__Satz__

Sei p eine Primzahl, $p = 8\ell - 1$ für ein $\ell > 0$;

sei $\Theta_{[1,1,2\ell]}(z) = \sum_{r,s \in \mathbb{Z}} q^{r^2 + rs + 2\ell s^2}$ $\quad (q = e^{2\pi i z})$.

Dann besteht eine Kongruenz der Gestalt

$$\Theta_{[1,1,2\ell]} \equiv \sum_{\lambda = 0}^{[\frac{\ell}{3}]} \alpha_\lambda E_4^{\ell - 3\lambda} \Delta^\lambda \quad \text{modulo } p$$

$\underline{\lambda} \quad \lambda = \lambda$

für geeignete ganze Zahlen α_λ; dabei ist

$$E_4 = 1 + 240 \sum_{n>0} \sigma_3(n) q^n, \quad \Delta = q \prod_{n>0} (1-q^n)^{24}.$$

Der Beweis geht über die Folgenden Lemmata.

Sei
$$\psi_0 = \sum_{n \in \mathbb{Z}} q^{n^2} = \prod_{n>0} (1 - q^{2n})(1 + q^{2n-1})^2,$$
$$\psi_1 = \sum_{n \in \mathbb{Z}} q^{\frac{(2n+1)^2}{4}} = 2 \times q^{\frac{1}{4}} \prod_{n>0} (1-q^{2n})(1+q^{2n})^2.$$

__Lemma 1__

$$\Theta_{[1,1,2\ell]} \equiv \psi_0^{p+1} + \psi_1^{p+1} \quad \text{modulo } p.$$

__Beweis__

$$\Theta_{[1,1,2\ell]} = \sum_{r,s} q^{r^2 + rs + 2\ell s^2} = \sum_{r,s} q^{\frac{(2r+s)^2 + (8\ell - 1)s^2}{4}}$$

$$= \sum_{t \bmod 2} \sum_{r \equiv t (2)} q^{\frac{r^2}{4}} \sum_{s \equiv t (2)} q^{\frac{p s^2}{4}} = \psi_0(z)\psi_0(pz) + \psi_1(z)\psi_1(pz)$$

$$= \Big\{\prod_{n>0} (1-q^{2n})(1+q^{2n-1})^2\Big\}\Big\{\prod_{n>0}(1-q^{p \times 2n})(1+q^{p(2n-1)})^2\Big\}$$

$$+ 2^2 q^{4\ell} \Big\{\prod_{n>0}(1-q^{2n})(1+q^{2n})^2\Big\}\Big\{\prod_{n>0}(1-q^{p\times 2n})(1+q^{p \times 2n})^2\Big\};$$

wegen $(1 \pm q^{p \times r}) \equiv (1 \pm q^r)^p$ modulo p und $2^2 \equiv 2^{p+1}$ mod p

folgt hieraus die Behauptung. ✓

$$f(q) \in \mathbb{Z}[[q]] \Rightarrow f(q^p) \equiv f(q)^p \ (\text{mod } p)$$

$f(z) \qquad f(pz)$

Lemma 2

$$\psi_0\left(-\frac{1}{z}\right) = \sqrt{-iz} \times \frac{1}{\sqrt{2}} \left(\psi_0(z) + \psi_1(z) \right),$$
$$\psi_1\left(-\frac{1}{z}\right) = \sqrt{-iz}\ \frac{1}{\sqrt{2}} \left(\psi_0(z) - \psi_1(z) \right).$$

Ein Beweis hierfür folgt weiter unten.

Im Folgenden sei K ein Körper (~~mit~~ Charakteristik $\neq 2$), mit der Eigenschaft, daß ein $w \in K$ mit $w^2 = 2^{-1}$ existiert;
da $p \equiv -1 \bmod 8$ ist $\left(\frac{2}{p}\right) = +1$, d.h. $\mathbb{Z}/p\mathbb{Z}$ ist insbesondere solch ein Körper K.

Für ein Polynom $h = h(X,Y) \in K[X,Y]$ sei
$$h^* = h(w(X+Y), w(X-Y)).$$
Offenbar ist $(-)^*$ ein K-Algebren-Automorphismus, der zu sich selbst invers ist (d.h. $(h^*)^* = h$).

Hieraus ergibt sich leicht, daß
$$(X+Y)X \quad \text{und} \quad (X-Y)Y$$
invariant unter $*$ sind ($h \in K[X,Y]$ heißt invariant (unter $*$), falls $h^* = h$!), daher auch
$$X^2 + Y^2, \quad (X^2-Y^2)XY$$
invariant sind,
und schließlich ~~somit~~
$$f := (X^2+Y^2)^4 - 4X^2Y^2(X^2-Y^2)^2$$
$$= X^8 + Y^8 + 14X^4Y^4$$
und
$$g := \left[(X^2+Y^2)(X^2-Y^2)XY\right]^4 = (X^4-Y^4)^4 X^4 Y^4$$
invariant sind.

Mit Lemma 2 und der Produktdarstellung von ψ_0 und ψ_1 folgt nun aus der Invarianz von f und g, daß

$g(\psi_0, \psi_1)$ Spitzenform der Stufe 1 vom Gewicht 12

und $f(\psi_0, \psi_1)$ Modulform der Stufe 1 vom Gewicht 4 ist;

So folgt leicht:

$$\psi_0^8 + \psi_1^8 + 14\,\psi_0^4\psi_1^4 = E_{4}$$

$$(\psi_0^4 - \psi_1^4)^4\,\psi_0^4\psi_1^4 = 16\,\Delta .$$

<u>Lemma 3</u>

Es sei $h \in k[X,Y]$ invariant unter $(\,)^*$ und h sei von der Gestalt

$$h = \sum_{\cancel{r,s}\,n} a_{rs}\, X^{4r+2}\, Y^{4s+2} \qquad \text{für ein } 0 < 2 \leqq 4 .$$

Dann ist

$$h = (X^4 - Y^4)\, X Y\, h',$$

wo h' invariant unter $(\,)^*$ ist und von der Gestalt

$$h' = \sum a'_{rs}\, X^{4r+2-1}\, Y^{4s+2-1}.$$

<u>Beweis</u>

Aus der Invarianz von h folgt

$$h(Y,Y) = h^*(Y,Y) = h(2wX, 0) = 0 .$$

Wir haben somit

$$\begin{aligned} h &= h - h(Y,Y) \\ &= \sum a_{rs}\,(X^{4r+2} - Y^{4r+2})\, Y^{4s+2} \\ &= (XY)^2 \sum a_{rs}\,(X^{4r} - Y^{4r})\, Y^{4s} \\ &= (XY)^2 \sum a_{rs}\,(X^4 - Y^4)(X^{4(r-1)} + X^{4(r-2)}Y + \dots)\, Y^{4s} \\ &= (XY)^2 (X^4 - Y^4) \sum a'_{rs}\, X^{4r}\, Y^{4s} \qquad \text{für geeignete } a'_{rs} . \end{aligned}$$

Wir haben also eine Darstellung

$$h = (X^4 - Y^4)\, XY\, h'$$

der behaupteten Form; es bleibt zu zeigen, daß h' invariant ist.
Nun ist aber h und $(X^4 - Y^4)\,XY$ invariant, — woraus mit der Nullteilerfreiheit von $k[X,Y]$ — leicht die ~~[illegible]~~ Invarianz von h' folgt.

Korollar

Ist $h = \sum a_{rs} X^{4r+4} Y^{4s+4}$ invariant, so gibt es ein $h' = \sum a'_{rs} X^{4r} Y^{4s}$, ~~sodaß~~ welches invariant ist, sodaß

$$h = (X^4 - Y^4)^4 X^4 Y^4 \cdot h'.$$

~~Lemma 4~~

~~Ist h invariant unter $(-)^*$~~ und

Lemma 4

Sei $h \in K[X,Y]$ eine Form vom Grade $8n$, h sei symmetrisch in X und Y, und invariant unter $(-)^*$; zudem enthalte h nur Monome der Gestalt $X^{4r} Y^{4s}$.

Dann gibt es $a_z \in K$, sodaß

$$h = \sum_{z=0}^{[\frac{n}{3}]} a_z f^{n-3z} g^z.$$

Beweis (durch Induktion über n)

Für $n = 0$ ist nichts zu zeigen.

~~Die B~~ Sei also $n > 0$, und die Behauptung gelte für alle $k < n$.

Fall 1 h ist von der Gestalt: $h = \sum a_{rs} X^{4r+4} Y^{4s+4}$.

Dann gibt es ein h' mit

$$h = g h';$$

wie man leicht sieht, läßt sich aber auf h' die Induktionsvoraussetzung anwenden; damit folgt aber leicht die Induktionsbehauptung.

Fall 2 h ist von der Gestalt $h = a(X^{8n} + Y^{8n}) + \sum a_{rs} X^{4r+4} X^{4s+4}$;

Dann erfüllt $h - a f^n$ die Voraussetzung von Fall 1, besitzt also eine Darstellung der gewünschten Art, woraus die Behauptung für h folgt. □

Es ist nun

$$X^{p+1} + Y^{p+1}$$

– aufgefasst als Polynom über $\mathbb{Z}/p\mathbb{Z}$ – invariant unter $(\ )^{\tau}$:

$$[w(X+Y)]^{p+1} + [w(X-Y)]^{p+1}$$

$$\equiv w^{p+1} \{ [X^{p+1} + X^p Y + X Y^p + Y^{p+1}] + [X^{p+1} - X^p Y - X Y^p + Y^{p+1}] \}$$

$$\equiv w^2 \{ 2 X^{p+1} + 2 Y^{p+1} \} \equiv X^{p+1} + Y^{p+1} \text{ modulo } p.$$

Also gilt es ganze Zahlen a_λ, sodass

$$X^{p+1} + Y^{p+1} \equiv \sum_{\lambda=0}^{[\frac{\ell}{3}]} a_\lambda f^{\frac{\ell}{4}-3\lambda} g^\lambda \mod p.$$

Diese Kongruenz bleibt richtig, wenn wir X und Y durch ψ_0 und ψ_1 ersetzen, wodurch dann der angekündigte Satz folgt.

So folgt also:

$$\Theta_{[1,1,2]} \equiv E_4 \mod 7$$

Q

$$\Theta_{[1,1,6]} \equiv E_4^3 ~~+~~ 5\Delta \mod 23$$

$Q^3 - 5\frac{(Q^3-R^2)}{1728}$

$$\Theta_{[1,1,8]} \equiv E_4^4 + 3 E_4 \Delta \mod 31$$

$P = G_2$

$Q = E_4$

$R = E_6$

$\Delta = \frac{Q^3-R^2}{1728}$

$$E_4 = \sum{}' \sigma_3(n) q^n$$

$$\sigma_3(n) \underset{7}{\equiv} \underbrace{\sum_{d|n} \left(\frac{-7}{d}\right)}$$

$$\sum_{d|n} \left(\frac{-23}{d}\right) \underset{23}{\equiv} \sigma_{11}$$

$$\Theta_{[1,1,6]} + 2\Theta_{[2,1,3]} \underset{23}{\equiv} E_{12}$$

$$\frac{1}{2}\left(\Theta_{[1,1,6]} - \Theta_{[2,1,3]}\right) \equiv \Delta \quad (23)$$

$\tau(p)$

$\equiv \sigma_{11}(p)$

$\left(\frac{-23}{p}\right) = -1 \quad p \neq 23$

Sei $A > 0$ und für $0 \leq t \leq A$:

$$\psi_t(z) = \sum_{r \equiv t\,(2A)} q^{\frac{r^2}{4A}} = q^{\frac{t^2}{4A}} \prod_{n>0} (1-q^{2An})(1+q^{2An-A+t})(1+q^{2An-A-t});$$

ferner (*).
insbesondere

$$\psi_0 = \prod_{n>0}(1-q^{2An})(1+q^{(2n-1)A})^2,$$

$$\psi_A = 2\,q^{\frac{A}{4}} \prod_{n>0}(1-q^{2An})(1+q^{2An})^2.$$

Lemma 1

$$\psi_s\left(-\frac{1}{z}\right) = \sqrt{-iz}\,\frac{1}{\sqrt{2A}}\left\{\psi_0 + 2\cos\frac{2\pi s}{2A}\,\psi_1 + \dots + 2\cos\frac{2\pi s(A-1)}{2A}\,\psi_{A-1} + (-1)^s\psi_A\right\}.$$

Der Beweis folgt weiter unten.

~~Lemma 2~~

Sei $p = 4AC - B^2$ eine Primzahl, $\theta_{[A,B,C]}(z) = \sum_{r,s\in\mathbb{Z}} q^{Ar^2+Brs+Cs^2}$ und $q = e^{2\pi i z}$.

Dann gilt:

Lemma 2

$$\theta_{[A,B,C]} \equiv \sum_{s \bmod 2A} \psi_s(pz)\,\psi_{Bs}(z) \quad \text{~~modulo~~}$$

Beweis

$$\theta_{[A,B,C]} = \sum_{r,s} q^{Ar^2+Brs+Cs^2} = \sum_{r,s} q^{\frac{(2Ar+Bs)^2+ps^2}{4A}}$$

$$= \sum_{t \bmod 2A}\ \sum_{s\equiv t\,(2A)} q^{\frac{ps^2}{4A}} \sum_r q^{(2Ar+Bs)^2/4A}$$

$$= \sum_{t \bmod 2A}\Big(\sum_{s\equiv t\,(2A)} q^{\frac{ps^2}{4A}}\Big)\Big(\sum_{r\equiv Bt\,(2A)} q^{\frac{r^2}{4A}}\Big).$$

(*) Zu jeder Zahl s gibt es genau ein t mit $0 \leq t \leq A$, sodaß ~~$s \equiv \pm t$~~ $s \equiv t\ (2A)$ oder $s \equiv -t\ (2A)$; wir bezeichnen dieses t mit $t = \langle s \rangle$;
Sei $\psi_s := \psi_t$.