

5. Proof completed

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

We shall employ a special case of the function (4.1) due to Jacobi. Let $p = ef + 1$ and β be a primitive e -th root of unity. In (4.1) take $\alpha = \beta^n$ (n -integer). We know ([3] page 395) that if e does not divide n then

$$(4.2) \quad F(\beta^n) F(\beta^{-n}) = (-1)^{nf} \cdot p$$

and if we put

$$(4.3) \quad R(n, m) = \frac{F(\beta^n) F(\beta^m)}{F(\beta^{m+n})},$$

then

$$(4.4) \quad R(n, m) = \sum_{h=0}^{e-1} \beta^{nh} \sum_{k=0}^{e-1} \beta^{-(m+n)k} (h, k).$$

From (4.2) and (4.3) it follows that if e does not divide m, n and $m + n$ then

$$(4.5) \quad R(n, m) R(-n, -m) = p$$

and from (4.4) it follows that $R(-n, -m)$ is got from $R(n, m)$ by replacing β by β^{-1} . Let now $e = 4$ and $\beta = \sqrt{-1}$; using (4.4) we get

$$R(1, 1) = (A - B - C - D + 2E) + i(2D - 2B) \text{ in case } p \equiv 1 \pmod{8}$$

$$R(1, 1) = (L - M - R - N + 2S) + i(2M - 2R) \text{ in case } p \equiv 5 \pmod{8}.$$

5. PROOF COMPLETED

If $p \equiv 1 \pmod{4}$ then p splits in $Z[i]$ as $p = \pi \bar{\pi}$ where π is prime in $Z[i]$.

Case 1: $p \equiv 1 \pmod{8}$.

$$\begin{aligned} \sum_{\text{all } v} \chi(v) \chi(v+1) &= \sum_{v \in A_0, A_1, A_2, A_3} \chi(v) \chi(v+1) = \sum_{A_0} + \sum_{A_1} + \sum_{A_2} + \sum_{A_3} \\ &= 1[A + Di - C - Bi] + i[D + Bi - E - Ei] \\ &\quad - 1[C + Ei - C - Ei] - i[B + Ei - E - Di] \\ &= [A - B - C - D + 2E] + i[2D - 2B] \\ (5.1) \quad &= R(1, 1) = (-2f + 8(1, 2) - 1) - 2i[D - B] \end{aligned}$$

where $R(1, 1) \equiv -1 \pmod{2(1+i)}$ (as $D - B = f - 2B - 2E$ by (3.5))

$$\begin{aligned} \text{and } \sum_{\text{all } v} \chi^2(v) \chi^2(v+1) &= (A - D + C - B) - (D - B + E - E) \\ &\quad + (C - E + C - E) - (B - E + E - D) \\ &= A + 3C - D - 2E - B = -1, \end{aligned}$$

by (3.4)

Therefore we have

$$S = \left(\frac{-a}{p}\right) [\chi(-4a) R(1, 1) + \bar{\chi}(-4a) \overline{R(1, 1)} + \chi^2(-4a)(-1)].$$

We put $\pi = -R(1, 1)$, then $\pi \equiv +1 \pmod{2(1+i)}$.

$$\text{Therefore } S = \left(\frac{-a}{p}\right) [-\chi(-4a)\pi - \bar{\chi}(-4a)\bar{\pi} - \chi^2(-4a)].$$

Let g be the primitive root mod p which we have already fixed in § 2. We now have two possibilities:

$$(i) \quad \left(\frac{g}{\pi}\right)_4 = i \quad \text{i.e.} \quad \left(\frac{d}{\pi}\right)_4 = \chi(d) \text{ for all } d.$$

$$(ii) \quad \left(\frac{g}{\pi}\right)_4 = -i \quad \text{i.e.} \quad \left(\frac{d}{\pi}\right)_4 = \bar{\chi}(d) \text{ for all } d.$$

Let $\chi(d) = \left(\frac{d}{\pi^*}\right)_4$ where $\pi^* = \pi$ or $\bar{\pi}$.

We shall show that $\pi^* = \pi$. We have

$$\begin{aligned} \pi &= -\sum \chi(v)\chi(v+1) \equiv -\sum_0^{p-1} v^{\frac{1}{4}(p-1)}(v+1)^{\frac{1}{4}(p-1)} \pmod{\pi^*} \\ &\equiv -[v^{\frac{1}{4}(p-1)}(1 + \frac{1}{4}(p-1)v + \dots + v^{\frac{1}{4}(p-1)})] \pmod{\pi^*}. \end{aligned}$$

In the last sum each term is divisible by $p = \pi\bar{\pi}$, because we know that $\sum_v v^k \equiv 0 \pmod{p}$ unless $p-1/k$. Hence the right hand side of the above is congruent to zero mod π^* . Hence $\pi \equiv 0 \pmod{\pi^*}$ giving $\pi = \pi^*$.

Therefore

$$\begin{aligned} S &= -\left(\frac{-a}{p}\right)\left(\frac{-4a}{\pi}\right)_4 \pi - \left(\frac{-a}{p}\right)\left(\frac{-4a}{\bar{\pi}}\right)_4 \bar{\pi} - \left(\frac{-a}{p}\right)\left(\frac{-4a}{\pi}\right)_4^2 \\ &= -\left(\frac{-4a}{\pi}\right)_4^3 \pi - \left(\frac{-4a}{\bar{\pi}}\right)_4^3 \bar{\pi} - 1 = -\left(\frac{a}{\pi}\right)_4^3 \pi - \left(\frac{a}{\bar{\pi}}\right)_4^3 \bar{\pi} - 1 \\ &= -\left(\frac{a}{\pi}\right)_4 \pi - \left(\frac{a}{\bar{\pi}}\right)_4 \bar{\pi} - 1, \end{aligned}$$

using (i) $\left(\frac{d}{p}\right) = \left(\frac{d}{\pi}\right)_4^2 = \left(\frac{d}{\bar{\pi}}\right)_4^2$

(ii) $\left(\frac{d}{\pi}\right)_4^3 = \left(\frac{d}{\bar{\pi}}\right)_4$

(iii) $\left(\frac{-4}{\pi}\right)_4 = \left(\frac{-4}{\bar{\pi}}\right)_4 = 1$ since $-4 = (1+i)^4$ — a fourth power.

This gives the required value of S .

Case 2: $p \equiv 5 \pmod{8}$. In this case as before

$$\begin{aligned} \sum \chi(v) \chi(v+1) &= [N - L + R + M - 2S] + i[2R - 2M] \\ &= -R(1, 1) \text{ (see [3])} \end{aligned}$$

and $\sum \chi^2(v) \chi^2(v+1) = 3N + L - 2S - R - M = -1$,
using (3.4)', (3.5)', (3.6)', and therefore

$$S = \left(\frac{-a}{p}\right) \left[-\chi(-4a) R(1, 1) - \bar{\chi}(-4a) \overline{R(1, 1)} - 1 \cdot \chi^2(-4a) \right].$$

$$\begin{aligned} \text{Here } R(1, 1) &= (L - M - R - N + 2S) + i(2M - 2R) \\ &= (-2f + 8(1, 0) + 1) + i(2M - 2R) \text{ (see [3])}. \end{aligned}$$

We put $R(1, 1) = \pi$, then $\pi \equiv 1 \pmod{(2+2i)}$ and we get

$$S = \left(\frac{-a}{p}\right) \left[-\chi(-4a) \pi - \bar{\chi}(-4a) \bar{\pi} - \chi^2(-4a) \right]$$

and as before this

$$= -\left(\frac{a}{\bar{\pi}}\right)_4 \pi - \left(\frac{a}{\pi}\right)_4 \bar{\pi} - 1,$$

as required. This completes the proof of the Theorem.