

## ARITHMETIC SUMS THAT DETERMINE LINEAR CHARACTERS ON $\Gamma(N)$

RANDY TULER

A new class of arithmetic sums is defined and used to explicitly exhibit linear characters on  $\Gamma(N)$ , the principal congruence subgroup of level  $N$  in  $SL(2, \mathbf{Z})$ . As an application of this, we get a striking result on the structure of the commutator subgroup of  $\Gamma(N)$ .

**1. Introduction.** Let  $\alpha, \beta, N \in \mathbf{Z}$  with  $N > 1$ ,  $(\alpha, \beta) = 1$ , and  $\alpha - 1 \equiv \beta \equiv 0 \pmod{N}$ . For any function  $\chi: \mathbf{Z}/N\mathbf{Z} \rightarrow \mathbf{R}$  define the arithmetic sum

$$t_{N,\chi}(\alpha, \beta) = \begin{cases} \sum_{\substack{k=1 \\ k \neq 0 \pmod{N}}}^{\beta-1} \chi\left(\left[\frac{k\alpha}{\beta}\right] \pmod{N}\right), & \beta > 0 \\ 0 & , \beta = 0 \\ -t_{N,\chi}(\alpha, -\beta) & , \beta < 0 \end{cases}$$

where  $[ \ ]$  denotes the integer part.

**EXAMPLE 1.** With  $N = 2$ ,  $\chi(0) = 1$ , and  $\chi(1) = -1$  we have  $t_{2,\chi}(1, 2) = \chi([1/2]) = \chi(0) = 1$ ;  $t_{2,\chi}(5, 8) = \chi([5/8]) + \chi([15/8]) + \chi([25/8]) + \chi([35/8]) = \chi(0) + \chi(1) + \chi(3) + \chi(4) = 1 - 1 - 1 + 1 = 0$ .

The principal congruence subgroup of level  $N$  in  $SL(2, \mathbf{Z})$  is

$$\Gamma(N) = \{A \in SL(2, \mathbf{Z}) \mid A \equiv I \pmod{N}\}.$$

After preliminary work in §2 we prove

**THEOREM 1.** *If  $\sum_{g \in \mathbf{Z}/N\mathbf{Z}} \chi(g) = 0$ , then the map  $\Gamma(N) \rightarrow \mathbf{C}$  defined by*

$$\begin{pmatrix} \delta & \gamma \\ \beta & \alpha \end{pmatrix} \longrightarrow \exp(it_{N,\chi}(\alpha, \beta))$$

*is a linear character on  $\Gamma(N)$ .*

See [1] for the relation of this result to modular forms, knot theory, and recent work of J. B. Wagoner on diffeomorphisms of manifolds.

In §4, as an application of Theorem 1, we get a new result on the structure of the commutator subgroup of  $\Gamma(N)$ .

**2. Preliminaries.** We develop an analytic expression for  $t_{N,\chi}(\alpha, \beta)$

that is instrumental in the proof of Theorem 1. Let  $p, q, r \in \mathbf{R}^2$ , and let  $I(p, q)$  and  $I(p, q) + r$  denote the directed line segment from  $p$  to  $q$  and its translation by  $r$  respectively. Denote the oriented parallelogram in  $\mathbf{R}^2$  with sides  $I((0, 1), (0, 0), p)$ ,  $I((0, 0), p)$ ,  $I((0, 0), (0, 1) + p)$ , and  $I(p, (0, 0) + (0, 1))$  by  $\mathcal{R}(p)$ . Define the function  $\psi$  on  $\mathbf{Z}/N\mathbf{Z}$  by

$$\psi g() = \begin{cases} 1, & g \not\equiv 0(\text{mod } N) \\ 0, & g \equiv 0(\text{mod } N) . \end{cases}$$

LEMMA 1. *Let  $\{(m_k, n_k)\}$  be the points of  $\mathbf{Z} \oplus \mathbf{Z}$  contained in the convex hull of  $\mathcal{R}((\beta, \alpha))$ . Then*

$$\sum_k \psi(m_k)\chi(n_k - 1) = t_{N,\chi}(\alpha, |\beta|) .$$

*Proof.* For  $\beta > 0$ , the set of points of  $\mathbf{Z} \oplus \mathbf{Z}$  in the interior of the convex hull of  $\mathcal{R}((\beta, \alpha))$  is precisely

$$\left\{ \left( k, \left[ \frac{k\alpha}{\beta} \right] + 1 \right) \mid 0 < k < \beta \right\}$$

since  $(\alpha, \beta) = 1$ . The four points of  $\mathbf{Z} \oplus \mathbf{Z}$  on  $\mathcal{R}((\beta, \alpha))$  have  $m_k \equiv 0 \pmod{N}$ . Consequently,

$$\begin{aligned} \sum_k \psi(m_k)\chi(n_k - 1) &= \sum_{k=1}^{\beta-1} \psi(k)\chi\left(\left[ \frac{k\alpha}{\beta} \right]\right) \\ &= \sum_{\substack{k=1 \\ k \not\equiv 0 \pmod{N}}}^{\beta-1} \chi\left(\left[ \frac{k\alpha}{\beta} \right]\right) = t_{N,\chi}(\alpha, \beta) . \end{aligned}$$

The cases  $\beta = 0$  and  $\beta < 0$  are handled similarly.

For the rest of the paper, we assume  $\sum_{g \in \mathbf{Z}/N\mathbf{Z}} \chi(g) = 0$ .

LEMMA 2. *There is an elliptic function  $f$  (see [2]) with the following properties:*

- (1) *The period lattice of  $f$  is  $N\mathbf{Z} \oplus N\mathbf{Z}$ .*
- (2) *The pole set of  $f$  is  $S = \{(m, n) \in \mathbf{Z} \oplus \mathbf{Z} \mid m \not\equiv 0(\text{mod } N)\}$ .*
- (3) *If  $r = (m, n) \in S$ , then the residue of  $f$  at  $r$  is  $\chi(n - 1)$ .*

*Proof.* The pole set  $S$  is well-defined modulo the period lattice  $N\mathbf{Z} \oplus N\mathbf{Z}$ . The set of assigned residues is well-defined modulo  $N\mathbf{Z} \oplus N\mathbf{Z}$  since  $\chi$  is defined on  $\mathbf{Z}/N\mathbf{Z}$ . Furthermore, the sum of the assigned residues over a fundamental region of  $N\mathbf{Z} \oplus N\mathbf{Z}$  vanishes because  $\sum_{g \in \mathbf{Z}/N\mathbf{Z}} \chi(g) = 0$ . Under these conditions we may apply the Riemann-Roch theorem to assert the existence of  $f$ .

LEMMA 3. *The integral  $\int_{\mathcal{R}((\beta, \alpha))} f$  is well-defined.*

*Proof.* No point of  $S$  is on  $\mathcal{R}((\beta, \alpha))$ .

PROPOSITION 1.  $2\pi i t_{N, \chi}(\alpha, \beta) = \int_{\mathcal{R}((\beta, \alpha))} f$ .

*Proof.* Follows immediately from the preceding three lemmas and the residue theorem.

3. **Proof of Theorem 1.** For  $A \in \Gamma(N)$ , let  $\mathcal{R}((\beta, \alpha))A$  denote the parallelogram in  $\mathbf{R}^2$  obtained by applying the linear transformation  $A$  pointwise to  $\mathcal{R}((\beta, \alpha))$ .

LEMMA 4. *If  $A \in \Gamma(N)$ , then*

$$\int_{\mathcal{R}((\beta, \alpha))A} f = \int_{\mathcal{R}((\beta, \alpha))} f .$$

*Proof.*  $A$  fixes the lattice  $\mathbf{Z} \oplus \mathbf{Z}$  modulo  $N\mathbf{Z} \oplus N\mathbf{Z}$ . Consequently, the sum of the residues of  $f$  inside  $\mathcal{R}((\beta, \alpha))A$  is precisely the sum of the residues inside  $\mathcal{R}((\beta, \alpha))$ . Observing that  $A$  preserves orientation and applying the residue theorem finishes the proof.

LEMMA 5. *If  $A = \begin{pmatrix} \delta & \gamma \\ \beta & \alpha \end{pmatrix} \in \Gamma(N)$ , then*

$$2\pi i t_{N, \chi}(\alpha, \beta) = \int_{\mathcal{R}((0, 1)A)} f .$$

*Proof.*  $(0, 1)A = (\beta, \alpha)$ , so  $\mathcal{R}((0, 1)A) = \mathcal{R}((\beta, \alpha))$ . Apply Proposition 1.

*Proof of Theorem 1.* By Lemma 5, it suffices to show

$$\int_{\mathcal{R}((0, 1)A)} f + \int_{\mathcal{R}((0, 1)B)} f = \int_{\mathcal{R}((0, 1)BA)} f$$

for  $A, B \in \Gamma(N)$ . By Lemma 4,

$$\int_{\mathcal{R}((0, 1)A)} f + \int_{\mathcal{R}((0, 1)B)} f = \int_{\mathcal{R}((0, 1)A)} f + \int_{\mathcal{R}((0, 1)B)A} f .$$

Breaking up the path of integration into directed line segments, we write the right hand side of the last expression as

$$\begin{aligned} & \int_{\mathbb{I}((0,1),(0,0))} f + \int_{\mathbb{I}((0,0),(0,1)A)} f + \int_{\mathbb{I}((0,0),(0,1))+(0,1)A} f + \int_{\mathbb{I}((0,1)A,(0,0))+(0,1)} f \\ & + \int_{\mathbb{I}((0,1)A,(0,0))} f + \int_{\mathbb{I}((0,0),(0,1)BA)} f + \int_{\mathbb{I}((0,0),(0,1)A)+(0,1)BA} f \\ & + \int_{\mathbb{I}((0,1)BA,(0,0))+(0,1)A} f . \end{aligned}$$

Since  $A$  and  $B$  fix  $(0, 1)$  modulo  $N\mathbb{Z} \oplus N\mathbb{Z}$  and  $f$  has period lattice  $N\mathbb{Z} \oplus N\mathbb{Z}$ , we have the following relations:

$$(1) \quad \int_{\mathbb{I}((0,0),(0,1)A)+(0,1)BA} f + \int_{\mathbb{I}((0,1)A,(0,0))+(0,1)} f = 0$$

$$(2) \quad \int_{\mathbb{I}((0,0),(0,1))+(0,1)A} f = \int_{\mathbb{I}((0,0),(0,1))+(0,1)BA} f$$

$$(3) \quad \int_{\mathbb{I}((0,0),(0,1)A)} f + \int_{\mathbb{I}((0,1)A,(0,0))} f = 0$$

$$(4) \quad \int_{\mathbb{I}((0,1)BA,(0,0))+(0,1)A} f = \int_{\mathbb{I}((0,1)BA,(0,0))+(0,1)} f .$$

Applying (1), (2), (3), and (4) to the preceding sum of eight integrals gives

$$\begin{aligned} & \int_{\mathbb{I}((0,1),(0,0))} f + \int_{\mathbb{I}((0,0),(0,1)BA)} f \\ & + \int_{\mathbb{I}((0,0),(0,1))+(0,1)BA} f + \int_{\mathbb{I}((0,1)BA,(0,0))+(0,1)} f . \end{aligned}$$

To finish the proof of Theorem 1, we recognize this last sum as

$$\int_{\mathcal{L}((0,1)BA)} f .$$

EXAMPLE 2. Let  $N = 2$ ,  $\chi(0) = 1$ , and  $\chi(1) = -1$ . We have  $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix} \in \Gamma(2)$  and  $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix} = \begin{pmatrix} 13 & 8 \\ 34 & 21 \end{pmatrix}$ . Since  $\sum_{g \in \mathbb{Z}/2\mathbb{Z}} \chi(g) = 0$ , Theorem 1 asserts that  $t_{2,\chi}(21, 34) = t_{2,\chi}(1, 2) + t_{2,\chi}(5, 8)$ . From Example 1,  $t_{2,\chi}(1, 2) = 1$  and  $t_{2,\chi}(5, 8) = 0$ . Therefore  $t_{2,\chi}(21, 34) = 1 + 0 = 1$ . Checking this directly gives

$$\begin{aligned} t_{2,\chi}(21, 34) &= \sum_{\substack{k=1 \\ k \neq 0 \pmod{2}}}^{33} \chi\left(\left[\frac{21k}{34}\right]\right) \\ &= \chi(0) + \chi(1) + \chi(3) + \chi(4) + \chi(5) + \chi(6) + \chi(8) \\ &+ \chi(9) + \chi(10) + \chi(11) + \chi(12) + \chi(14) + \chi(15) \\ &+ \chi(16) + \chi(17) + \chi(19) + \chi(20) = 1 - 1 - 1 + 1 - 1 \\ &+ 1 + 1 - 1 + 1 - 1 + 1 + 1 - 1 + 1 - 1 - 1 + 1 = 1 . \end{aligned}$$

4. A structural theorem for the commutator subgroup of  $\Gamma(N)$ . Let  $\Gamma(N)'$  denote the commutator subgroup of  $\Gamma(N)$ .

**THEOREM 2.** Suppose  $\begin{pmatrix} \delta & \gamma \\ \beta & \alpha \end{pmatrix} \in \Gamma(N)'$  with  $\beta > 0$ . Then for any  $m \in \mathbf{Z}$  there are precisely  $1/N(\beta - \beta/N)$  elements of the set  $C = \{[k\alpha/\beta]\}_{\substack{k=1 \\ k \not\equiv 0 \pmod{N}}}^{\beta-1}$  that satisfy  $[k\alpha/\beta] \equiv m \pmod{N}$ .

*Proof.* For a fixed  $m \not\equiv 0 \pmod{N}$ , define

$$\chi(g) = \begin{cases} 1, & g \equiv 0 \pmod{N} \\ -1, & g \equiv m \pmod{N} \\ 0, & \text{otherwise.} \end{cases}$$

Using Theorem 1 along with the observation that the image of  $\Gamma(N)'$  under a linear character is trivial, we deduce that the number of elements of  $C$  that satisfy  $[k\alpha/\beta] \equiv m \pmod{N}$  is the same as the number of elements of  $C$  that satisfy  $[k\alpha/\beta] \equiv 0 \pmod{N}$ . Since this holds for any  $m \not\equiv 0 \pmod{N}$ , and since there are precisely  $\beta - \beta/N$  elements in  $C$ , we get the theorem.

**COROLLARY.** If  $\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \in \Gamma(N)'$ , then  $\beta = 0$ .

*Proof.* If  $\beta > 0$ , then every element of  $C$  vanishes. By Theorem 2,  $\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \notin \Gamma(N)'$ . If  $\beta < 0$ , use the preceding argument on  $\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}^{-1} \in \Gamma(N)'$ .

#### REFERENCES

1. R. Tuler, *Topological construction of multiplier systems on  $\Gamma(N)$* , dissertation, University of California at Berkeley, 1979.
2. S. Lang, *Elliptic Functions*, Addison-Wesley, 1973.
3. R. Rankin, *The modular group and its subgroups*, Ramanujan Institute, 1969.

Received October 30, 1979. This work is a part of the author's doctoral dissertation written under the supervision of J. B. Wagoner at the University of California, Berkeley.

UNIVERSITY OF GEORGIA  
ATHENS, GA 30602

