $\hat{Q}$ der Ordnung ℓ^d, wo $d = \max[d_1, \dots, d_r]$, und man sieht leicht, daß $\hat{Q}^A = Q$.

Es ist Q_2 positiv und für $y \in M$ folgt aus der Definition von d, daß $Q_2(y) \in \mathbb{Z}$; also ist $\hat{Q}$ positiv und hat ganzzahlige Koeffizienten; es ist $r(\hat{Q}) = 2e(Q)$. Ferner ist $d\,\mathbb{Z}^{\hat{r}} \subseteq M$, daher ist $[\mathbb{Z}^{\hat{r}} : M]$ ein Teiler von $d^{\hat{r}}$, also ein Element von $\bigcap\limits_{p=0,-1(\ell)} \mathbb{Z}_p^*$, sodaß schließlich

$$d(\hat{Q}) = 2^{\hat{r}} a_1^{\ell^{d_1}} \times \ldots \times a_r^{\ell^{d_r}} \times [\mathbb{Z}^{\hat{r}} : M]^2 \in \bigcap_{p=0,-1(\ell)} \mathbb{Z}_p^* . \quad \boxed{\;}$$

Zu Q nehmen wir nun eine Form $\hat{Q}$ wie in Lemma 3; für jede Zahl n operiert dann die von β erzeugte Gruppe von Automorphismen auf der Menge $\{y \in \mathbb{Z}^{\hat{r}} \mid n = \hat{Q}(y)\}$, die daher bzgl. dieser Operation in Bahnen zerfällt; mit Hilfe dieser Zerlegung in Bahnen sieht man leicht

$$\Theta_Q \equiv \Theta_{\hat{Q}} \mod \ell$$

Indem man $q = e^{2\pi i z}$, $\operatorname{Im} z > 0$, setzt, wird $\Theta_{\hat{Q}}$ zu einer Modulform für $\Gamma_0(s(\hat{Q}))$ – vom Gewicht $e(Q)$, falls $\hat{Q}$ so gewählt wird, daß $r(\hat{Q}) = 2e(Q)$ gilt –.

Wir werden in 4. zeigen, daß für jedes $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ die Funktion $\Theta_{\hat{Q}}\left(\frac{az+b}{cz+d}\right) \Big/ (cz+d)^{e(Q)}$ ℓ-ganze Fourier-koeffizienten hat, und daß

$$\Theta_{\hat{Q}}\left(\frac{az+b}{cz+d}\right) \Big/ (cz+d)^{e(Q)} \equiv \Theta_{\hat{Q}} \mod \ell$$

gilt (es ist $\Theta_{\hat{Q}}\left(\frac{az+b}{cz+d}\right) / (cz+d)^{e(Q)} = \sum\limits_{n \geq 0} a_n e^{2\pi i z n/t}$ für geeignete a_n und eine ganze Zahl $t > 0$; "a_n ist ℓ-ganz" heißt, daß $u a_n$ ganz-algebraisch über $\mathbb{Z}$ ist für eine ganz-rationale Zahl $u \not\equiv 0 \mod \ell$, und die angegebene Kongruenz ist so zu lesen, daß

$a_n \equiv 0 \mod l$ gilt – d.h. $\frac{a_n}{l}$ l-ganz ist – falls $\frac{n}{t}$ nicht ganz ist, und $a_n \equiv \#\{y \in \mathbb{Z}^{\hat{r}} \mid \frac{n}{t} = \hat{Q}(y)\} \mod l$ gilt, falls $\frac{n}{t}$ ganz ist.)

Aus dieser Kongruenz folgt, daß $\Theta_{\hat{Q}}$ vom Haupttyp ist, also

$$f := \sum \Theta_{\hat{Q}}\left(\frac{az+b}{cz+d}\right) \Big/ (cz+d)^{e(Q)}$$

– wo $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ein Repräsentantensystem für $\Gamma_0(S(\hat{Q}))\backslash Sl_2\mathbb{Z}$ durchläuft – von der Wahl der Repräsentanten unabhängig ist und eine Modulform der Stufe 1 mit l-ganzen Fourierkoeffizienten vom Gewicht $e(Q)$ darstellt, und daß

$$f \equiv [Sl_2(\mathbb{Z}) : \Gamma_0(S(\hat{Q}))]\, \Theta_{\hat{Q}} \mod l$$

gilt. Es ist aber $S(\hat{Q}) \in \bigcap_{p \in v_{i-1}(l)} \mathbb{Z}_p^*$, daher

$$[Sl_2(\mathbb{Z}) : \Gamma_0(S(\hat{Q}))] = S(\hat{Q}) \prod_{p \mid S(\hat{Q})} \left(1 + \frac{1}{p}\right) \not\equiv 0 \mod l,$$

so daß wir also eine Modulform f' der Stufe 1 vom Gewicht $e(Q)$ mit l-ganzen Koeffizienten und $f' \equiv \Theta_Q \mod l$ finden; bekanntlich kann f' geschrieben werden als $f' = \sum_i c_i g_i$ für geeignete l-ganze Zahlen c_i und Modulformen g_i der Stufe 1, Gewicht $e(Q)$, mit ganz-rationalen Fourierkoeffizienten, so daß man unter Beachtung von $\Theta_Q \in \mathbb{Z}[\![q]\!]$ leicht einsieht, daß $f' \in \mathbb{Z}[\![q]\!]$ gewählt werden kann. Damit wäre der angekündigte Satz dann bewiesen.

4. Ist Q eine positive Form mit ganzzahligen Koeffizienten in einer geraden Anzahl r von Variablen, so setzen wir $\Lambda = M^*/\mathbb{Z}^r$, wo $M^* = \{ y \in \mathbb{Q}^r \mid x.y \in \mathbb{Z} \text{ für alle } x \in \mathbb{Z}^r \}$ und $x.y = Q(x+y) - Q(x) - Q(y)$ ist. Λ ist eine endliche abelsche Gruppe der Ordnung $d(Q)$.

Sei $\mathbb{C}[\Lambda]$ der von (der Menge) Λ erzeugte freie $\mathbb{C}$-Modul. Bekanntlich gibt es eine Operation von $SL_2(\mathbb{Z})$ auf $\mathbb{C}[\Lambda]$ mit folgenden Eigenschaften:

Ist $S \in SL_2(\mathbb{Z})$, $\lambda \in \Lambda$ und

$$S\lambda = \sum_{\mu \in \Lambda} z_\mu \cdot \mu ,$$

so ist

$$\Theta_\lambda |_S = \sum_{\mu \in \Lambda} z_\mu \, \Theta_\mu ,$$

wo

$$\Theta_\lambda = \sum_{y \in \lambda} e^{2\pi i z \, Q(y)}, \quad \text{also } \Theta_0 = \Theta_Q ,$$

und

$$\Theta_\lambda |_S (z) = \Theta_\lambda \left(\frac{az+b}{cz+d} \right) \Big/ (cz+d)^{r/2} \quad \text{ist.}$$

Dabei ist für $\lambda = x + \mathbb{Z}^r$:

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \lambda = \frac{e^{-\pi i r/4}}{\sqrt{d(\Lambda)}} \sum_{\mu = y + \mathbb{Z}^r \in \Lambda} e^{2\pi i \, x.y} \, \mu ,$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \lambda = e^{2\pi i \, Q(x)} \, \lambda .$$

Daneben gibt es eine Operation der Automorphismengruppe $\mathfrak{A}$ von Q auf Λ:

Ist $\lambda = x + \mathbb{Z}^r \in \Lambda$, $A \in \mathfrak{A}$, so ist

$$A\lambda = Ax + \mathbb{Z}^r .$$

Diese Operation setzt sich in natürlicher Weise fort zu einer Operation von $\mathfrak{A}$ auf dem freien $\mathbb{C}$-Modul $\mathbb{C}[\Lambda]$.

Es gilt

Lemma 4

Für $\rho \in \mathbb{C}[\Lambda]$, $A \in \mathfrak{A}$, $S \in Sl_2(\mathbb{Z})$ gilt:
$$A(S\rho) = S(A\rho).$$

Beweis

Für $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ prüft man das Lemma mit Hilfe der angegebenen Formeln leicht nach. Für allgemeine S folgt die Behauptung durch Induktion über die Länge eines Wortes in $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. $\square$

Wir zeigen schließlich

Lemma 5

Gibt es einen Automorphismus A von Q, dessen Ordnung eine Potenz der Primzahl ℓ ist, sodaß $Q^A \neq 0$ und $d(Q)$ und $d(Q^A)$ teilerfremd sind, so sind zwei Fälle möglich:

i) $d(Q^A) = 1$

oder

ii) $d(Q^A) = \ell^n$ für ein $n > 0$.

Im Fall ii) hat $\Theta_Q|S$ für jedes $S \in Sl_2(\mathbb{Z})$ ℓ-ganze Fourierkoeffizienten und es gilt
$$\Theta_Q|S \equiv \Theta_Q \mod \ell.$$

Beweis:

Wir betrachten die folgenden $\mathbb{Z}$-Moduln:

$M = \mathbb{Z}^r$, $M^* = \{y \in \mathbb{Q}^r \mid x.y \in \mathbb{Z}$ für alle $x \in M\}$,

$M^A = \{x \in M \mid Ax = x\}$, $(M^*)^A = \{y \in M^* \mid Ay = y\}$,

$(M^A)^* = \{y \in \mathbb{Q}^r \mid Ay = y$ und $x.y \in \mathbb{Z}$ für alle $x \in M^A\}$.

Offenbar ist $(M^*)^A \subseteq (M^A)^*$.

Daneben gilt $\ell^t (M^A)^* \subseteq (M^*)^A$, wenn ℓ^t die Ordnung von A ist:
ist nämlich $y \in (M^A)^*$, $x \in M$, so haben wir
$\ell^t y \cdot x = (\sum_{i=1}^{\ell^t} A^i y) \cdot x = y \cdot \sum_{i=1}^{\ell^t} A^i x \in \mathbb{Z}$, denn $\sum_{i=1}^{\ell^t} A^i x \in M^A$.

Aus $\ell^t (M^A)^* \subseteq (M^*)^A$ folgt nun $[(M^A)^* : (M^*)^A] = \ell^n$ für ein $n \geq 0$, daher

$$d(Q^A) = [(M^A)^* : M^A] = [(M^A)^* : (M^*)^A] \times [(M^*)^A : M^A]$$
$$= \ell^n \times [(M^*)^A : M^A].$$

Die kanonische Abbildung $(M^*)^A / M^A \longrightarrow M^*/M$ ist aber injektiv, daher ist $[(M^*)^A : M^A]$ ein Teiler von $d(Q)$; $d(Q)$ und $d(Q^A)$ sind teilerfremd, sodaß $[(M^*)^A : M^A] = 1$ gelten muß.

Damit ist $d(Q^A) = \ell^n$.

Sei nun $n > 0$, sodaß insbesondere $d(Q) \not\equiv 0 \mod \ell$ gilt:
Ist $\lambda = y + M \in \Lambda = M^*/M$ und gilt $A\lambda = \lambda$, d.h. $Ay \equiv y \mod M$, so ist einerseits $\sum_{i=1}^{\ell^t} A^i y \equiv \ell^t y \mod M$, andererseits $\sum_{i=1}^{\ell^t} A^i y \in M^A \subseteq M$; daher ist $\ell^t y \equiv 0 \mod M$, und wegen $[M^* : M] = d(Q) \not\equiv 0 \mod \ell$ folgt $y \equiv 0 \mod M$, d.h. $\lambda = 0$.

Ist daher $\langle A \rangle$ die von A erzeugte zyklische Gruppe der Ordnung ℓ^t, und bezeichnet $_{\langle A \rangle}\backslash\Lambda$ die Menge der Bahnen in die Λ bzgl. der Operation von $\langle A \rangle$ zerfällt, so ist für jedes $B \in {}_{\langle A \rangle}\backslash\Lambda$, $B \neq \{0\}$ nach bekannten Schlüssen: $\# B \equiv 0 \mod \ell$.

Mit

$$S\lambda = \sum_{\mu\in\Lambda} z_\mu \mu ,$$

erhalten wir

$$\Theta_Q|_S = \sum_{\mu\in\Lambda} z_\mu \Theta_\mu$$

$$= z_0 \Theta_Q + \sum_{\substack{B\in \langle A\rangle\backslash\Lambda \\ B\neq\{0\}}} \sum_{\mu\in B} z_\mu\cdot \Theta_\mu ;$$

für $\mu,\mu'\in B$ ist aber $z_\mu = z_{\mu'}$ – wie man aus Lemma 4 abliest – und offenbar $\Theta_\mu = \Theta_{\mu'}$; also folgt für $B\neq\{0\}$ aus $\# B \equiv 0 \bmod \ell$, daß $\sum_{\mu\in B} z_\mu \Theta_\mu \equiv 0 \bmod \ell$, d.h.

$$\Theta_Q|_S \equiv z_0\Theta_Q \mod \ell .$$

Dabei ist noch nachzuprüfen, daß $\Theta_Q|_S$ ℓ-ganze Fourierkoeffizienten hat; dies folgt aber leicht durch Induktion über die Länge eines Wortes in $\begin{bmatrix}0&-1\\1&0\end{bmatrix}$, $\begin{bmatrix}1&1\\0&1\end{bmatrix}$, wobei man die angegebenen Formeln für das Transformationsverhalten der Θ_λ bzgl $\begin{bmatrix}0&-1\\1&0\end{bmatrix}$, $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ und $d(Q)\not\equiv 0 \bmod \ell$ benutzt.

Ist $\mathfrak{R}$ der Ring der ℓ-ganzen Zahlen, $\mathfrak{K}$ die Kommutatoruntergruppe von $Sl_2(\mathbb{Z})$, so sieht man leicht, daß $S\mapsto z_0$ einen Homomorphismus $Sl_2(\mathbb{Z})/\mathfrak{K} \longrightarrow \mathfrak{R}^*$ induziert; dabei ist $\begin{bmatrix}1&1\\0&1\end{bmatrix}\mathfrak{K} \longmapsto 1$, und da $\begin{bmatrix}1&1\\0&1\end{bmatrix}\mathfrak{K}$ die Gruppe $Sl_2(\mathbb{Z})/\mathfrak{K}$ erzeugt, gilt stets $z_0 \equiv 1 \bmod \ell$, womit alles bewiesen ist. $\square$