Here besides (5) we have the other trivial relations

$$a_m + a_{p-m} = 0 \qquad [m < \tfrac{1}{2}p). \tag{6}$$

It is reasonable to suppose that all the trivial linear relations between the a's in this special case are "derived" from (6), as (5) certainly may. In the special case when both p and $\frac{p-1}{2}$ are primes I proved this in a letter to Prof. C. L. Siegel (1949). Prof. Siegel considerably generalized my result. Recently Prof. Hasse has found simple and elegant proofs of such "tan-cot" theorems. See his paper in this volume. As one may expect all the proofs rely on the non-vanishing of series $\sum_1^\infty \frac{\chi(n)}{n}$ where $\chi(n)$ is a character (mod$p$).

§ 3. Recently Prof. Hasse and I have found the following result which will appear in Crelles journal. Let $x = x_0(p)$, $y = y_0(p)$ be the *smallest* positive solution of the Pellian equation

$$x^2 - py^2 = \pm 1.$$

One may conjecture that there are infinitely many primies p such that

$$x_0(p) > p^A$$

where A is an arbitrary real number. We prove that this conjecture is true if one assumes the "reasonable" conjecture that there are infinitely many primes of the form x^2+36.

For a superficial connection of this result with a Davis–Putnam hypothesis concerning Hilbert's Tenth problem, see a paper by me in the Proceedings of the Number-theory Conference at Boulder, Colorado, in 1963.

Received on 15. 3. 1970

ACTA ARITHMETICA
XVIII (1971)

On a question of S. Chowla

by

Helmut Hasse (Ahrensburg)

To the memory of my friend Harold Davenport

0. S. Chowla has raised the question whether for an odd prime $p = 2n+1$ the n division values

$$\tan\frac{r\pi}{p}, \qquad \cot\frac{r\pi}{p} \qquad (r = 1, \ldots, n), \tag{1}$$

respectively, are linearly independent over the rationals.

I shall prove here:

Theorem. *Necessary and sufficient for the linear independence over the rationals of the n values* (1) *is that the sums*

$$\sum_{s=1}^{n} (-1)^s \chi(s) = \chi(2)\sum_{s=1}^{n} \chi(s), \qquad \sum_{s=1}^{n} (2s-p)\chi(s) = \sum_{s=1}^{n} s\chi(s), \tag{2}$$

respectively, over the values of the n odd characters χ mod$p$ *are all different from zero.*

Since the second sums in (2) are known to be the factors of $-(-2p)^{n-1}h^*(p)$ where $h^*(p)$ is the relative class-number of the pth cyclotomic field $C(p)$ [1], it follows from this Theorem that *the answer to Chowla's question for the* cot-*values is in the positive.*

For the tan-values, however, I succeeded to answer it only in the special cases where n is either an odd prime or a power of 2, again in the positive [2]. In these special cases I could moreover give a proof of the positive answer for the cot-values, which is not based on the analytic class-number formula, but proceeds quite elementarily.

1. The values (1) belong to the cyclotomic field $C(2^2p)$ but can be brought to $C(p)$ by a factor i which is irrelevant for Chowla's question.

[1] Cf. the author's monography *Über die Klassenzahl abelscher Zahlkörper*, Berlin 1952, p. 12, (3b) and p. 68, Satz 23.

[2] See, however, the Addendum at the end.

For arithmetical reasons it is thus preferable to consider the adapted values

$$(3)\qquad \tau_r = i\tan\frac{r\pi}{p} = \frac{\zeta^{r/2}-\zeta^{-r/2}}{\zeta^{r/2}+\zeta^{-r/2}}, \qquad \tau'_r = i\cot\frac{r\pi}{p} = \frac{\zeta^{r/2}+\zeta^{-r/2}}{\zeta^{r/2}-\zeta^{-r/2}}$$

$(r = 1, \ldots, n)$ in $C(p)$. Here

$$\zeta = \exp\frac{2\pi i}{p}, \qquad \zeta^{1/2} = \exp\frac{\pi i}{p} = -\zeta^{-n}.$$

We have first to find expressions for these values with only rational denominators. In this respect observe the known facts that the $\zeta^{r/2}+\zeta^{-r/2}$ are algebraic units, whereas the $\zeta^{r/2}-\zeta^{-r/2}$ are algebraic primes dividing p. Therefore the tan- and cot-values can be expressed as polynomials in ζ with denominators 1 and p, respectively. It is, however, not necessary here to know this beforehand.

Since the τ_r, τ'_r are odd functions of the residue class $r \bmod p$, i.e.,

$$\tau_{p-r} = \tau_{-r} = -\tau_r, \qquad \tau'_{p-r} = \tau'_{-r} = -\tau'_r,$$

it seems reasonable to represent them by the odd part π_s of the basis

$$\varepsilon_s = \zeta^s+\zeta^{-s}, \qquad \pi_s = \zeta^s-\zeta^{-s} \qquad (s = 1, \ldots, n)$$

of $C(p)$, in which the ε_s and π_s are bases of the real and purely imaginary submodules of $C(p)$, respectively, and are accordingly even and odd, respectively. The fact that each of the two sets is linearly independent over the rationals is immediately evident from the irreducibility of the pth cyclotomic equation $\sum_{s=0}^{2n}\zeta^s = 0$.

It suffices to find the representation by the basis π_s for the tan- and cot-value with $r = 1$, viz.,

$$(4)\qquad \tau = \frac{\zeta^{1/2}-\zeta^{-1/2}}{\zeta^{1/2}+\zeta^{-1/2}} = -\frac{\pi_n}{\varepsilon_n}, \qquad \tau' = \frac{\zeta^{1/2}+\zeta^{-1/2}}{\zeta^{1/2}-\zeta^{-1/2}} = -\frac{\varepsilon_n}{\pi_n},$$

respectively, from which the τ_r, τ'_r are obtained by the automorphisms $\zeta \to \zeta^r$ of $C(p)$. Let

$$(5)\qquad \tau = \sum_{s=1}^{n} a_s\pi_s, \qquad \tau' = \sum_{s=1}^{n} b_s\pi_s$$

be this basis representation, with rational coefficients a_s, b_s. These can be determined in virtue of the multiplication formulae

$$\begin{aligned} \varepsilon_n\pi_s &= \pi_{n+s}-\pi_{n-s} & \qquad \pi_n\pi_s &= \varepsilon_{n+s}-\varepsilon_{n-s} \\ &= -\pi_{n+1-s}-\pi_{n-s}, & &= \varepsilon_{n+1-s}-\varepsilon_{n-s}, \end{aligned}$$

observing the marginal values

$$\varepsilon_0 = 2, \qquad \pi_0 = 0,$$

and the cyclotomic equation

$$\sum_{s=1}^{n}\varepsilon_s = -1,$$

as follows. By (4), (5),

$$\begin{aligned} \pi_n = -\varepsilon_n\tau &= -\sum_{s=1}^{n} a_s\varepsilon_n\pi_s, & \qquad -p\varepsilon_n = \pi_n p\tau' &= \sum_{s=1}^{n} b_s\pi_n\pi_s \\ &= \sum_{s=1}^{n} a_s\pi_{n+1-s} + \sum_{s=1}^{n} a_s\pi_{n-s} & &= \sum_{s=1}^{n} b_s\varepsilon_{n+1-s} - \sum_{s=1}^{n} b_s\varepsilon_{n-s} \\ &= \sum_{s=1}^{n-1}(a_{s+1}+a_s)\pi_{n-s} + a_1\pi_n, & &= \sum_{s=1}^{n-1}(b_{s+1}-b_s)\varepsilon_{n-s} + b_1\varepsilon_n - 2b_n\varepsilon_0 \\ & & &= \sum_{s=1}^{n-1}(b_{s+1}-b_s+2b_n)\varepsilon_{n-s} + (b_1+2b_n)\varepsilon_n. \end{aligned}$$

Comparison of coefficients yields the recurrent relations

$$\begin{aligned} a_{s+1} &= -a_s, & \qquad b_{s+1} &= b_s - 2b_n \qquad (s = 1, \ldots, n-1), \\ a_1 &= 1, & b_1 &= -2b_n - p, \end{aligned}$$

with the explicit solution

$$a_s = (-1)^{s-1}, \qquad b_s = 2s - p,$$

and thus the looked for basis representation

$$(6)\qquad -\tau = \sum_{s=1}^{n}(-1)^s\pi_s, \qquad p\tau' = \sum_{s=1}^{n}(2s-p)\pi_s.$$

2. By applying the automorphisms $\zeta \to \zeta^r$ to (6) we obtain the following expressions for the adapted tan- and cot-values:

$$(7)\qquad -\tau_r = \sum_{s=1}^{n}(-1)^s\pi_{rs}, \qquad p\tau'_r = \sum_{s=1}^{n}(2s-p)\pi_{rs} \qquad (r = 1, \ldots, n).$$

In order to investigate them as to their linear independence, we have to reduce the conjugates π_{rs} to the π_r.

For this purpose we consider the familiar reduction

$$(8)\qquad rs \equiv \pm r' \bmod p$$

of the products rs to their absolutely least residues $\pm r' \bmod p$, where the r' are a permutation of the r which, as well as the signs, depends on $s \bmod p$. We write (8) as a matrix equation

$$(8^*)\qquad \mathfrak{r}s \equiv M(s)\,\mathfrak{r} \bmod p,$$

where $\mathfrak{r}$ denotes the column consisting of $r = 1, \ldots, n$ and the $M(s)$ are monomial $n \times n$ matrices whose non-vanishing entries are ± 1. These matrices constitute an isomorphic representation of the (cyclic) prime residue class group $\operatorname{mod} p$.

Now, application of the automorphisms $\zeta \to \zeta^s$ to the basis π_r yields

$$\pi_{rs} = \pm \pi_{r'}$$

with the same r' and signs as in (8). Hence, letting $\mathfrak{p}_{\mathfrak{r}}$ denote the column consisting of the π_r, we have

$$\mathfrak{p}_{\mathfrak{r}s} = M(s)\mathfrak{p}_{\mathfrak{r}}$$

with the same matrices $M(s)$ as in (8*), and letting further $\mathfrak{t}_{\mathfrak{r}}, \mathfrak{t}'_{\mathfrak{r}}$ denote the columns consisting of the values τ_r, τ'_r, we obtain from (7)

$$-\mathfrak{t}_{\mathfrak{r}} = \Big(\sum_{s=1}^{n} (-1)^s M(s)\Big)\mathfrak{p}_{\mathfrak{r}}, \qquad p\mathfrak{t}'_{\mathfrak{r}} = \Big(\sum_{s=1}^{n} (2s-p)\, M(s)\Big)\mathfrak{p}_{\mathfrak{r}}.$$

Since the π_r are linearly independent over the rationals, the same holds for the τ_r, τ'_r if and only if the matrices

$$(9) \qquad \sum_{s=1}^{n} (-1)^s M(s), \qquad \sum_{s=1}^{n} (2s-p) M(s),$$

respectively, are regular, i.e., have determinants different from zero, or else, have all their eigenvalues different from zero.

3. These eigenvalues can easily be determined by the main theorem of representation theory, viz., that two representations are equivalent, and hence have the same eigenvalues, if and only if they have the same traces. By (8), (8*) the representation $M(s)$ has

$$\operatorname{tr} M(s) = \left\{\begin{matrix} \pm n & \text{for } s \equiv \pm 1 \operatorname{mod} p \\ 0 & \text{otherwise} \end{matrix}\right\}.$$

This trace is the same as that of the diagonal representation

$$D(s) = \begin{pmatrix} \ddots & & \\ & \chi(s) & \\ & & \ddots \end{pmatrix}$$

where χ runs through the odd characters $\operatorname{mod} p$. For, writing these χ as the odd powers $\omega^{2\nu+1}$ $(\nu = 0, \ldots, n-1)$ of a generating character $\omega \operatorname{mod} p$, we have

$$\operatorname{tr} D(s) = \sum_{\chi} \chi(s) = \omega(s) \sum_{\nu=0}^{n-1} \omega(s)^{2\nu} = \left\{\begin{matrix} \pm n & \text{for } s \equiv \pm 1 \operatorname{mod} p \\ 0 & \text{otherwise} \end{matrix}\right\},$$

because $\omega(s)^2$ runs through the nth roots of unity and $\omega(s)^2 = 1$ only for $s \equiv \pm 1 \operatorname{mod} p$.

Having thus verified that the eigenvalues of $M(s)$ are the same as those of $D(s)$, viz., the odd character values $\chi(s)$, we can conclude that the eigenvalues of the matrix sums (9) are the corresponding odd character sums (2) in our Theorem.

After what has been said before, this proves the Theorem.

4. Let us finally consider the two special cases mentioned at the end of the introduction.

I. n is an odd prime. In this case, of the n character sums (2) one is rational, viz., the one corresponding to the quadratic character $\operatorname{mod} p$, which here is indeed odd since $p = 2n+1 = -1 \operatorname{mod} 2^2$. This sum

$$(10) \quad \sum_{s=1}^{n} (-1)^s \left(\frac{s}{p}\right) = \left(\frac{2}{p}\right) \sum_{s=1}^{n} \left(\frac{s}{p}\right), \qquad \sum_{s=1}^{n} (2s-p) \left(\frac{s}{p}\right) = \sum_{s=1}^{2n} s \left(\frac{s}{p}\right),$$

respectively, is obviously different from zero, because its terms (in the cot-case only those of the first form) are odd and in odd number.

The other $n-1$ sums constitute a complete set of algebraically conjugate numbers in the cyclotomic field $C(2n)$. Hence they are either all zero or all different from zero. Suppose they were all zero. Since addition of all n sums yields the value

$$(11) \qquad -n, \qquad\qquad (2-p)n,$$

respectively, the sum (10) would then have this value. But this leads to a contradiction with its second form, as follows.

In the tan-case all terms would have to be -1, which is obviously wrong for $s = 2$.

In the cot-case, Eulers criterion would yield

$$\sum_{s=1}^{2n} s \left(\frac{s}{p}\right) \equiv \sum_{s=1}^{2n} s^{n+1} \equiv (2-p)n \not\equiv 0 \operatorname{mod} p,$$

whereas this sum is surely $\equiv 0 \operatorname{mod} p$ since the exponent $n+1 < 2n = p-1$.

II. n is a power of 2. In this case all the n character sums (2) constitute a complete set of algebraically conjugate numbers in the cyclotomic field $C(2n)$. Suppose they were all zero. Then their sum would be zero, too, whereas this sum has the non-zero values (11). Hence all those sums are different from zero.

We have thus proved by quite elementary means that in the special cases I and II the answer to Chowla's question is in the positive.

Addendum during proof correction (2.5.1971). As I have learn from a latter by Dr. Morris Newman, Washington, D. C., a simple argument, based on § 27, (3), of my monography quoted on p. 275, allows to conclude that also the *first* sums in (2) are all different from zero, simply because between them and the *second* sums in (2) the following elementary connection holds:

$$p\chi(2)\sum_{s=1}^{n}\chi(s) = \bigl(1-2\chi(2)\bigr)\sum_{s=1}^{n}s\chi(s).$$

Hence *the answer to Chowla's question is in the positive also for the tan-values.*

Received on 15. 3. 1970

ACTA ARITHMETICA
XVIII (1971)

The distribution of Farey points, I

by

M. N. Huxley (Cambridge)

Dedicated to the memory of
Professor H. Davenport

The "Farey sequence" of rational points with denominators not exceeding some bound Q has many amusing properties (see [2], chapter III). We are concerned here with the uniform distribution of the sequence modulo 1 as Q tends to infinity. By Weyl's principle the distribution is uniform if and only if certain exponential sums are small; for the Farey sequence these exponential sums transform by way of Ramanujan sums into expressions involving the Möbius function. In 1924 J. Franel [1] produced a quantitative form of this equivalence: he found an elegant identity for the sum of the squares of the values of the discrepancy function corresponding to our $E(a)$ below at the Farey points in terms of the sum-function of the Möbius function. In fact he showed that the infimum of θ for which (in our notation, for which see below)

$$\sum_{i=1}^{F}|E(f_i)|^2 \ll Q^{2+2\theta}$$

was the supremum of real parts of zeros of the Riemann zeta-function. (We use $\ll$ to indicate an inequality with an unspecified absolute constant.)

Davenport proposed in his problems list that an analogous result should hold for the zeros of a fixed Dirichlet L-function. In this note we supply the analogue by elementary arguments. We state our theorem with a general weight $\lambda(q)$, not necessarily a Dirichlet character, on the Farey point a/q. First we introduce the notation.

Let $f_1, \ldots, f_F$, where $f_i = a_i/q_i$, be the Farey sequence of order Q, that is, the sequence of rationals a/q with $(a, q) = 1$, $0 < a \leqslant q$ and $0 < q \leqslant Q$, arranged in ascending order. Let $\lambda(1), \ldots, \lambda(Q)$ be any complex numbers, and for each integer m write

$$L(m) = \sum_{n\leqslant Q/m}\lambda(mn)\sum_{d|n}\frac{\mu(d)d}{n}, \tag{1}$$