Über die Kloostermanschen Summen $S(u, v; q)$.

Von

Hans Salié in Leipzig.

Sei $q \geqq 1$ eine positive ganze Zahl und

$$\varepsilon = e^{\frac{2\pi i}{q}} \tag{1}$$

q-te Einheitswurzel. Sei ferner $(h, q) = 1$, dann gehört zu jedem ganzen $h \geqq 1$ eindeutig ein ganzes $\bar{h}$, so daß

$$h\bar{h} \equiv 1 \pmod{q}, \quad 0 < \bar{h} \leqq q \tag{2}$$

ist.

Bedeuten u, v beliebige ganze Zahlen, so ist nach Herrn Kloosterman [1])

$$S(u, v; q) = \sum_{\substack{0 < h \leqq q \\ (h, q) = 1}} \varepsilon^{uh + v\bar{h}}. \tag{3}$$

Da die Summen (3) in den Untersuchungen über die Abschätzungen von Fourierkoeffizienten ganzer Modulformen und deren Anwendungen auf die additive Zahlentheorie eine entscheidende Rolle spielen [2]), sei mir gestattet, auf die Eigenschaften der $S(u, v; q)$ zurückzukommen.

Es genügt im folgenden, $S(u, v; q)$ für den Fall

$$q = p^m, \quad m \geqq 1 \text{ ganz}, \quad p \text{ Primzahl} \tag{4}$$

zu untersuchen; denn für jedes

$$q = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}, \quad p_1 \neq p_2 \neq \dots \neq p_r \tag{5}$$

kann man $S(u, v; q)$ multiplikativ aus Summen (3) mit $q = p_r^{m_r}$ zusammensetzen. Es lassen sich nämlich [3]) bei jedem ganzen u zu jeder ganzen Zahl v

[1]) Acta math. 49 (1926), S. 420.

[2]) Kloosterman, I) Acta math. 49 (1926), S. 407—464; II) Hamb. Abh. V (1927), S. 337—352. — Estermann, Hamb. Abh. VII (1929), S. 82—98 (kurz E. zitiert).

[3]) E., S. 91.

ganze Zahlen $v_1, v_2, \ldots, v_\nu$ finden, so daß

$$S(u, v; q) = \prod_{r=1}^{\nu} S(u, v_r; p_r^{m_r}) \tag{6}$$

wird.

Bisher scheint nicht bemerkt worden zu sein, daß sich für

$$q = p^m, \quad m > 1 \text{ ganz}, \quad p \text{ Primzahl}, \quad (u, q) = (v, q) = 1 \tag{7}$$

$S(u, v; q)$ durch Gaußsche Summen ausdrücken läßt, woraus insbesondere

$$|S(u, v; q)| < C\sqrt{q}, \quad C \text{ unabhängig von } u, v, q, \tag{7a}$$

folgt.

Durch Herrn Estermann[4]) ist bis jetzt für alle q

$$|S(u, v; q)| \leqq \left[d\left(\frac{q}{(u, q)}\right)\right]^{\frac{3}{4}} q^{\frac{3}{4}} (u, q)^{\frac{1}{4}} \tag{8}$$

bekannt, wobei $d(x)$ die Anzahl der positiven Teiler von x bezeichnet.

In der vorliegenden Arbeit werden (§ 1) die $S(u, v; q)$ nach dem quadratischen Restcharakter von u und v eingeteilt. Die dadurch sich ergebenden Summen $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu, N_0)$ — N_0 ein Nichtrest mod q — erweisen sich in manchen Formeln zweckmäßiger als die bezüglich u, v nicht getrennten $S(u, v; q)$. Vor allem tritt die Berechtigung der Aufspaltung beim Beweise von (7a) zutage (§ 2, § 3).

Wenn q Primzahl ist (§§ 4, 5, 6), gelingt zwar eine explizite Auswertung von $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu)$ durch Gaußsche Summen nicht, wie es unter der Voraussetzung von (7) möglich war. Doch lassen sich für die $f(\varepsilon^\nu)$ Formeln aufstellen, die mit Gaußschen Summen verknüpft und der Bauart nach verwandt erscheinen.

Weiter zeigt sich, daß $f(\varepsilon^\nu)^2$ und $g(\varepsilon^\nu)^2$ linear darstellbar (mit Koeffizienten $\leqq 1$) durch die $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu)$ sind.

Schließlich geben die mit $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu)$ gebildeten Summen Zusammenhänge mit Formeln, wie sie in der Theorie der Verteilung der quadratischen Reste aufgestellt werden[5]).

---

[4]) E., S. 83. Vermutlich ist die Abschätzung (7a) in der Form

$$|S(u, v; q)| < C q^{\frac{1}{2}+\varepsilon} (u, q)^{\frac{1}{2}} \quad \varepsilon > 0 \text{ beliebig}$$

für alle q gültig. Auf den Beweis dieser Abschätzung hoffe ich demnächst zurückkommen zu können. Der Hauptsatz in K. II (siehe auch E., S. 83) würde dann

$$c_n = O\left(n^{\frac{\pi}{2}-\frac{1}{4}+\varepsilon}\right)$$

lauten.

[5]) E. Jacobsthal, J. f. d. r. u. angew. Math. 132 (1907), S. 238—245. — H. Hopf, Math. Zeitschr. 32 (1930), S. 222—231.

§ 1.

Alle $S(u, v; q)$ sind reell, wie aus der Darstellung

$$(9)\qquad \begin{aligned} S(u, v; q) &= 1 && \text{für } q = 1\\ &= (-1)^{u+v} && \text{für } q = 2\\ &= \sum_{\substack{0<h\leqq\frac{q}{2}\\(h,q)=1}} \left(\varepsilon^{uh+v\bar{h}} + \varepsilon^{-(uh+v\bar{h})}\right) && \text{für } q \geqq 3\\ &= 2\sum_{\substack{0<h\leqq\frac{q}{2}\\(h,q)=1}} \cos\frac{2\pi}{q}(uh + v\bar{h}) \end{aligned}$$

hervorgeht, die überdies

$$(10)\qquad S(-u, -v; q) = S(u, v; q)$$

zeigt.

Unter den bekannten, für alle q gültigen Eigenschaften der $S(u, v; q)$ hebe ich hervor:

1. die Symmetrie-Eigenschaft:

$$(11)\qquad S(u, v; q) = S(v, u; q)\ ^{6});$$

2. $(u, q) = 1$, v beliebig,

$$(12)\qquad S(u, v; q) = S(1, uv; q)\ ^{7})$$

und entsprechend

$(v, q) = 1$, u beliebig,

$$(12a)\qquad S(u, v; q) = S(1, uv; q);$$

3. $v \equiv 0 \pmod q$

$$(13)\qquad S(u, v; q) = \sum_{t/(u, q)} t\,\mu\left(\frac{q}{t}\right).$$

4. $(u, q) = 1$, $v \equiv 0 \pmod q$

$$(13a)\qquad S(u, v; q) = \mu(q)$$

und $u \equiv 0$, $v \equiv 0 \pmod q$

$$(13b)\qquad S(u, v; q) = \varphi(q),$$

wobei $\mu(q)$ das Möbiussche Symbol und $\varphi(q)$ die Eulersche Funktion bezeichnet.

---

6) E., S. 89.
7) E., S. 87.

Sei nunmehr

$$f(\varepsilon) = \sum_{\substack{0<h<q \\ (h,q)=1}} \varepsilon^{h+\bar{h}}, \qquad q \geqq 2, \tag{14}$$

und

$$g(\varepsilon, N_0) = \sum_{\substack{0<h<q \\ (h,q)=1}} \varepsilon^{h+N_0\bar{h}}, \qquad q \geqq 3, \tag{15}$$

mit $(N_0, q) = 1$, N_0 quadratischer Nichtrest mod q.

Bildet man für jedes zu q prime ν $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu, N_0)$ unter Berücksichtigung von (12), so folgt:

$$f(\varepsilon^\nu) = \sum_{\substack{0<h<q \\ (h,q)=1}} \varepsilon^{\nu(h+\bar{h})} = \sum_{\substack{0<h<q \\ (h,q)=1}} \varepsilon^{h+\nu^2\bar{h}} = S(1, \nu^2; q), \tag{16}$$

$$g(\varepsilon^\nu, N_0) = \sum_{\substack{0<h<q \\ (h,q)=1}} \varepsilon^{\nu(h+N_0\bar{h})} = \sum_{\substack{0<h<q \\ (h,q)=1}} \varepsilon^{h+N_0\nu^2\bar{h}} = S(1, N_0\nu^2; q). \tag{17}$$

Es ist also:

$$(u, q) = 1, \ (v, q) = 1,$$

$$S(u, v; q) = \begin{cases} f(\varepsilon^\nu), & \nu^2 \equiv uv \pmod q \\ g(\varepsilon^\nu, N_0), & N_0\nu^2 \equiv uv \pmod q, \end{cases} \tag{18}$$

je nachdem sich ν aus der ersten oder zweiten Kongruenz finden läßt[8]).

Offenbar ist

$$f(\varepsilon^{-\nu}) = f(\varepsilon^\nu), \quad g(\varepsilon^{-\nu}, N_0) = g(\varepsilon^\nu, N_0). \tag{19}$$

Die unter (12) bis (18) aufgeführten Gleichungen setzen voraus, daß mindestens eine der Zahlen u, v zu q teilerfremd ist. Wenn u und v mit q einen Teiler gemeinsam haben, sind Reduktionen der $S(u, v; q)$ möglich, die jedoch nur für $q = p^m$, $m \geqq 1$ durchgeführt werden sollen.

§ 2.

In diesem Abschnitt ist beständig

$$q = p^m, \quad m \geqq 2, \quad p \text{ Primzahl}. \tag{20}$$

Die Zahlen

$$0 < h \leqq q, \quad (h, q) = 1$$

stimmen überein mit den Zahlen

$$h = l + rp^{m-1}, \quad \begin{matrix} r = 0, 1, 2, \ldots, p-1, \\ l = 1, 2, 3, \ldots, p^{m-1}-1, \end{matrix} \quad l \not\equiv 0 \pmod p;$$

[8]) Im allgemeinen nur bei passend gewähltem N_0.

zu denen

$$\bar{h} \equiv \bar{l} - r\bar{l}^2 p^{m-1} \pmod{q}, \qquad m \geqq 2$$

gehören, wie man durch $h\bar{h} \equiv 1 \pmod{q}$ bestätigt.

Hierdurch läßt sich (3) in der Form

$$S(u, v; q) = \sum_{\substack{0<l<p^{m-1} \\ l \not\equiv 0 \pmod{p}}} \varepsilon^{ul+v\bar{l}} \cdot \sum_{r=0}^{p-1} e^{\frac{2\pi i}{p}(u-v\bar{l}^2)r} \tag{21}$$

schreiben.

Die Summe über r ist stets Null, wenn $u \equiv 0 \pmod{p}$ und $v \not\equiv 0 \pmod{p}$ ist, also auch

$$S(u, v; q) = 0 \text{ [9]}, \qquad u \equiv 0 \pmod{p}, \qquad v \not\equiv 0 \pmod{p}, \tag{22}$$

und wegen (11) (oder direkt aus (21))

$$S(u, v; q) = 0, \qquad u \not\equiv 0 \pmod{p}, \qquad v \equiv 0 \pmod{p}. \tag{22a}$$

Sind u und v beide durch p teilbar, so ist nach Gl. (21)

$$S(u, v; q) = p \sum_{\substack{0<l<p^{m-1} \\ l \not\equiv 0 \pmod{p}}} \varepsilon^{ul+v\bar{l}} = pS\left(\frac{u}{p}, \frac{v}{p}; \frac{q}{p}\right),$$

oder durch wiederholte Anwendung dieser Beziehung:

$$S(u, v; q) = p^k S\left(\frac{u}{p^k}, \frac{v}{p^k}; p^{m-k}\right) \text{ [10]}, \qquad \begin{matrix} u \equiv 0 \pmod{p^k}, \\ v \equiv 0 \pmod{p^k}, \\ 1 \leqq k < m \end{matrix} \tag{23}$$

und

$$S(u, v; q) = p^m - p^{m-1}, \qquad u \equiv v \equiv 0 \pmod{q}. \tag{23a}$$

Es zerfallen die zu

$$u \not\equiv 0 \pmod{p}, \qquad v \not\equiv 0 \pmod{p}$$

gehörigen $S(u, v; q)$ nach (18) für $p > 2$ in $\frac{1}{2}\varphi(q)$ Funktionen $f(\varepsilon^\nu)$ und $\frac{1}{2}\varphi(q)$ Funktionen $g(\varepsilon^\nu, N_0)$, wobei

$$\nu \not\equiv 0 \pmod{p}, \qquad 1 \leqq \nu \leqq \frac{q-1}{2}$$

genommen werden kann, da (19) gilt. N_0 sei ein fester Nichtrest $\not\equiv 0 \pmod{p}$. Bei Übergang zu einem anderen Nichtrest $N_0' \not\equiv 0 \pmod{p}$ ergeben sich dieselben Funktionen $g(\varepsilon^\nu, N_0)$ abgesehen von der Reihenfolge.

Nach (21) ist

$$g(\varepsilon^\nu, N_0) = \sum_{\substack{0<l<p^{m-1} \\ l \not\equiv 0 \pmod{p}}} \varepsilon^{\nu(l+N_0\bar{l})} \cdot \sum_{r=0}^{p-1} e^{\frac{2\pi i}{p} r(1-N_0\bar{l}^2)\nu} \tag{24}$$

---

[9]) E., S. 89.

[10]) E., S. 90.

und

$$f(\varepsilon^\nu) = \sum_{\substack{0<l<p^{m-1}\\ l\not\equiv 0 \,(\mathrm{mod}\, p)}} \varepsilon^{\nu(l+\bar{l})} \sum_{r=0}^{p-1} e^{\frac{2\pi i}{p} r(1-\bar{l}^2)\nu} \tag{25}$$

oder, nach Auswertung der Summen über r:

$$g(\varepsilon^\nu, N_0) = 0, \quad p>2, \quad m \geqq 2, \tag{26}$$

$$f(\varepsilon^\nu) = p \sum_{\substack{0<l<p^{m-1}\\ l\equiv \pm 1 \,(\mathrm{mod}\, p)}} \varepsilon^{\nu(l+\bar{l})}, \quad p>2, \quad m \geqq 2. \tag{27}$$

(27) ist nur der Spezialfall $\tau = 1$ der folgenden Gleichung

$$f(\varepsilon^\nu) = p^\tau \sum_{\substack{0<h<p^{m-\tau}\\ h\equiv \pm 1 \,(\mathrm{mod}\, p^\tau)}} \varepsilon^{\nu(h+\bar{h})}, \quad m \geqq 2\tau, \quad p>2, \tag{28}$$

die durch Induktionsschluß von τ auf $\tau+1$ für alle τ als gültig erwiesen wird.

Wenn nämlich $m \geqq 2\tau+2$ ist, darf man in (28) die durch

$$0 < h < p^{m-\tau}, \quad h \equiv \pm 1 \,(\mathrm{mod}\, p^\tau)$$

gekennzeichneten Zahlen aufspalten in:

$$h = l + r p^{m-\tau-1}, \quad \begin{matrix} l = 1, \ldots, p^{m-\tau-1}-1, \\ r = 0, 1, 2, \ldots, p-1, \end{matrix} \quad l \equiv \pm 1 \,(\mathrm{mod}\, p^\tau) \tag{29}$$

und $\bar{h}$ in der Form schreiben:

$$\bar{h} \equiv \bar{l} - r\bar{l}^2 p^{m-\tau-1}.$$

Durch Einsetzen von (29) in (28) entsteht:

$$f(\varepsilon^\nu) = p^\tau \sum_{\substack{0<l<p^{m-\tau-1}\\ l\equiv \pm 1 \,(\mathrm{mod}\, p^\tau)}} \varepsilon^{\nu(l+\bar{l})} \cdot \sum_{r=0}^{p-1} \varepsilon^{\nu(1-\bar{l}^2)p^{m-\tau-1}r}, \quad m \geqq 2(\tau+1) \tag{30}$$

oder unter Beachtung von

$$\sum_{\substack{r=0\\ l\equiv \pm 1 \,(\mathrm{mod}\, p^\tau)}}^{p-1} \varepsilon^{\nu(1-\bar{l}^2)p^{m-\tau-1}r} = \begin{cases} p, & l \equiv \pm 1 \,(\mathrm{mod}\, p^{\tau+1}), \\ 0 & \text{sonst,} \end{cases}$$

$$f(\varepsilon^\nu) = p^{\tau+1} \sum_{\substack{<l<p^{m-\tau-1}\\ l\equiv \pm 1 \,(\mathrm{mod}\, p^{\tau+1})}} \varepsilon^{\nu(l+\bar{l})}, \quad m \geqq 2(\tau+1), \quad p>2, \tag{31}$$

wodurch (28) bewiesen ist.

Für gerades m ergibt $\tau = \frac{m}{2}$ in (28) eingesetzt, wegen $h = 1$, $p^{\frac{m}{2}} - 1$ mit $\bar{h} \equiv 1$, $-p^{\frac{m}{2}} - 1 \pmod q$

$$(32) \qquad f(\varepsilon^\nu) = p^{\frac{m}{2}}(\varepsilon^{2\nu} + \varepsilon^{-2\nu}) \qquad p > 2, \quad m \equiv 0 \pmod 2$$
$$= 2\sqrt{q}\cos\frac{4\pi\nu}{q}. \qquad \nu \not\equiv 0 \pmod p.$$

Entsprechend entsteht bei ungeradem m für $\tau = \frac{m-1}{2}$ mit $h = \pm 1 + rp^{\frac{m-1}{2}}$ und $\bar{h} \equiv \pm 1 - rp^{\frac{m-1}{2}} \pm r^2 p^{m-1} \pmod q$ — $r \to$ volles Restsystem $\bmod p$ —

$$f(\varepsilon^\nu) = p^{\frac{m-1}{2}}\left[\varepsilon^{2\nu}\sum_{r=0}^{p-1} e^{\frac{2\pi i}{p}\nu r^2} + \varepsilon^{-2\nu}\sum_{r=0}^{p-1} e^{-\frac{2\pi i}{p}\nu r^2}\right]$$
$$= \left(\frac{\nu}{p}\right) p^{\frac{m-1}{2}}\sqrt{(-1)^{\frac{p-1}{2}} p}\left(\varepsilon^{2\nu} + (-1)^{\frac{p-1}{2}}\varepsilon^{-2\nu}\right),$$

d. h. es ist für $m \equiv 1 \pmod 2$, $p > 2$

$$(33) \qquad f(\varepsilon^\nu) = \begin{cases} 2\left(\frac{\nu}{q}\right)\sqrt{q}\cos\frac{4\pi\nu}{q}, & p \equiv 1 \pmod 4 \\ -2\left(\frac{\nu}{q}\right)\sqrt{q}\sin\frac{4\pi\nu}{q}, & p \equiv 3 \pmod 4. \end{cases}$$

Zusammenfassend läßt sich sagen, daß im Falle

$$q = p^m, \quad p \geqq 3, \quad \text{Primzahl}, \quad m \geqq 2$$

nur die $S(u, v; q)$ von Null verschieden sind, für die entweder

$$u \equiv 0 \pmod q, \quad v \equiv 0 \pmod q \quad \text{(vgl. (24a))},$$

oder

$$(u, q) = (v, q) \not\equiv p^{m-1}\ ^{11}),$$

$$\frac{u}{(u, q)} \not\equiv 0 \left(\bmod \frac{q}{(u, q)}\right), \quad \frac{v}{(u, q)} \not\equiv 0 \left(\bmod \frac{q}{(v, q)}\right),$$

$$\frac{uv}{(uv, q)} \text{ quadratischer Rest } \bmod \frac{q}{(u, q)}$$

ist. Hinsichtlich der Größenordnung gilt für alle $S(u, v; q)$:

$$|S(u, v; q)| < 2q^{\frac{1}{2}}(u, q)^{\frac{1}{2}}, \quad (u, v, q) \not\equiv p^{m-1}.$$

---

[11]) Für $(u, q) = (v, q) = p^{m-1}$ ist $S(u, v; q) = p^{m-1} S\left(\frac{u}{p^{m-1}}, \frac{v}{p^{m-1}}; p\right)$.

§ 3.

Der Fall $q = 2^m$ erfordert besondere Behandlung:

$$(34)\qquad \begin{aligned} m &= 1 \quad S(u, v; q) = (-1)^{u+v}, \\ m &= 2 \quad S(u, v; q) = i^{u+v} + i^{-(u+v)}. \end{aligned}$$

Für $m \geqq 3$ gibt es $\frac{1}{4}\varphi(q) = 2^{m-3}$ Funktionen $f(\varepsilon^\nu)$ und $\frac{3}{4}\varphi(q) = 3 \cdot 2^{m-3}$ Funktionen $g(\varepsilon^\nu, N_0)$. Sobald $m \geqq 6$ ist, sind auch hier alle

$$(35)\qquad g(\varepsilon^\nu, N_0) = 0.$$

Beweis. Ist

$$(36)\qquad h = k + 2^{m-\lambda}, \quad m \geqq 2\lambda, \quad \lambda \geqq 0 \text{ ganz}, \quad k \text{ ungerade},$$

so folgt

$$\bar{h} \equiv \bar{k} - \bar{k}^2 2^{m-\lambda} \pmod{q},$$

oder, falls $\lambda = 1, 2, 3$ genommen wird:

$$\bar{h} \equiv \bar{k} - 2^{m-\lambda} \pmod{q} \qquad (\lambda = 1, 2, 3),$$

da $\bar{k}^2 \equiv 1 \pmod 8$ ist.

Setzt man nun (36) mit $\lambda = 1$ in

$$(37)\qquad S(1, \mu; 2^m) = \sum_{\substack{1 \leqq h < 2^m \\ h \equiv 1 \,(\mathrm{mod}\, 2)}} \varepsilon^{h+\mu\bar{h}}, \quad \mu \text{ beliebig, ganz},$$

ein, so entsteht

$$(38)\qquad S(1, \mu; 2^m) = (1 + (-1)^{\mu+1}) \sum_{\substack{1 \leqq h < 2^{m-1} \\ h \equiv 1 \,(\mathrm{mod}\, 2)}} \varepsilon^{h+\mu\bar{h}}, \quad m \geqq 2.$$

Für gerade μ ist $S(1, \mu; 2^m) = 0$, $m \geqq 2$, was oben schon § 2 zu entnehmen ist. Sei nunmehr μ ungerade. Wendet man (36) jetzt mit $\lambda = 2$ auf (38) an, so wird:

$$(39)\qquad S(1, \mu; 2^m) = 2(1 + i^{1-\mu}) \sum_{\substack{1 \leqq h < 2^{m-2} \\ h \equiv 1 \,(\mathrm{mod}\, 2)}} \varepsilon^{h+\mu\bar{h}}, \quad m \geqq 4,$$

woraus

$$(39a)\qquad S(1, \mu; 2^m) = 0, \quad \mu \equiv 3 \pmod 4, \quad m \geqq 4$$

hervorgeht.

Schließlich werde für $\mu = 4\alpha + 1$ in (39) die Substitution (36) mit $\lambda = 3$ eingeführt, um

$$(40)\quad S(1, \mu; 2^m) = 4\left(1 + (-1)^{\frac{\mu-1}{4}}\right) \sum_{\substack{1 \leqq h < 2^{m-3} \\ h \equiv 1 \,(\mathrm{mod}\, 2)}} \varepsilon^{h+\mu\bar{h}}, \quad m \geqq 6, \quad \mu \equiv 1 \pmod 4$$

zu erhalten, d. h.

$$S(1, \mu; 2^m) = 0, \qquad \mu \equiv 5 \pmod 8, \quad m \geqq 6, \tag{40a}$$

$$S(1, \mu; 2^m) = 8 \sum_{\substack{1 \leqq h < 2^{m-2} \\ h \equiv 1 \pmod 2}} \varepsilon^{h+\mu\bar{h}}, \qquad \mu \equiv 1 \pmod 8, \quad m \geqq 6. \tag{40b}$$

Durch (39a) und (40a) ist (35) bewiesen. Aus (18) und (40b) folgt:

$$f(\varepsilon^\nu) = 8 \sum_{\substack{0 < h < 2^{m-2} \\ h \equiv 1 \pmod 2}} \varepsilon^{\nu(h+\bar{h})}, \qquad m \geqq 6, \quad \nu \equiv 1 \pmod 2. \tag{41}$$

Für die weitere Berechnung von $f(\varepsilon^\nu)$ brauche ich den folgenden

Hilfssatz. Ist

$$m \geqq 2\tau, \quad h = 2^{m-\tau} - k, \quad k^2 \equiv 1 \pmod{2^{\tau-1}}, \tag{42}$$

so ist

$$\bar{h} \equiv -2^{m-\tau} - \bar{k} + \varrho_k 2^{m-1} \pmod{2^m}, \tag{42a}$$

wobei

$$\varrho_k = \begin{cases} 0 & \text{für } k^2 \equiv 1 \pmod{2^\tau} \\ 1 & \text{sonst} \end{cases}$$

ist.

Beweis. Es ist

$$\begin{aligned} h\bar{h} &\equiv -2^{2m-2\tau} + 2^{m-\tau}(k - \bar{k}) + 1 + \varrho_k 2^{2m-\tau-1} - k\varrho_k 2^{m-1} \\ &\equiv 1 + 2^{m-\tau}(k - \bar{k}) - \varrho_k \cdot 2^{m-1}, \end{aligned}$$

da $m \geqq 2\tau$ und $k \equiv 1 \pmod 2$ ist.

Nun folgt aus $k^2 \equiv 1 \pmod{2^{\tau-1}}$

$$k - \bar{k} \equiv \varrho_k 2^{\tau-1} \pmod{2^\tau},$$

so daß also $h \cdot \bar{h} \equiv 1 \pmod{2^m}$ und damit der Ausdruck (42a) als richtig nachgewiesen ist.

Wird der obige Hilfssatz mit $\tau = 3$ für alle ungeraden h

$$2^{m-4} < h < 2^{m-3}$$

angewendet (ϱ_k ist dann stets Null) und in (41) verwertet, so entsteht:

$$f(\varepsilon^\nu) = 8 \sum_{\substack{0 < h < 2^{m-4} \\ h \equiv \pm 1 \pmod 4}} (\varepsilon^{\nu(h+\bar{h})} + \varepsilon^{-\nu(h+\bar{h})}), \qquad m \geqq 6 \tag{43}$$

oder, wenn jetzt $\tau = 4$ bedeutet:

$$f(\varepsilon^\nu) = 2^{\tau-1} \sum_{\substack{0 < h < 2^{m-\tau} \\ h \equiv \pm 1 \pmod{2^{\tau-2}}}} (\varepsilon^{\nu(h+\bar{h})} + \varepsilon^{-\nu(h+\bar{h})}), \qquad m \geqq 2(\tau - 1). \tag{44}$$

Ich zeige durch vollständige Induktion, daß (44) für alle τ, $4 \leqq \tau \leqq \frac{m}{2} + 1$ gilt.

In der zweiten Summe der aus (44) folgenden Gleichung

$$(44a)\qquad f(\varepsilon^\nu)=2^{\tau-1}\sum_{\substack{0<h\leqq 2^{m-\tau-1}\\ h\equiv\pm 1\,(\mathrm{mod}\,2^{\tau-2})}}{}'(\varepsilon^{\nu(h+\bar h)}+\varepsilon^{-\nu(h+\bar h)})$$
$$+2^{\tau-1}\sum_{\substack{2^{m-\tau-1}<h<2^{m-\tau}\\ h\equiv\pm 1\,(\mathrm{mod}\,2^{\tau-2})}}{}'(\varepsilon^{\nu(h+\bar h)}+\varepsilon^{-\nu(h+\bar h)})$$

werde unter der Voraussetzung $m\geqq 2\tau$ (42) eingeführt, so daß

$$(45)\qquad f(\varepsilon^\nu)=2^{\tau-1}\sum_{\substack{0<h<2^{m-\tau-1}\\ h\equiv\pm 1\,(\mathrm{mod}\,2^{\tau-2})}}{}'[\varepsilon^{\nu(h+\bar h)}+\varepsilon^{-\nu(h+\bar h)}+$$
$$+(-1)^{\varrho_h}(\varepsilon^{\nu(h+\bar h)}+\varepsilon^{-\nu(h+\bar h)})],\qquad m\geqq 2\tau$$

wird, oder unter Benutzung der Bedeutung der ϱ_h

$$(46)\qquad f(\varepsilon^\nu)=2^{\tau}\sum_{\substack{0<h<2^{m-\tau-1}\\ h\equiv\pm 1\,(\mathrm{mod}\,2^{\tau-1})}}{}'(\varepsilon^{\nu(h+\bar h)}+\varepsilon^{-\nu(h+\bar h)}),\qquad m\geqq 2\tau$$

eine Gleichung, die aus (44) durch Übergang von τ auf $\tau+1$ zu erhalten ist. Die Angabe der endgültigen Formeln für $f(\varepsilon^\nu)$ aus (46) macht nun keine Schwierigkeiten mehr:

a) m gerade, $\tau=\frac{m}{2}$, es ist $h=1$ und $h=2^{\frac{m}{2}-1}-1$, wozu $\bar h\equiv 1$ bzw. $\bar h\equiv -2^{m-2}-2^{\frac{m}{2}-1}-1$ gehören;

$$(47)\quad f(\varepsilon^\nu)=2^{\frac{m}{2}}(\varepsilon^{2\nu}+\varepsilon^{-2\nu}+\varepsilon^{2\nu+2^{m-2}\nu}+\varepsilon^{-2\nu-2^{m-2}\nu})$$
$$=2\sqrt{2q}\cos\Big(\frac{\pi}{4}+(-1)^{\frac{\nu-1}{2}}\frac{4\pi\nu}{q}\Big),\qquad \begin{matrix} m\geqq 6,\ \nu\equiv 1 \bmod 2,\\ m\equiv 0 \bmod 2.\end{matrix}$$

b) m ungerade, $\tau=\frac{m-1}{2}$, $m\geqq 9$

$$h=1,\quad 2^{\frac{m-3}{2}}-1,\quad 2^{\frac{m-3}{2}}+1,\quad 2^{\frac{m-1}{2}}-1$$
$$\bar h\equiv 1,\quad -2^{m-3}-2^{\frac{m-3}{2}}-1,\quad 2^{m-3}-2^{\frac{m-3}{2}}+1,\quad -2^{m-1}-2^{\frac{m-1}{2}}-1,$$

$$(48)\quad f(\varepsilon^\nu)=2^{\frac{m-1}{2}}(\varepsilon^{2\nu}+\varepsilon^{-2\nu}+2\varepsilon^{2\nu+2^{m-2}\nu}+2\varepsilon^{-2\nu-2^{m-2}\nu}$$
$$+\varepsilon^{2\nu+2^{m-1}\nu}+\varepsilon^{-2\nu-2^{m-1}\nu})$$
$$=2\sqrt{2q}\cos\Big(\frac{4\pi\nu}{q}+\frac{\pi\nu}{4}\Big),\quad \nu\equiv 1\,(\mathrm{mod}\,2),\ m\equiv 1\,(\mathrm{mod}\,2),\ m\geqq 9$$
$$=2(-1)^{\frac{\nu^2-1}{8}}\sqrt{2q}\cos\Big(\frac{\pi}{4}+(-1)^{\frac{\nu-1}{2}}\frac{4\pi\nu}{q}\Big).$$

Von den noch fehlenden $f(\varepsilon^\nu)$ stellt man leicht fest:

$$m = 3, \quad f(\varepsilon^\nu) = 0$$
$$m = 4, \quad f(\varepsilon^\nu) = 4\left(\frac{\nu}{-1}\right)^{\frac{\nu^2-1}{8}}\sqrt{2}$$
$$m = 5, \quad f(\varepsilon^\nu) = 0$$
$$m = 7, \quad f(\varepsilon^\nu) = -32\cos\left(\frac{4\pi\nu}{2^7} + \frac{\pi\nu}{4}\right).$$

Es ist stets

$$|f(\varepsilon^\nu)| \leqq 2\sqrt{2q} \quad \text{für alle } q = 2^m. \tag{49}$$

§ 4.

Es sei q ungerade Primzahl. Zur Übersicht werden die möglichen Werte der $S(u, v; q)$ zusammengestellt:

$$(50)\quad \begin{cases} u \equiv 0, \ v \equiv 0, & S(u, v; q) = q - 1; \\ u \equiv 0, \ v \not\equiv 0, & S(u, v; q) = -1; \\ u \not\equiv 0, \ v \equiv 0, & S(u, v; q) = -1; \\ u \not\equiv 0, \ v \not\equiv 0, & S(u, v; q) = \begin{cases} f(\varepsilon^\nu), & \nu^2 \equiv uv \pmod q; \\ g(\varepsilon^\nu, N_0), & \nu^2 \equiv uv\bar{N}_0 \pmod q. \end{cases} \end{cases}$$

Da im folgenden der einmal gewählte Nichtrest N_0 beibehalten wird, soll $g(\varepsilon^\nu)$ statt $g(\varepsilon^\nu, N_0)$ geschrieben werden.

Mit Hilfe des Legendreschen Symbols

$$\left(\frac{a}{q}\right) = \left\{\begin{array}{ll} 0, & a \equiv 0 \pmod q, \\ 1, & a \text{ quadr. Rest} \\ -1, & a \text{ quadr. Nichtrest} \end{array}\right\} \bmod q$$

kann man (14) und (15) in die Form

$$f(\varepsilon^\nu) = \sum_{h=0}^{q-1}\left(\frac{h^2-4}{q}\right)\varepsilon^{\nu h}, \tag{51}$$

$$g(\varepsilon^\nu) = \sum_{h=0}^{q-1}\left(\frac{h^2-4N_0}{q}\right)\varepsilon^{\nu h} \tag{52}$$

bringen, da für jede eindeutige Funktion $F(x)$ mit der Periode q die Beziehung[12])

$$\lambda \not\equiv 0 \pmod q, \qquad \sum_{h=1}^{q-1} F(h + \lambda\bar{h}) = \sum_{h=0}^{q-1} F(h) + \sum_{h=0}^{q-1}\left(\frac{h^2-4\lambda}{q}\right)F(h) \tag{53}$$

[12]) E. Jacobsthal, a. a. O. [5]) S. 239.

gilt. Für $\nu \equiv 0 \pmod q$ soll

$$f(\varepsilon^\nu) = g(\varepsilon^\nu) = -1, \quad \nu \equiv 0 \pmod q \tag{52a}$$

festgesetzt werden in Übereinstimmung mit

$$\sum_{h=0}^{q-1}\left(\frac{h^2-4}{q}\right) = \sum_{h=0}^{q-1}\left(\frac{h^2-4N_0}{q}\right) = -1.$$

Die Beziehung (53) werde jetzt noch zweimal angewendet:

1. für $\lambda = 1$, $F(x) = \varepsilon^{\nu x^2}$ liefert sie

$$\varepsilon^{2\nu}\sum_{h=1}^{q-1}\varepsilon^{\nu(h^2+\bar h^2)} = \left(\frac{\nu}{q}\right)\sqrt{(-1)^{\frac{q-1}{2}}q} + \sum_{h=0}^{q-1}\left(\frac{h^2-4}{q}\right)\varepsilon^{\nu h^2}; \tag{53a}$$

2. für $\lambda = N_0$, $F(x) = \varepsilon^{\nu \bar N_0 x^2}$ liefert sie

$$\varepsilon^{2\nu}\sum_{h=1}^{q-1}\varepsilon^{\nu(\bar N_0 h^2 + N_0 \bar h^2)} = -\left(\frac{\nu}{q}\right)\sqrt{(-1)^{\frac{q-1}{2}}q} + \sum_{h=0}^{q-1}\left(\frac{h^2-4N_0}{q}\right)\varepsilon^{\nu \bar N_0 h^2}. \tag{53b}$$

Wegen

$$\sum_{h=0}^{q-1}\left(\frac{h^2-4}{q}\right)\varepsilon^{\nu h^2} - \sum_{h=0}^{q-1}\left(\frac{h^2-4N_0}{q}\right)\varepsilon^{\nu \bar N_0 h^2} = 2\sum_{k=0}^{q-1}\left(\frac{k-4}{q}\right)\varepsilon^{\nu k}$$

$$= 2\varepsilon^{4\nu}\left(\frac{\nu}{q}\right)\sqrt{(-1)^{\frac{q-1}{2}}q}$$

erhält man durch Subtraktion und Addition von (53a) und (53b)

$$\sum_{h=1}^{q-1}\left(\frac{h}{q}\right)\varepsilon^{(h+\bar h)\nu} = \left(\frac{\nu}{q}\right)\sqrt{(-1)^{\frac{q-1}{2}}q}\,(\varepsilon^{2\nu} + \varepsilon^{-2\nu}), \tag{54}$$

$$f(\varepsilon^\nu) = -\left(\frac{\nu}{q}\right)\varepsilon^{2\nu}\sqrt{(-1)^{\frac{q-1}{2}}q} + \varepsilon^{-2\nu}\sum_{h=0}^{q-1}\left(\frac{h^2-4}{q}\right)\varepsilon^{\nu h^2} \tag{55}$$

bzw.

$$f(\varepsilon^\nu) = \left(\frac{\nu}{q}\right)\varepsilon^{2\nu}\sqrt{(-1)^{\frac{q-1}{2}}q} + \varepsilon^{-2\nu}\sum_{h=0}^{q-1}\left(\frac{h^2-4N_0}{q}\right)\varepsilon^{\nu \bar N_0 h^2}. \tag{56}$$

Für $g(\varepsilon^\nu)$ bestehen keine genau entsprechenden Formeln:

$$\sum_{h=1}^{q-1}\left(\frac{h}{q}\right)\varepsilon^{(h+N_0\bar h)\nu} = 0; \tag{57}$$

denn die Summe links nimmt ihren negativen Wert an, wenn $h \equiv N_0 \bar k$ eingeführt wird. Aus (57) folgt:

$$g(\varepsilon^\nu) = \sum_{h=1}^{q-1}\varepsilon^{\nu(lh^2 + N_0\bar h^2 \bar l)}, \quad l \not\equiv 0 \pmod q. \tag{58}$$

Ist χ ein Charakter mod q, so ist

$$\sum_{\chi} \chi(lh) = \begin{cases} q-1, & lh \equiv 1 \pmod{q}, \\ 0 & \text{sonst} \end{cases}$$

woraus

$$\sum_{l=1}^{q-1} \varepsilon^{vl} \sum_{\chi} \chi(l)\,\chi(h) = (q-1)\,\varepsilon^{v\bar{h}}$$

und

$$S(u, v; q) = \frac{1}{q-1} \sum_{\chi} \sum_{h=1}^{q-1} \chi(h)\,\varepsilon^{uh} \cdot \sum_{h=1}^{q-1} \chi(h)\,\varepsilon^{vh} \tag{59}$$

folgt. Diese Form der Kloostermanschen Summen liefert für $u \equiv v \equiv \nu \pmod{q}$

$$f(\varepsilon^{\nu}) = \frac{1}{q-1} \sum_{\chi} \left(\sum_{h=1}^{q-1} \chi(h)\,\varepsilon^{\nu h} \right)^2, \qquad \nu \not\equiv 0 \pmod{q}. \tag{59a}$$

Hierin ist bekanntlich[13])

$$\left| \sum_{h=1}^{q-1} \chi(h)\,\varepsilon^{\nu h} \right| \leqq \sqrt{q}.$$

Das Auftreten von $\sqrt{(-1)^{\frac{q-1}{2}} q}$ in den verschiedenen Darstellungen legt die Bildung von $f(\varepsilon^{\nu})^2$ und $g(\varepsilon^{\nu})^2$ nahe.

Nach (58) ist:

$$\varepsilon^{\nu(l+N_0\bar{l})}\, g(\varepsilon^{\nu}) = \sum_{h=1}^{q-1} \varepsilon^{\nu(lh^2+N_0\bar{l}\bar{h}^2+l+N_0\bar{l})},$$

$$g(\varepsilon^{\nu})^2 = \sum_{h=1}^{q-1} \sum_{l=1}^{q-1} \varepsilon^{\nu(lh^2+N_0\bar{l}\bar{h}^2+l+N_0\bar{l})},$$

und, wenn $l \equiv k\bar{h}$ eingeführt wird,

$$g(\varepsilon^{\nu})^2 = \sum_{h=1}^{q-1} \sum_{k=1}^{q-1} \varepsilon^{\nu(h+\bar{h})(k+N_0\bar{k})},$$

also

$$g(\varepsilon^{\nu})^2 = \left(1 + (-1)^{\frac{q-1}{2}}\right) q + \sum_{h=1}^{q-1} g(\varepsilon^{\nu(h+\bar{h})}), \qquad \nu \not\equiv 0 \pmod{q} \tag{60}$$

und

$$g(\varepsilon^{\nu})^2 = \left(1 - (-1)^{\frac{q-1}{2}}\right) q + \sum_{h=1}^{q-1} f(\varepsilon^{\nu(h+N_0\bar{h})}), \qquad \nu \not\equiv 0 \pmod{q} \tag{60a}$$

unter Berücksichtigung der Festsetzung (52a).

---

[13]) E. Landau, Vorlesungen über Zahlentheorie (Leipzig 1927), Bd. I, S. 189.

Schließlich ist nach (53)

$$(61)\qquad g(\varepsilon^\nu)^2 = q + \sum_{h=0}^{q-1}\left(\frac{h^2-4}{q}\right) g(\varepsilon^{\nu h}) = q + \sum_{h=0}^{q-1}\left(\frac{h^2-4N_0}{q}\right) f(\varepsilon^{\nu h}),$$

$$\nu \not\equiv 0 \pmod q,$$

wenn man

$$(62)\qquad \sum_{\nu=0}^{q-1} f(\varepsilon^\nu) = -\sum_{\nu=0}^{q-1} g(\varepsilon^\nu) = (-1)^{\frac{q-1}{2}} q$$

beachtet.

Ähnlich beweist man:

$$(63)\quad f(\varepsilon^\nu)^2 = \left(1+(-1)^{\frac{q-1}{2}}\right) q - (-1)^{\frac{q-1}{2}} q\,(\varepsilon^{2\nu}+\varepsilon^{-2\nu})^2 + \sum_{h=0}^{q-1} f(\varepsilon^{\nu(h+\bar{h})})$$

$$= \left(1-(-1)^{\frac{q-1}{2}}\right) q + (-1)^{\frac{q-1}{2}} q\,(\varepsilon^{2\nu}+\varepsilon^{-2\nu})^2 + \sum_{h=0}^{q-1} g(\varepsilon^{\nu(h+\bar{N}_0\bar{h})})$$

und

$$(63\text{a})\quad f(\varepsilon^\nu)^2 = q - (-1)^{\frac{q-1}{2}} q\,(\varepsilon^{4\nu}+\varepsilon^{-4\nu}) + \sum_{h=0}^{q-1}\left(\frac{h^2-4}{q}\right) f(\varepsilon^{\nu h})$$

$$= q + (-1)^{\frac{q-1}{2}} q\,(\varepsilon^{4\nu}+\varepsilon^{-4\nu}) + \sum_{h=0}^{q-1}\left(\frac{h^2-4\bar{N}_0}{q}\right) g(\varepsilon^{\nu h}).$$

An den gegebenen Darstellungen für $f(\varepsilon^\nu)^2$ und $g(\varepsilon^\nu)^2$ ist bemerkenswert, daß sie sich wieder in gewissen $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu)$ ausdrücken.

§ 5.

Da[14])

$$(64)\qquad \operatorname{Max} S(1,\lambda;q)^2 = \lim_{n\to\infty} \sqrt[n]{\sum_{\lambda=0}^{q-1} S(1,\lambda;q)^{2n}}$$

ist, kann die Ermittlung der genauen Größenordnung der $S(u,v;q)$ in q, die für q als ungerade Primzahl noch aussteht, auf die Bestimmung der Potenzsummen der $S(u,v;q)$ zurückgeführt werden.

Um zu einem Ausdruck für

$$\sum_{\lambda=0}^{q-1} S(1,\lambda;q)^n = \frac{1}{2}\sum_{\nu=0}^{q-1} f(\varepsilon^\nu)^n + \frac{1}{2}\sum_{\nu=0}^{q-1} g(\varepsilon^\nu)^n$$

[14]) Pólya-Szegö, Aufgaben und Lehrsätze aus der Analysis (Berlin 1925), Bd. I, S. 77, Nr. 195.

zu gelangen, setze man in

$$\sum_{\lambda=0}^{q-1} \varepsilon^{-\lambda k} S(1, \lambda; q) = q\,\varepsilon^{\bar{k}}, \qquad k \not\equiv 0 \pmod q$$

ein:

$$k \equiv -(k_1 + k_2 + \ldots + k_{n-1}) \pmod q, \qquad n \geqq 2, \qquad 1 \leqq k_\nu \leqq q-1$$
$$(\nu = 1, 2, \ldots, n-1),$$

multipliziere mit $\varepsilon^{\bar{k}_1+\bar{k}_2+\ldots+\bar{k}_{n-1}}$ und summiere über alle k_ν. Es entsteht:

$$\sum_{\lambda=0}^{q-1} S(1, \lambda; q)^n = q \sum_{k_1, k_2, \ldots, k_{n-1}}^{1,2,\ldots,q-1} \varepsilon^{\bar{k}_1+\bar{k}_2+\ldots+\bar{k}_{n-1}-\overline{(k_1+k_2+\ldots+k_{n-1})}}$$

$$= q \sum_{\nu=1}^{q-1} \sum_{\substack{k_1, k_2, \ldots, k_{n-1} \\ k_1+k_2+\ldots+k_{n-1} \equiv \nu \pmod q}} \varepsilon^{\bar{k}_1+\bar{k}_2+\ldots+\bar{k}_{n-1}-\bar{\nu}}$$

$$= q \sum_{r=1}^{q-1} \sum_{\substack{l_1, l_2, \ldots, l_{n-1} \\ l_1+l_2+\ldots+l_{n-1} \equiv 1 \pmod q}} \varepsilon^{\bar{r}(\bar{l}_1+\bar{l}_2+\ldots+\bar{l}_{n-1}-1)},$$

falls $k_r \equiv r\,l_r \pmod q$ $(r = 1, 2, \ldots, n-1)$ gesetzt wird.

Nach Ausführung der Summation über r ergibt sich:

$$\sum_{\lambda=0}^{q-1} S(1, \lambda; q)^n = q(q-1)\,M_{n-1} - q\,M_{n-1}^*, \tag{65}$$

wobei M_{n-1} die Anzahl der Lösungen $1 \leqq l_r \leqq q-1$ $(r = 1, 2, \ldots, n-1)$ von

$$\left| \begin{matrix} l_1 + l_2 + \ldots + l_{n-1} \equiv 1 \\ \bar{l}_1 + \bar{l}_2 + \ldots + \bar{l}_{n-1} \equiv 1 \end{matrix} \pmod q \right| \tag{66}$$

und M_{n-1}^* die Anzahl der Lösungen $1 \leqq l_r \leqq q-1$ $(r = 1, 2, \ldots, n-1)$ von

$$\left| \begin{matrix} l_1 + l_2 + \ldots + l_{n-1} \equiv 1 \\ \bar{l}_1 + \bar{l}_2 + \ldots + \bar{l}_{n-1} \not\equiv 1 \end{matrix} \pmod q \right| \tag{67}$$

bezeichnet.

Durch eine leichte Abzählung findet man, daß

$$M_{n-1} + M_{n-1}^* = \frac{(q-1)^{n-1} - (-1)^{n-1}}{q} \tag{68}$$

ist als Anzahl der Zahlen $1 \leqq l_r \leqq q-1$ $(r = 1, 2, \ldots, n-1)$, für die

$$l_1 + l_2 + \ldots + l_{n-1} \equiv 1 \pmod q.$$

(65) geht durch (68) über in:

$$\sum_{\lambda=0}^{q-1} S(1, \lambda; q)^n = q^2 M_{n-1} - (q-1)^{n-1} + (-1)^{n-1} \qquad (n \geqq 2). \tag{69}$$

Für $n = 2, 3, 4$ gelingt die Bestimmung von M_{n-1} sehr leicht. Es ist

$$M_1 = 1,$$

$$M_2 = \begin{cases} 1, & q = 3, \\ 1 + \left(\frac{-3}{q}\right), & q > 3, \end{cases}$$

denn $\begin{vmatrix} l_1 + l_2 \equiv 1 \\ \bar{l}_1 + \bar{l}_2 \equiv 1 \end{vmatrix}$ ist für $q > 3$ nur im Falle $\left(\frac{-3}{q}\right) = +1$ lösbar.

Bei festem $l_3 \not\equiv 1$ hat (66) für $n = 4$ die Lösungen

$$\text{und} \qquad \begin{matrix} l_1 \equiv 1, & l_2 \equiv -l_3 \\ l_1 \equiv -l_3, & l_2 \equiv 1 \end{matrix} \pmod q.$$

Die beiden Lösungspaare fallen nur für $l_3 \equiv q - 1$ zusammen. Ist $l_3 \equiv 1$, so sind $(q-1)$ Lösungspaare

$$l_1 \equiv l, \qquad l_2 \equiv -l \qquad (l = 1, 2, \ldots, q-1)$$

vorhanden. Somit ist

$$M_3 = 2(q-3) + 1 + (q-1) = 3(q-2)$$

und[15])

$$(70) \qquad \begin{cases} \sum_{\lambda=0}^{q-1} S(1, \lambda; q)^2 = q^2 - q. \\ \sum_{\lambda=0}^{q-1} S(1, \lambda; q)^3 = \left(\frac{-3}{q}\right) q^2 + 2q, \\ \sum_{\lambda=0}^{q-1} S(1, \lambda; q)^4 = 2q^3 - 3q^2 - 3q. \end{cases}$$

Der Limes (64) ist hinsichtlich seines Verhaltens für große q bis jetzt nicht bekannt. (70) liefert jedoch, da

$$\left(\frac{\sum_{\lambda=0}^{q-1} S(1, \lambda; q)^{2n}}{q} \right)^{\frac{1}{n}}$$

eine monoton wachsende Funktion von n ist[16]),

$$(71) \qquad \sum_{\lambda=0}^{q-1} S(1, \lambda; q)^{2n} > 2^{\frac{n}{2}} (q-1)^{n+1},\ ^{17})$$

und außerdem

$$(72) \qquad |S(1, \lambda; q)| < \sqrt[4]{\sum_{\lambda=0}^{q-1} S(1, \lambda; q)^4} < 2^{\frac{1}{4}} q^{\frac{3}{4}},$$

---

[15]) Bei E., S. 89 findet sich nur $\sum_{\substack{0 < w \leqq q \\ (w, q) = 1}} |S(1, w; q)|^4 \leqq 8q^3$ abgeschätzt.

[16]) a. a. O. [14]) S. 54, Nr. 82.

[17]) Vermutlich ist auch $\sum_{\lambda=0}^{q-1} S(1, \lambda; q)^{2n} < (Cq)^{n+1}$, wo C von q unabhängig ist.

eine Abschätzung, die sich nur in der Konstanten von der Abschätzung (8) des Herrn Estermann unterscheidet.

Zu einer zweiten Darstellung der Summen (69) gelangt man, wenn man die Gleichungen

$$(73)\qquad \sum_{\nu=0}^{q-1} f(\varepsilon^\nu)^n = q \sum_{\substack{0\leqq h_\nu<q\\ h_1+\ldots+h_n\equiv 0 \,(\mathrm{mod}\, q)}} \left(\frac{h_1^2-\alpha^2}{q}\right)\left(\frac{h_2^2-\alpha^2}{q}\right)\ldots\left(\frac{h_n^2-\alpha^2}{q}\right)$$

$$\alpha \not\equiv 0 \,(\mathrm{mod}\, q), \qquad n \geqq 1, \text{ ganz}$$

$$(74)\qquad \sum_{\nu=0}^{q-1} g(\varepsilon^\nu)^n = q \sum_{\substack{0\leqq h_\nu<q\\ h_1+\ldots+h_n\equiv 0 \,(\mathrm{mod}\, q)}} \left(\frac{h_1^2-\alpha^2 N_0}{q}\right)\left(\frac{h_2^2-\alpha^2 N_0}{q}\right)\ldots\left(\frac{h_n^2-\alpha^2 N_0}{q}\right),$$

die sich unmittelbar aus (51) und (52) mit $\alpha = 2$ ergeben — offenbar aber für alle $\alpha \not\equiv 0 \,(\mathrm{mod}\, q)$ gelten — zu

$$(75)\qquad \sum_{\lambda=0}^{q-1} S(1, \lambda; q)^n = \frac{q}{q-1} \sum_{a=1}^{q-1} \sum_{\substack{0\leqq h_\nu<q\\ h_1+\ldots+h_n\equiv 0 \,(\mathrm{mod}\, q)}} \left(\frac{h_1^2+a}{q}\right)\left(\frac{h_2^2+a}{q}\right)\ldots\left(\frac{h_n^2+a}{q}\right)$$

zusammenzieht. $n = 2$ liefert in (73) und (74)

$$\sum_{\nu=0}^{q-1} f(\varepsilon^\nu)^2 = q^2 - 2q,$$

$$\sum_{\nu=0}^{q-1} g(\varepsilon^\nu)^2 = q^2,$$

woraus hervorgeht, daß in einer für alle ν gültigen asymptotischen Abschätzung

$$\left.\begin{matrix} f(\varepsilon^\nu) \\ g(\varepsilon^\nu) \end{matrix}\right\} = O(q^\beta),$$

$\beta \geqq \frac{1}{2}$ sein muß (nach (72) ist $\beta \leqq \frac{3}{4}$).

Es sollen im folgenden noch einige Summen, in denen $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu)$ auftreten, gebildet werden, die wie (73) und (74) Zusammenhänge mit Summen Legendrescher Symbole ergeben.

Man stellt leicht fest, daß z. B.

$$(76)\qquad \sum_{\nu=0}^{q-1} \left(\frac{\nu}{q}\right) \varepsilon^{k\nu} f(\varepsilon^\nu) = \sqrt{(-1)^{\frac{q-1}{2}} q} \sum_{h=0}^{q-1} \left(\frac{h^2-4}{q}\right)\left(\frac{h+k}{q}\right),$$

$$(77)\qquad \sum_{\nu=0}^{q-1} f(\varepsilon^\nu) f(\varepsilon^{\lambda\nu}) = q \sum_{h=0}^{q-1} \left(\frac{h^2-4}{q}\right)\left(\frac{h^2-4\lambda^2}{q}\right),$$

$$(78)\qquad \sum_{\nu=0}^{q-1} \varepsilon^{4\lambda\nu} f(\varepsilon^\nu)^2 = q \sum_{h=0}^{q-1} \left(\frac{h^2-4}{q}\right)\left(\frac{(h-4\lambda)^2-4}{q}\right).$$

Die drei Summen, deren asymptotisches Verhalten in q bei Fragen der Verteilung der quadratischen Reste eine Rolle spielt[18]), hängen untereinander einfach zusammen. Ihre wahre Größenordnung ist im allgemeinen noch nicht bekannt, dagegen ist sie im Spezialfall $k = 0$ in (76) durch Jacobsthal[19])

$$\left[\sum_{h=1}^{q-1}\left(\frac{h+\bar{h}}{q}\right)\right]^2+\left[\sum_{h=1}^{q-1}\left(\frac{h+N_0\bar{h}}{q}\right)\right]^2=\begin{cases}0, & q\equiv 3\,(\mathrm{mod}\,4)\\ 4q, & q\equiv 1\,(\mathrm{mod}\,4)\end{cases}$$

bestimmt, die der Beziehung

$$\left[\sum_{\nu=0}^{q-1}\left(\frac{\nu}{q}\right)f(\varepsilon^\nu)\right]^2+\left[\sum_{\nu=0}^{q-1}\left(\frac{\nu}{q}\right)g(\varepsilon^\nu)\right]^2=\begin{cases}0, & q\equiv 3\,(\mathrm{mod}\,4)\\ 4q^2, & q\equiv 1\,(\mathrm{mod}\,4)\end{cases}$$

entspricht. Auf weitere (Gleichungen (76) bis (78)) ähnliche Formeln, die sich in großer Zahl finden lassen, soll nicht eingegangen werden. Vielleicht kann für die Ermittlung der Größenordnung der Summen Legendrescher Symbole die Kenntnis des Zusammenhangs mit den Kloostermanschen Summen von Nutzen sein.

§ 6.

Zum Schluß sei noch darauf hingewiesen, daß $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu)$ primitive Zahlen des durch Adjunktion von $\varepsilon+\varepsilon^{-1}$ zum natürlichen Rationalitätsbereich $\mathfrak{R}$ erweiterten Körpers vom Grade $\frac{q-1}{2}$ sind, wenn q eine ungerade Primzahl ist. Es genügen also $f(\varepsilon^\nu)$ und $g(\varepsilon^\nu)$ je einer in $\mathfrak{R}$ irreduziblen Gleichung $\frac{q-1}{2}$-ten Grades.

Da nach einem bekannten Satz über zyklische Determinanten[20])

$$\prod_{\nu=0}^{q-1}(x-f(\varepsilon^\nu))=-\begin{vmatrix} a_0-x & a_1 & \dots & a_{q-1}\\ a_{q-1} & a_0-x & \dots & a_{q-2}\\ \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots\\ a_1 & a_2 & \dots & a_0-x\end{vmatrix},\qquad a_h=\left(\frac{h^2-4}{q}\right),$$

[18]) H. Hopf, a. a. O. [5]). Der Zusammenhang mit dem dortigen $\chi(c)$ wird etwa durch die Formel

$$\sum_{h=0}^{q-1}\left(\frac{h^2+a}{q}\right)\left(\frac{h^2+ca}{q}\right)=-1+\left(\frac{a}{q}\right)\sum_{h=0}^{q-1}\left(\frac{h}{q}\right)\left(\frac{h+1}{q}\right)\left(\frac{h+c}{q}\right),\qquad a\not\equiv 0\,(\mathrm{mod}\,q)$$

hergestellt.

[19]) a. a. O. [5]) S. 239—240.

[20]) G. Kowalewski, Einführung in die Determinantentheorie (Leipzig 1909), S. 116.

oder unter beiderseitiger Abspaltung des Faktors

$$x - f(\varepsilon^0) = x + 1 = -(a_0 + a_1 + \ldots + a_{q-1} - x):$$

$$F(x)^2 \equiv \left[\prod_{\nu=1}^{\frac{q-1}{2}} (x - f(\varepsilon^\nu))\right]^2 = \begin{vmatrix} 1 & a_1 & \ldots & a_{q-1} \\ 1 & a_0 - x & \ldots & a_{q-2} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & a_2 & \ldots & a_0 - x \end{vmatrix}$$

ist[21]), stellt

$$F(x) = 0$$

die irreduzible Gleichung dar, der die $f(\varepsilon^\nu)$ genügen.

Entsprechend findet man die irreduzible Gleichung für die $g(\varepsilon^\nu)$, wenn $a_h = \left(\frac{h^2 - 4N_0}{q}\right)$ bedeutet.

---

[21]) Nach dem Hadamardschen Determinantensatz ist übrigens

$$\prod_{\nu=1}^{\frac{q-1}{2}} |f(\varepsilon^\nu)| \leqq q^{\frac{q}{4}}.$$

(Eingegangen am 10. Januar 1931.)