Satz

Unter der Voraussetzung $r \equiv \frac{p+1}{2} \mod p-1$ gilt:

$$\Theta(\mathcal{O}_p) \bmod p \subseteq M_r(\mathcal{O}_p) \bmod p$$

und für jedes Primideal $\mathfrak{P}$ mit $\mathfrak{P} \mid p$:

$$\Theta(\mathcal{O}_{\mathfrak{P}}) \bmod \mathfrak{P} \subseteq M_r(\mathcal{O}_{\mathfrak{P}}) \bmod \mathfrak{P}.$$

Beweis

Weiter unten in 4.) wird bewiesen, daß zu jeder Idealklasse C von $\mathbb{Q}(\sqrt{-p})$ eine $f \in M_{\frac{p+1}{2}}(\mathbb{Z})$ existiert, sodaß $\Theta_C \equiv f \mod p$.

~~Ist $r = \frac{p+1}{2} + t(p-1)$~~,

Nach der Von-Staudtschen Kongruenz für die Bernoullischen Zahlen ist $E_{p-1} \equiv 1 \mod p$,

Daher haben wir – mit $r = \frac{p+1}{2} + t(p-1)$ für eine geeignete Zahl t –:

$$\Theta_C \equiv f E_{p-1}^{t} \mod p \quad \text{und} \quad f E_{p-1}^{t} \in M_r(\mathbb{Z}).$$

Der Satz folgt nun unmittelbar aus Proposition 1. □

Mit den üblichen Schlußweisen der linearen Algebra sieht man leicht, daß

$$M_r(\mathcal{O}_p) \bmod p = \Theta(\mathcal{O}_p) \bmod p \oplus \bigoplus_{n=1}^{\dim S_r - \frac{h(-p)-1}{2}} \mathcal{O}_p/p\mathcal{O}_p \; \overline{g_{i_n}}$$

(für geeignete Zahlen i_n, wo $g_1, g_2, \ldots$ die oben erwähnte $\mathbb{Z}$-Basis von $S_r(\mathbb{Z})$ bedeutet; wir können $g_i = \Delta^i E_4^a E_6^b$ für geeignete Zahlen a, b und mit $\Delta = q \prod_{n=1}^{\infty}(1-q^n)^{12}$ wählen.

So erhält man beispielsweise für $p \leq 163$:

$$M_{\frac{p+1}{2}}(\mathcal{O}_p) \bmod p = \Theta(\mathcal{O}_p) \bmod p \quad \text{für } p = 7, 11, 19, 23, 31, 47, 71$$

$$\Theta(\mathcal{O}_p) \bmod p = \mathcal{O}_p/p\mathcal{O}_p \, E_{\frac{p+1}{2}} \quad \text{für } p = 7, 11, 19, 43, 67, 103, 163$$

und für die übrigen p: