Mathematika 63 (2017) 919–943
doi:10.1112/S0025579317000304

HARMONIC ANALYSIS ON THE POSITIVE RATIONALS. DETERMINATION OF THE GROUP GENERATED BY THE RATIOS $(an + b)/(An + B)$

P. D. T. A. ELLIOTT AND JONATHAN KISH

In memory of Klaus Roth

Abstract. The multiplicative group generated by a certain sequence of rationals is determined, settling a 30-year conjecture.

§1. *Introduction.* The present paper settles in the affirmative a 30-year-old conjecture of the first author concerning the representation of an arbitrary positive rational by products and quotients of rationals taken from the sequence $(an + b)/(An + B)$, $n = 1, 2, \dots$, the fixed coefficient integers a, b, A, B to satisfy $a > 0$, $A > 0$, $\Delta = aB - Ab \neq 0$, cf. [**8**, Ch. 23, Unsolved Problems 11, 12].

To appreciate the underlying abstract problem, let $\mathbb{Q}^*$ denote the multiplicative group of positive rationals, Γ its subgroup generated by a given sequence of positive rationals r_n, $n = 1, 2, \dots$. The extent to which any further positive rational, w, has a representation

$$w = \prod_{j=1}^{m} r_j^{\varepsilon_j}, \quad \varepsilon_j = \pm 1,$$

is encoded in the structure of the quotient group $G = \mathbb{Q}^*/\Gamma$.

We may view G as free on the positive rational primes, restricted by the relations $r_n =$ identity, $n = 1, 2, \dots$. It is known that no finite recursive algorithm can be given to determine an arbitrary denumerably infinite abelian group presented in this manner, cf. [**2**, **8**], [**23**, Ch. 23, Exercises 106–108].

However, if U denotes the complex unit circle and we canonically extend a standard character $G \to U$ by $\mathbb{Q}^* \to \mathbb{Q}^*/\Gamma \to U$, then we obtain a complex-valued completely multiplicative function g on the positive rationals, of absolute value 1, i.e., a character on the group $\mathbb{Q}^*$, that satisfies $g(r_n) = 1$ on each of the rationals r_n, $n \geqslant 1$. We may ask whether the sequence r_n bears enough form to explicitly determine the dual group of G, hence G itself.

To this end, following examples of Gauss and Dirichlet, we ask for the asymptotic behaviour of the mean values

$$x^{-1} \sum_{n \leqslant x} g(r_n)$$

as x becomes unbounded.

Received 30 July 2016.
MSC (2010): 11K65, 11K70, 11K99, 20K99, 11L05, 11L99, 11N64, 11N99 (primary).

Viewed within this aesthetic, an *implicit* early application of harmonic analysis on $\mathbb{Q}^*$ is that of Elliott [4], in which probabilistic number theory is employed to settle affirmatively a 1968 conjecture of Kátai, [20], that a real-valued additive function vanishing on the shifted primes $p+1$ vanishes identically.

A more elaborate harmonic treatment of the shifted primes may be found in Elliott [15], 1995, where the quotient groups G_k corresponding to the subgroups of $\mathbb{Q}^*$ generated by the shifted primes $p+1$, $p>k$, are for all positive k shown to be of order at most 3.

Moreover, every positive integer w has infinitely many representations

$$w^{|G_k|}=\prod_{j=1}^{m}(p_j+1)^{\varepsilon_j},\quad \varepsilon_j=\pm 1,$$

with the number of shifted primes necessary for such representations bounded uniformly in w and k. Subsequent arguments reduced this bound to 9, cf. Berrizbeitia and Elliott [1], Elliott [17].

Note that since they are nested and their orders are uniformly bounded, for all sufficiently large values of k the groups G_k are isomorphic, cf. Elliott [18, §6].

Doubtless, in accordance with a century-old conjecture of Dickson, every group G_k is trivial and a single representing ratio $(p_1+1)/(p_2+1)$ will suffice.

A mainspring of the upper bound on the orders of the groups G_k is the inequality

$$\sum_{p+1\leqslant x}\left|\sum_{j=1}^{k}c_j g_j(p+1)\right|^2\leqslant\left(\lambda\frac{x}{\log x}+O\left(\frac{xk}{(\log x)^{21/20}}\right)\right)\sum_{j=1}^{k}|c_j|^2$$

with

$$\lambda=4+\max_{1\leqslant\ell\leqslant k}\sum_{\substack{j=1\\ j\neq\ell}}^{k}\max_{\chi\,(\mathrm{mod}\,d)}\frac{44d}{\phi(d)^2}\left|\frac{1}{x}\sum_{n\leqslant x}\overline{g_\ell(n)}g_j(n)\chi(n)\right|,$$

and its variants, cf. Elliott [15, Theorem 3 and Lemma 15], which hold uniformly for $x\geqslant 2$, multiplicative functions g_j with values in the complex unit disc, and complex c_j, $1\leqslant j\leqslant k$. The inner maximum runs over characters to squarefree moduli.

In particular, the size of the groups G_k is controlled by the size of the partial sums

$$\sum_{p\leqslant x}p^{-1}(1-\mathrm{Re}\,g(p)\chi(p)p^{it}),$$

the typical character g of $\mathbb{Q}^*$ braided with a Dirichlet character to an essentially bounded modulus and a standard unitary character on the multiplicative positive reals.

The genesis of the study of products of shifted primes and its connection with illuminating remarks of Wolke [25], Dress and Volkmann [3], and Meyer [21],

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

is considered in detail in Chapter 15 of the first author's 1985 Springer volume, [8]. An upshot of their results, and which is established in that same chapter, is that the torsion elements of a typical group $\mathbb{Q}^*/\Gamma$ are precisely those on which every homomorphism of the group into the additive reals vanishes.

In what follows G will denote the quotient group $\mathbb{Q}^*/\Gamma$ with Γ generated by the rationals $(an+b)/(An+B)$, $n>k$, $\Delta = aB-Ab \neq 0$, $k > \max(|a^{-1}b|, |A^{-1}B|)$. To simplify the exposition it will be further assumed that a and A are positive. Replacing $\mathbb{Q}^*$ by the multiplicative group of all rationals, simple changes allow that condition to be removed.

It was shown in that same Springer volume that this particular group is finitely generated. A study of the differences $f(an+b)-f(An+B)$ of a real-valued additive function f, hence of the homomorphisms of G into the additive reals, enabled a set of generators for the associated free group and membership of the attached torsion group to be determined.

As its main result the present paper determines the fine structure of the torsion group and establishes the conjecture.

THEOREM 1. *The dual of the group G, hence G itself, may be determined. In particular, G is finitely generated and its torsion group is an identifiable subgroup of the reduced residue class group* $(\mathrm{mod}\, 6(a,A)(aA)^2\Delta^3)$, *hence its homomorphic image.*

In the terminology of [8, Ch. 22], suitably interpreted G is *arithmic*.

The following waystation in the proof is of independent interest.

THEOREM 2. *Let integers $a>0$, $A>0$, b, B, satisfy $\Delta = aB-Ab\neq 0$. Set $\delta = 6(a,A)(aA)^2\Delta^3$.*

If a completely multiplicative complex-valued function g satisfies

$$g\left(\frac{an+b}{An+B}\right) = c \neq 0$$

on all but finitely many positive integers, n, then there is a Dirichlet character $(\mathrm{mod}\,\delta)$ *with which g coincides on all primes that do not divide δ.*

Theorem 2 is established in §2. Viewed as a character on $\mathbb{Q}^*$ restricted to the integers prime to $aA\Delta$, the function g is shown to have bounded order, to be essentially a Dirichlet character, then to be exactly a Dirichlet character, and with a modulus that divides $6(a,A)(aA)^2\Delta^3$.

Attention is drawn to application of a (recent) result of Tao [24], that a sufficiency of large sums $\sum_{p\leqslant x} p^{-1}(1-\mathrm{Re}\, g_1(p)\chi(p)p^{it})$, χ a Dirichlet character, t real, forces the logarithmically weighted correlation

$$(\log x)^{-1}\sum_{n\leqslant x} n^{-1} g_1(an+b)g_2(An+B), \quad \Delta\neq 0,$$

of multiplicative functions g_j, $j=1,2$ with values in the complex unit disc, to be small. This is an important step towards a suitably modified version of the

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

first author's conjecture, dating from the late 1980s, cf. [**11**, Conjecture II], see also [**12**], that if for multiplicative functions g_j, $1 \leqslant j \leqslant k$, with values in the complex unit disc, and integers $a_r > 0$, b_s, $a_r b_s - a_s b_r \neq 0$, $1 \leqslant r < s \leqslant k$,

$$\limsup_{x\to\infty} x^{-1}\left|\sum_{n\leqslant x}\prod_{j=1}^{k} g_j(a_j n + b_j)\right| > 0,$$

then there are Dirichlet characters χ_j and reals τ_j, so that the series

$$\sum \frac{1}{p}(1 - \operatorname{Re} g_j(p)\chi_j(p)p^{i\tau_j}), \quad j = 1, \dots, k,$$

converge.

That the correlation of two multiplicative functions can be controlled by just one of the functions is already manifest in the first author's 1994 AMS Memoir in probabilistic number theory, [**14**].

Theorem 1 is established in §3. The argument employs Theorem 2 to characterize the group G theoretically, then reduce its computation to a practicality.

Section 4 contains further practical matters, illustrated by examples. Section 5 considers simultaneous representations and offers variant arguments. Section 6 concludes the paper with a number of historical remarks by the first author concerning the asymptotic estimation of correlations of multiplicative functions.

Here it is convenient to note some constraints.

Constraints. Given integers $a > 0$, $A > 0$, b, B with $\Delta = aB - Ab \neq 0$, define $\alpha = (a, b)$, $\beta = (A, B)$, $a_1 = a\alpha^{-1}$, $b_1 = b\alpha^{-1}$, $A_1 = A\beta^{-1}$, $B_1 = B\beta^{-1}$, $\rho = \alpha\beta^{-1}$ in lowest terms and $\Delta_1 = a_1 B_1 - A_1 b_1$, so that $\Delta = \alpha\beta\Delta_1$. Define ρ_0 to be that part of ρ made up of primes that divide (a_1, A_1), to be 1 if there are none. This notation is consistent with that of [**8**, Ch. 16].

Since there are only two constraints upon n, we can find a positive n, and so a complete residue class, for which $(a_1 n + b_1)(A_1 n + B_1)$ is not divisible by a given odd prime, p.

Moreover, either this is possible for $p = 2$ or there is a pair of integers n_1, n_2 for which $2\|(a_1 n_1 + b_1)$, $\frac{1}{2}(a_1 n_1 + b_1)(A_1 n_1 + B_1)$ is odd, and $2\|(A_1 n_2 + B_1)$, $(a_1 n_2 + b_1)\frac{1}{2}(A_1 n_2 + B_1)$ is odd.

Hence we can either arrange for $(an + b)/(An + B) = \rho r$ with $(r, \delta) = 1$, or for the pair $(an_1 + b)/(An_1 + B) = 2\rho r_1$, $(an_2 + b)/(An_2 + B) = (\rho/2)r_2$, with $(r_1 r_2, \delta) = 1$.

For each prime divisor p of δ that does not divide (a_1, A_1) we can arrange a value of n such that $p\|(a_1 n + b_1)/(A_1 n + B_1)$. If $p^z\|\Delta_1$ and $p \nmid a_1$ (say), then we choose n such that $p^{z+1}\|(a_1 n + b_1)$. The identity $a_1(A_1 n + B_1) - A_1(a_1 n + b_1) = \Delta_1$ shows that $p^z\|(A_1 n + B_1)$.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

§2. *Proof of Theorem 2.* The argument is in four steps, annotated individually. Without loss of generality $(a, b) = 1 = (A, B)$.

Step 1. There is an integer m for which $g(p)^m = 1$ whenever $(p, aA\Delta) = 1$. Moreover, c is a root of unity.

For immediacy, in this step only we appeal to results from the first author's volume on arithmetic functions, [**8**], in which L^2 additive analogues of correlations are characterized, homomorphisms into the unit circle are replaced by homomorphisms into the additive reals. A merit is that their strong localization lends itself well to computation.

Choose a rational r for which $g(r)c = 1$. Then g has the value 1 on all but finitely many of the fractions $r(an+b)(An+B)^{-1}, n > 0$. Let Γ_0 be the subgroup of $\mathbb{Q}^*$ that they generate.

We may regard g as a character on the group $G_0 = \mathbb{Q}^*/\Gamma_0$.

Let f be a homomorphism of G_0 into the additive reals, i.e., a completely additive function that satisfies

$$f(an+b) - f(An+B) = -f(r), \quad n > n_0.$$

According to [**8**, Ch. 13], there is a real H so that $f(m) = H \log m$ whenever $(m, aA\Delta) = 1$.

There are two cases. As in Constraints, in the first case there is a residue class for which $an+b$, $An+B$ are both prime to $aA\Delta$. In this case

$$H \log\left(\frac{an+b}{An+B}\right) = -f(r)$$

for infinitely many positive integers, untenable unless $H = 0$.

Thus $f(p) = 0$ if $(p, aA\Delta) = 1$, and $f(r) = 0$.

For each such prime p there is a positive integer v, possibly depending upon p, and a representation

$$p^v = \prod_{j=1}^{k}\left(\frac{r(an_j+b)}{An_j+B}\right)^{\varepsilon_j}, \quad \varepsilon_j = \pm 1, n_j > n_0.$$

As a consequence $g(p)^v = 1$.

Likewise $g(r)^w = 1$ for some positive integer, guaranteeing c to be a root of unity.

If we choose a residue class $s \pmod{aA\Delta}$ for which $((as+b)(As+B), aA\Delta) = 1$, and consider the ratios

$$(a(aA\Delta n + s) + b)(A(aA\Delta n + s) + B)^{-1},$$

then the argument of [**8**, Ch. 4], shows that the subgroup of G generated by the cosets $p \pmod{\Gamma_0}$, $(p, aA\Delta) = 1$, is finitely generated, and by similar cosets.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

The existence of an integer m so that the $g(p)$ are all mth roots of unity is now clear.

In the second case we can find a residue class for which $an + b$ is divisible exactly by 2, but by no other prime divisor of $aA\Delta$, whilst $An + B$ is coprime to $aA\Delta$; also a residue class for which the roles of the parameters a, b, A, B are reversed.

Once again

$$f(2) - H\log 2 + H\log\left(\frac{an+b}{An+B}\right) = -f(r), \quad n > n_1$$

so that $H = 0$, $f(2) = -f(r)$.

Moreover,

$$-f(2) + H\log 2 + H\log\left(\frac{am+b}{Am+B}\right) = -f(r), \quad m > m_1,$$

so that $H = 0$, $f(2) = f(r)$.

Hence $f(2) = 0 = f(r)$.

Since we may choose r to have the form $2r_1$, where the rational r_1 is comprised only of primes not dividing $aA\Delta$, c itself is again a root of unity.

The inductive argument of [8, Ch. 4], proceeds, since the class 2 (mod Γ_0) has torsion, and for some m, $g(p)^m = 1$ on all primes not dividing $aA\Delta$.

Step 2. There is a Dirichlet character χ (mod D) and a set of primes q with $\sum q^{-1}$ convergent, such that $g(p) = \chi(p)$ on all remaining primes.

Remark. Without loss of generality we may assume χ to be primitive.

The following is Tao [24, Theorem 1.3].

LEMMA 1. *Let the integers $a > 0$, $b > 0$, c, d, satisfy $ad - bc \neq 0$. Let $\varepsilon > 0$ and suppose that A_0 is sufficiently large depending upon ε, a, b, c, d. Let $x \geqslant w \geqslant A_0$ and let g_1, g_2 be multiplicative functions, with values in the complex unit disc, for which*

$$\sum_{p\leqslant x} p^{-1}(1 - \operatorname{Re} g_1(p)\overline{\chi}(p)p^{-it}) \geqslant A_0$$

for all Dirichlet characters of period at most A_0, and all real numbers t with $|t| \leqslant A_0 x$.

Then

$$\left|\sum_{x/w<n\leqslant x} n^{-1} g_1(an+b)g_2(cn+d)\right| \leqslant \varepsilon \log w.$$

To implement the result of Tao we apply the following.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

LEMMA 2. *If* $|g(p)| \leqslant 1$ *on the primes and*

$$\sum_{p\leqslant x} p^{-1}(1-\operatorname{Re} g(p)p^{i\lambda(x)}) \ll 1,$$

with $\lambda(x)$ *real and* $\lambda(x) \ll x$, *for* $x \geqslant 2$, *then there is a constant* α *for which* $\lambda(x) = \alpha + O((\log x)^{-1})$ *and the series* $\sum p^{-1}(1-\operatorname{Re} g(p)p^{i\alpha})$ *converges.*

A somewhat elaborate version of Lemma 2 is employed in the first author's study of correlations attached to the sums of renormalized shifted additive functions, [**14**, §10.3]. The present version may be found as [**19**, Lemma 17]. Note that on page 84 line 2 of that account the first sum over the primes contains a surplus factor of $g(p)$.

Applying Lemma 1 to $g(an+b)\overline{g}(An+B)$ guarantees a constant A_0 and for each x sufficiently large a pair $\chi \pmod{D_x}$, t_x real, with χ a Dirichlet character to a modulus $D_x \leqslant A_0$, $|t_x| \leqslant A_0 x$, for which the sums

$$\sum_{p\leqslant x} p^{-1}(1-\operatorname{Re} g(p)\overline{\chi}(p)p^{-it_x})$$

are uniformly bounded.

The characters belong to a finite set. This provides a positive integer k for which $\overline{\chi}(p)^k = 1$ on all but finitely many primes. The inequality $1-\operatorname{Re} z^k \leqslant k^2(1-\operatorname{Re} z)$, valid in the complex unit disc, shows the sums

$$\sum_{p\leqslant x} p^{-1}(1-\operatorname{Re} g(p)^k p^{-ikt_x})$$

to be uniformly bounded.

An application of Lemma 2 guarantees a real β for which $t_x = \beta + O((\log x)^{-1})$. Hence

$$\sum_{p\leqslant x} p^{-1}(1-\operatorname{Re} g(p)\overline{\chi}(p)p^{-it_x})$$

differs from a similar sum with t_x replaced by β, by

$$\ll \sum_{p\leqslant x} p^{-1}|p^{-it_x} - p^{-i\beta}| \ll \sum_{p\leqslant x} p^{-1}|t_x-\beta|\log p \ll 1.$$

The sums

$$\sum_{p\leqslant x} p^{-1}(1-\operatorname{Re} g(p)\overline{\chi}(p)p^{-i\beta})$$

are uniformly bounded and, since there are only finitely many possibilities for the character, for some character the corresponding infinite series converges.

Although we shall not need it, it is interesting to note the following.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

LEMMA 3. *If for multiplicative functions g_j, $j = 1, 2$, with values in the complex unit disc,*

$$\liminf_{x\to\infty}(\log x)^{-1}\left|\sum_{n\leqslant x} n^{-1}g_1(an+b)g_2(An+B)\right| > 0,$$

then for some Dirichlet characters χ_j and reals β_j the series $\sum p^{-1}(1 - \operatorname{Re} g_j(p)\chi_j(p)p^{i\beta_j})$, $j = 1, 2$, converge.

To complete Step 2 we note that by Step 1, $g(p)^m = 1$ on all but finitely many primes. Hence the series

$$\sum p^{-1}(1 - \operatorname{Re} p^{-imk\beta})$$

converges; and that is only tenable if $\beta = 0$.

On the primes for which $g(p) \neq \chi(p)$, $g(p)\overline{\chi}(p)$ is a non-trivial mkth root of unity and the corresponding summands are uniformly bounded from below.

Step 3. $g(p) = \chi(p)$ provided $(p, D) = 1$, $(p, aA\Delta) = 1$.

It is convenient to establish a more general result.

LEMMA 4. *Let the integers $a > 0$, $A > 0$, b, B satisfy $\Delta = aB - Ab \neq 0$. Let g be a completely multiplicative function, with values in the complex unit disc, that satisfies*

$$\limsup_{x\to\infty} x^{-1}\left|\sum_{n\leqslant x} g(an+b)\overline{g}(An+B)\right| = 1,$$

it being understood that finitely many of the summands may be omitted.

If g is 1 on all primes that do not belong to a set of primes q for which $\sum q^{-1}$ converges, then g is 1 on all the primes that do not divide Δ.

In the particular case that g has a non-zero constant value on all but finitely many of the ratios $(an + b)/(An + B)$, it is further 1 on the primes that do not divide $(a/(a, b), A/(A, B))$.

The next result is a particular case of a theorem of Stepanauskas, [22], who was concerned with allowing the parameters a_j, b_j and functions g_j, $j = 1, 2$, to grow with the variable, x.

LEMMA 5. *Let g_1, g_2 be multiplicative arithmetic functions with values in the complex unit disc. Define the multiplicative functions h_j by $h_j(p^m) = g_j(p^m) - g_j(p^{m-1})$, $m = 1, 2, \ldots$, $j = 1, 2$. Let a_1, a_2, b_1, b_2 be integers satisfying $a_1 > 0$, $a_2 > 0$, $(a_j, b_j) = 1$, $j = 1, 2$, $\Delta = a_1b_2 - a_2b_1 \neq 0$.*

Define

$$w_p = \sum_{\substack{m_1=0\\(p_j^{m_j},a_j)=1,j=1,2\\(p^{m_1},p^{m_2})|\Delta}}^{\infty}\sum_{m_2=0}^{\infty} \frac{h_1(p^{m_1})h_2(p^{m_2})}{[p^{m_1}, p^{m_2}]},$$

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

$$S(x) = \sum_{j=1}^{2} \sum_{\log x < p \leqslant x} \frac{|s_j(p)|^2}{p},$$

where

$$s_j(p) = \begin{cases} g_j(p) - 1 & \text{if } p \nmid \Delta a_j, \\ g_1(p)g_2(p) - 1 & \text{if } p \mid \Delta,\ p \nmid a_j, \\ 0 & \text{if } p \mid a_j. \end{cases}$$

Then, uniformly in $x \geqslant 2$,

$$x^{-1} \sum_{n \leqslant x} g_1(a_1 n + b_1) g_2(a_2 n + b_2) - \prod_{p \leqslant x} w_p \ll S(x)^{1/2} + (\log x)^{-1},$$

the implied constant independent of the g_j.

Proof of Lemma 4. We define the multiplicative function h by Dirichlet convolution, $g = 1 * h$, so that

$$h(p^m) = g(p^m) - g(p^{m-1}) = (g(p) - 1)g(p)^{m-1}, \quad m = 1, 2, \ldots.$$

Then by Lemma 5,

$$\lim_{x \to \infty} x^{-1} \sum_{n \leqslant x} g(an + b)\overline{g}(An + B) = \prod_{p} w_p,$$

where, since this result holds for any choices of the $g(p)$, we may set all but one $g(p) = 0$ and conclude that $|w_p| \leqslant 1$. The displayed hypothesis of Lemma 4 then shows that $|w_p| = 1$ for each prime p.

The most interesting case in evaluating the w_p is when $p \nmid aA$, but p may divide Δ. If v is the highest power of p to divide Δ, then

$$w_p = 2 \operatorname{Re} \sum_{k=0}^{v} \overline{h(p^k)} \sum_{m \geqslant k} \frac{h(p^m)}{p^m} - \sum_{k=0}^{v} \frac{|h(p^k)|^2}{p^k}$$

and is real, hence ± 1.

The various sums are now geometric progressions and may be readily evaluated.

In our present circumstances $v = 0$ and

$$\operatorname{Re}\left(\frac{1 - 1/p}{1 - g(p)/p} \right) = 1 \text{ or } 0$$

is required. As a diagram in the complex plane shows, the left-hand ratio is in absolute value less than 1 unless $g(p) = 1$, and is certainly not zero.

The cases when p divides (exactly) one of a and A are simpler.

In most applications $g(p)$ lies on the unit circle and the constraints upon the w_p force $\operatorname{Re} g(p)$ to satisfy a quadratic equation with real coefficients.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

In the narrower context that g has a fixed non-zero value on all but finitely many of the ratios $(an+b)/(An+B)$, let $p \nmid a$. If $p^s \| \Delta$ then, with possibly a simple modification in regard to the prime 2, as in Constraints, we can arrange that $p^r \| (an+b)$, $r > s$, $p^{-r}(an+b)$, $p^{-s}(An+B)$ free of prime factors of Δ.

Since $g(p)^r$ has a constant value for $r > s$, $g(p) = 1$.

Enhanced by an eratosthenian sieve, this second method will then obviate appeal to Lemma 5, cf. [**8**, Ch. 12, particularly Lemma 12.4].

Completion of Step 3. The argument differs slightly according to the circumstances of the cases considered in Step 1.

In the first case we choose a residue class $s \pmod{aA\Delta D}$ for which $((as+b)(As+B), aA\Delta D) = 1$ and apply Lemma 4 to the function

$$g\overline{\chi}(a(aA\Delta n + s) + b)\overline{g}\chi(A(aA\Delta n + s) + B).$$

On the primes for which $(p, aA\Delta D) = 1$, $g\overline{\chi} = 1$.

In the second case(s) we adopt the modifications employed in Step 1, noting that $|g(2)| = 1$.

Step 4. D divides $6(a, A)(aA)^2\Delta^3$.

To this end we apply the following result.

LEMMA 6. *Let the integers $u_j > 0$, v_j, $(u_j, v_j) = 1$, $j = 1, 2$ satisfy $\Delta_1 = u_1v_2 - u_2v_1 \neq 0$. Assume that the primitive Dirichlet character χ_D satisfies*

$$\chi_D\left(\frac{u_1k + v_1}{u_2k + v_2}\right) = c \neq 0$$

for all k such that $(u_jk + v_j, D) = 1$, $j = 1, 2$, and that there exists a k_0 for which this holds; hence a class $k_0 \pmod D$.

Then $D \mid 6(u_1, u_2)\Delta_1$.

Proof of Lemma 6. Define

$$\chi_D\left(\frac{u_1k + v_1}{u_2k + v_2}\right) = 0 \quad \text{if } ((u_1k + v_1)(u_2k + v_2), D) > 1.$$

If $D = \prod_{p^t \| D} p^t$, then there is a decomposition $\chi_D = \prod_{p^t \| D} \chi_{p^t}$.

Correspondingly

$$\chi_D\left(\frac{u_1k + v_1}{u_2k + v_2}\right) = \chi_{p^t}\left(\frac{u_1k + v_1}{u_2k + v_2}\right)\chi_{D_1}\left(\frac{u_1k + v_1}{u_2k + v_2}\right)$$

where $D_1 = p^{-t}D$.

If we set $k = \tilde{k}D_1 + k_0$, then $(u_j(\tilde{k}D_1 + k_0) + v_j, D_1) = 1$, $j = 1, 2$, hence

$$\chi_{D_1}\left(\frac{u_1(\tilde{k}D_1 + k_0) + v_1}{u_2(\tilde{k}D_1 + k_0) + v_2}\right) = \chi_{D_1}\left(\frac{u_1k_0 + v_1}{u_2k_0 + v_2}\right) \neq 0.$$

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

Replacing $\tilde{k}$ by k:

$$\chi_{p^t}\left(\frac{u_1(kD_1+k_0)+v_1}{u_2(kD_1+k_0)+v_2}\right) = \begin{cases} c_1 \neq 0 & \text{if } (u_j(kD_1+k_0)+v_j,\, p)=1,\ j=1,2,\\ 0 & \text{otherwise.}\end{cases}$$

We have reduced ourselves to the case $D=p^t$, with u_j, v_j replaced by u_jD_1, $k_0u_j+v_j$, $j=1,2$.

Note that $D_1u_1(k_0u_2+v_2)-D_1u_2(k_0u_1+v_1)=D_1\Delta_1$.

For convenience of exposition, write w_j for $k_0u_j+v_j$, $j=1,2$.

Assume that $p^{s_j}\|u_j$ with, without loss of generality, $s_2 \leqslant s_1$. Otherwise, consider $\overline{\chi}_{p^t}$.

If $s_2 \geqslant t$ we have $p^t \mid (u_1,u_2)$ and we (temporarily) stop. Otherwise, set $u_j=p^{s_j}m_j$, so that $p\nmid m_j$, $j=1,2$. Then

$$\begin{aligned}\frac{u_1D_1k+w_1}{u_2D_1k+w_2} &= \frac{m_2(u_1D_1k+w_1)}{m_2(u_2D_1k+w_2)}\\ &= \frac{m_1p^{s_1-s_2}p^{s_2}m_2D_1k+m_2w_1}{m_2(m_2p^{s_2}D_1k+w_2)}\\ &= \frac{m_1p^{s_1-s_2}(m_2p^{s_2}D_1k+w_2)+m_2w_1-m_1p^{s_1-s_2}w_2}{m_2(m_2p^{s_2}D_1k+w_2)}\\ &= \frac{m_1}{m_2}p^{s_1-s_2}+\frac{m_2w_1-m_1p^{s_1-s_2}w_2}{m_2(u_2D_1k+w_2)}.\end{aligned}$$

Since χ_{p^t} is primitive, for an appropriate Gauss sum $\varepsilon(\chi_{p^t})$ with $|\varepsilon(\chi_{p^t})|=p^{t/2}$,

$$\chi_{p^t}\left(\frac{u_1D_1k+w_1}{u_2D_1k+w_2}\right)\varepsilon(\chi_{p^t}) = \sum_{r=1}^{p^t}\overline{\chi}_{p^t}(r)\exp\left(\frac{2\pi ir}{p^t}\left(\frac{u_1D_1k+w_1}{u_2D_1k+w_2}\right)\right)$$

whenever $(u_2D_1k+w_2,\,p)=1$.

In particular,

$$\varepsilon(\chi_{p^t})\sum_{k=1}^{p^{t-s_2}}{}'\chi_{p^t}\left(\frac{u_1D_1k+w_1}{u_2D_1k+w_2}\right) = \sum_{r=1}^{p^t}\overline{\chi}_{p^t}(r)\sum_{k=1}^{p^{t-s_2}}{}'\exp\left(\frac{2\pi ir}{p^t}\left(\frac{u_1D_1k+w_1}{u_2D_1k+w_2}\right)\right), \tag{1}$$

where $'$ denotes that summation is confined to terms with $(u_2D_1k+w_2,\,p)=1$.

The second innersum has the alternative representation

$$M=\sum_{k=1}^{p^{t-s_2}}{}'\exp\left(\frac{2\pi ir}{p^t}\left(\frac{m_1}{m_2}p^{s_1-s_2}+\frac{L}{u_2D_1k+w_2}\right)\right)$$

where

$$L=\overline{m}_2(m_2w_1-m_1p^{s_1-s_2}w_2), \qquad m_2\overline{m}_2\equiv 1 \pmod{p^t}.$$

Here $1/(u_2D_1k+w_2)$ is likewise interpreted as a group inverse $\pmod{p^t}$.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

For ease of notation we replace s_2 by s.

Assume that $s \geqslant 1$. The restriction $(u_2 D_1 k + w_2,\ p) = 1$ is then automatically satisfied.

For $1 \leqslant k \leqslant p^{t-s}$, arguing via representations, we map the class $u_2 D_1 k + w_2 \pmod{p^t}$ onto the class $j_k \pmod{p^{t-s}}$ given by

$$j_k = \frac{\overline{m_2 p^s D_1 k + w_2} - \overline{w}_2}{p^s},$$

the inverses taken $\pmod{p^t}$. Since

$$w_2(m_2 p^s D_1 k + w_2)(\overline{m_2 p^s D_1 k + w_2} - \overline{w}_2) \equiv m_2 p^s D_1 k \pmod{p^t},$$

j_k is well defined. It is the class

$$(w_2(m_2 p^s D_1 k + w_2))^{-1} m_2 D_1 k \pmod{p^{t-s}},$$

the group inverse $^{-1}$ here taken in the reduced residue class group $\pmod{p^{t-s}}$.

Moreover, if $j_{k_1} \equiv j_{k_2} \pmod{p^{t-s}}$, $1 \leqslant k_1 \leqslant k_2 \leqslant p^{t-s}$, then

$$\overline{m_2 p^s D_1 k_1 + w_2} - \overline{w}_2 \equiv \overline{m_2 p^s D_1 k_2 + w_2} - \overline{w_2} \pmod{p^t},$$

from which $k_1 \equiv k_2 \pmod{p^{t-s}}$ rapidly follows. The map is one-to-one and covers every class $\pmod{p^{t-s}}$.

In this case

$$\begin{aligned} M &= \sum_{j=1}^{p^{t-s}} \exp\left(\frac{2\pi i r}{p^t}\left(\frac{m_1}{m_2} p^{s_1 - s} + L(p^s j + \overline{w}_2)\right)\right) \\ &= \exp\left(\frac{2\pi i r}{p^t}\left(\frac{m_1}{m_2} p^{s_1 - s} + L\overline{w}_2\right)\right) \sum_{j=1}^{p^{t-s}} \exp\left(\frac{2\pi i r L j}{p^{t-s}}\right) = 0, \end{aligned}$$

unless $p^{t-s} \mid L$. Note that from (1) we may assume that $(r, p) = 1$.

Hence $p^t \mid p^s L$, $p^t \mid (p^s m_2 w_1 - p^{s_1} m_1 w_2)$, i.e., $p^t \mid (u_1 v_2 - v_1 u_2)$, and once more we (temporarily) stop.

Variant. Suppose now that $s = s_2 = 0$, i.e., $p \nmid u_2$. In this case

$$M = \sum_{k=1}^{p^t}{}' \exp\left(\frac{2\pi i r}{p^t}\left(\frac{u_1}{u_2} + \frac{L}{u_2 D_1 k + w_2}\right)\right).$$

Set $\gamma = \exp(2\pi i r u_1 / p^t u_2)$. Working within the reduced residue class group $(\mathrm{mod}\ p^t)$, we introduce a new variable $z = \overline{u_2 D_1 k + w_2}$. Since $z \to \overline{z}$ permutes the group, M has a representation

$$M = \gamma \sum_{\substack{z=1 \\ (z,p)=1}}^{p^t} \exp\left(\frac{2\pi i r L z}{p^t}\right),$$

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

a Ramanujan sum with an alternative representation in terms of the Möbius function:

$$M = \gamma \sum_{d|(p^t, rL)} \mu\left(\frac{p^t}{d}\right) d.$$

If $p^{t-1} \nmid L$, then $d = p^h$ with $h \leqslant t-2$, $\mu(p^t d^{-1}) = 0$ and, from (1),

$$\sum_{k=1}^{p^t}{}' \chi_{p^t}\left(\frac{u_1 D_1 k + w_1}{u_2 D_1 k + w_2}\right) = 0.$$

Since the summand with $k = p^t$ is non-zero, this is impossible. Therefore $p^{t-1} \mid L$.

If $p^t \mid L$, *then we stop, for once again* $p^t \mid \overline{m}_2(m_2 w_1 - m_1 p^{s_1} w_2)$, $p^t \mid (u_2 w_1 - u_1 w_2)$, *i.e.*, $p^t \mid (u_1 v_2 - u_2 v_1)$. Otherwise, $p^{t-1} \| L$, and the Ramanujan sum has value $-p^{t-1}$.

The fundamental relation (1) becomes

$$\begin{aligned}\varepsilon(\chi_{p^t}) \sum_{k=1}^{p^t} \chi_{p^t}\left(\frac{u_1 D_1 k + w_1}{u_2 D_1 k + w_2}\right) &= -p^{t-1} \sum_{r=1}^{p^t} \overline{\chi}_{p^t}(r) \exp\left(\frac{2\pi i r u_1}{p^t u_2}\right) \\ &= -p^{t-1} \chi_{p^t}\left(\frac{u_1}{u_2}\right) \varepsilon(\chi_{p^t});\end{aligned}$$

we may cancel the gaussian factors.

Several arguments now present themselves. For example, in absolute value the left-hand sum is at least $p^t - 2p^{t-1}$, guaranteeing that the prime p is at most 3.

At this stage, our initial hypothesis implies one of:

(i) $p^t \mid (u_1, u_2)$;
(ii) $p^t \mid (u_1 v_2 - u_2 v_1)$ if $p \geqslant 3$;
(iii) $p^{t-1} \mid (u_1 v_2 - v_1 u_2)$ if $p = 2$ or 3.

The conclusion of Lemma 6 is now clear.

Completion of Step 4. Once again there are small modifications according to the cases of Step 1. In the notation for the first case of Step 3,

$$\begin{aligned}1 &= g\left(\frac{a(aA\Delta n + s) + b}{A(aA\Delta n + s) + B}\right) \\ &= \chi\left(\frac{a(aA\Delta n + s) + b}{A(aA\Delta n + s) + B}\right), \quad \chi \pmod D,\end{aligned}$$

as long as χ is non-zero. By Lemma 6, D divides $6(a, A)(aA)^2\Delta^3$.

The remaining cases proceed similarly. Theorem 2 is established. □

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

§3. *Proof of Theorem 1.* The argument is in three steps.

We view a standard character on G as a completely multiplicative function g with values on the complex unit circle that satisfies $g((an+b)/(An+B)) = 1$ for all but finitely many positive integers n. This enables us to apply Theorem 2 with $c = 1$ and show, in the notation of Constraints, that g must satisfy the following three conditions:

(i) *there is a Dirichlet character* $\chi \pmod{\delta}$ *so that* $g(p) = \chi(p)$ *whenever* $(p, \delta) = 1$,
(ii) $g(p)^{2\phi(\delta)} = 1$ if $p \nmid (a_1, A_1)$; $g(\rho)^{2\phi(\delta)} = 1$,
(iii) $S(g, \chi) = 1$,

where

$$S(g,\chi) = g(\rho) \sum_{\substack{d_j \mid \delta_\infty \\ (d_1,d_2) \mid \Delta_1}} g(d_1)\,\overline{g}(d_2)\theta_{d_1,d_2}(\chi),$$

$$\theta_{d_1,d_2}(\chi) = \frac{1}{\delta[d_1,d_2]} \sum_{n \,(\mathrm{mod}\, \delta[d_1,d_2])}{}' \chi\left(\frac{a_1n+b_1}{d_1}\right)\overline{\chi}\left(\frac{A_1n+B_1}{d_2}\right)$$

and δ is the modulus guaranteed by Theorem 2.

We shall then show that these conditions suffice to determine the dual group of G, hence G itself. Moreover, individual groups G may be determined recursively.

A characterization of G. Given any character $g : G \to \{z \in \mathbb{C}, |z| = 1\}$, Theorem 2 provides a Dirichlet character $\chi \pmod{\delta}$ for which condition (i) is satisfied.

The remarks of Constraints, with application of the Chinese Remainder theorem, show condition (ii) to be satisfied.

Moreover,

$$\sum_{n\leqslant x} g(an+b)\overline{g}(An+B)$$
$$= g(\rho) \sum_{\substack{d_j \mid \delta_\infty \\ (d_1,d_2) \mid \Delta_1}} g(d_1)\overline{g}(d_2) \sum_{n\leqslant x}{}' \chi\left(\frac{a_1n+b_1}{d_1}\right)\overline{\chi}\left(\frac{A_1n+B_1}{d_2}\right)$$

where $d_j \mid \delta_\infty$ denotes that d_j is comprised of powers of the primes that divide δ and the innersum is taken over integers n for which $a_1n + b_1$ is divisible by d_1 and $A_1n + B_1$ by d_2. The value of the innermost summand is determined by the residue class $(\mathrm{mod}\, \delta[d_1, d_2])$ to which n belongs.

A typical innersum has the uniform bound $O(x/\max(d_1, d_2))$, and the asymptotic estimate

$$\sum_{n \,(\mathrm{mod}\, \delta[d_1,d_2])}{}' \chi\left(\frac{a_1n+b_1}{d_1}\right)\overline{\chi}\left(\frac{A_1n+B_1}{d_2}\right)\left(\frac{x}{\delta[d_1,d_2]} + O(1)\right).$$

In particular, the sum $\theta_{d_1,d_2}(\chi)$ is $O(\max(d_1, d_2)^{-1})$.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

Noting that

$$\sum_{\substack{d\leqslant y\\ d\mid\delta_\infty}} 1 \leqslant \prod_{p\mid\delta}\left(\left[\frac{\log y}{\log p}\right]+1\right) \ll (\log y)^\omega$$

where ω denotes the number of distinct prime divisors of δ, we see that

$$\sum_{\sqrt{y}<[d_1,d_2]\leqslant y} |\theta_{d_1,d_2}(\chi)| \ll (\log y)^\omega \sum_{\substack{d\mid\delta_\infty\\ d>y^{1/4}}} \frac{1}{d}$$

$$\ll (\log y)^\omega \sum_{p\mid\delta}\sum_{p^m>y^{1/4\omega}} \frac{1}{p^m} \ll (\log y)^\omega y^{-1/4\omega}.$$

Hence

$$\lim_{x\to\infty} x^{-1}\sum_{n\leqslant x} g(an+b)\overline{g}(An+B) = g(\rho) \sum_{\substack{d_j\mid\delta_\infty\\ (d_1,d_2)\mid\Delta_1}} g(d_1)\overline{g}(d_2)\theta_{d_1,d_2}(\chi),$$

which sum is $S(g,\chi)$, and condition (iii) is satisfied.

Conversely, suppose that we choose a $\chi \pmod\delta$, with $\delta = 6(a,A)(aA)^2\Delta^3$, and set $g(p)=\chi(p)$ if $(p,\delta)=1$. If we can, we next choose the $g(p)$ for p dividing δ but not (a_1,A_1) to satisfy $g(p)^{2\phi(\delta)}=1$, $g(\rho)^{2\phi(\delta)}=1$, $g(\rho)S(g,\chi)=1$. Note that on some of the prime factors of ρ, the value of g may have been chosen in an earlier round.

Then the corresponding completely multiplicative function g, with values in the complex unit circle, satisfies

$$\lim_{x\to\infty} x^{-1}\sum_{n\leqslant x} g(an+b)\overline{g}(An+B) = 1.$$

Denoting $g(an+b)\overline{g}(An+B)$ by z_n for convenience, we note that

$$x^{-1}\sum_{n\leqslant x}(1-\operatorname{Re} z_n)\to 0, \quad x\to\infty.$$

Here, if $z_n\neq 1$, $z_n^{2\phi(\delta)}=1$ guarantees that $1-\operatorname{Re} z_n \geqslant c_0>0$, the value of c_0 depending only upon δ.

In particular, those n for which $z_n\neq 1$ have asymptotic density zero.

Given an integer n_0 for which $a_1n_0+b_1=w_1r_1$ with w_1 comprised of primes dividing δ, r_1 coprime to δ, likewise $A_1n_0+B_1=w_2r_2$, then for a sufficiently large k every integer of the class $n_0 \pmod{\delta^k}$ will give rise to integers a_1n+b_1, A_1n+B_1 of the same form, with identical values of the w_j and with their corresponding r_j belonging to a respective fixed residue class $\pmod\delta$.

Hence

$$g\left(\frac{an+b}{An+B}\right) = g(\rho)\frac{g(w_1)}{g(w_2)}\frac{g(r_1)}{g(r_2)}$$

has a constant value on a non-empty residue class.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

Such a class has positive asymptotic density, hence contains a representative on which g has the value 1. Thus g has the value 1 on the whole class.

In this way every $g((an+b)/(An+B)) = 1$, i.e. g is a character on G.

Remarks. The choice of a principal character $(\mathrm{mod}\,\delta)$ enables the character g identically 1 on G, so the conditions (i)–(iii) are consistent.

For a given character $\chi\ (\mathrm{mod}\,\delta)$ there can be at most one compatible set of values for g on ρ and the remaining torsion primes. The ratio of two compatible values would yield a character on G that is 1 on the primes not dividing δ. In view of Lemma 4, it would also be 1 on the primes not dividing (a_1, A_1), hence on ρ.

Not every Dirichlet character $(\mathrm{mod}\,\delta)$ need give rise to a character on G.

This gives a characterization of G in terms of its dual group.

Consideration of the dual of the exact sequence $1 \to \Gamma \to \mathbb{Q}^* \to G \to 1$ shows the dual group of Γ to be isomorphic to the quotient of denumerably many copies of the unit circle, one for each prime, by the dual of G.

Determination of G; practical matters. The function $S(g, \chi)$ is given by an infinite series. In this section it will be shown that it factorizes and each of the finitely many factors is a polynomial in its associated variable $g(p)$.

Consider a typical sum

$$\sum_{n\ (\mathrm{mod}\,\delta[d_1,d_2])}{}' \chi\left(\frac{a_1n+b_1}{d_1}\right)\overline{\chi}\left(\frac{A_1n+B_1}{d_2}\right).$$

Let $\delta = \prod_{j\leqslant v} \ell_j^{\alpha_j}$, ℓ_j distinct primes, $d_1 = \prod_{j\leqslant v} \ell_j^{\beta_j}$, $d_2 = \prod_{j\leqslant v} \ell_j^{\gamma_j}$, where $\beta_j = 0$, $\gamma_j = 0$ is possible, but $\min(\beta_j, \gamma_j)$ is bounded by the constraint $\ell_j^{\min(\beta_j,\gamma_j)} \mid \Delta_1$.

Consider the map

$$n\ (\mathrm{mod}\,\delta[d_1, d_2]) \to \otimes n\ (\mathrm{mod}\,\ell_j^{\alpha_j+\max(\beta_j,\gamma_j)})$$

given by

$$n \to \sum_{j\leqslant v} u_j L_j,$$

where $L_j \equiv 1\ (\mathrm{mod}\,\ell_j^{\alpha_j+\max(\beta_j,\gamma_j)})$, $L_j \equiv 0\ (\mathrm{mod}\,\ell_r^{\alpha_r+\max(\beta_r,\gamma_r)})$ if $1 \leqslant r \leqslant v$, $r \neq j$, (Chinese Remainder theorem).

Typically $a_1n + b_1 \equiv 0\ (\mathrm{mod}\,d_1)$ if and only if $a_1n + b_1 \equiv 0\ (\mathrm{mod}\,\ell_j^{\beta_j})$, i.e. $a_1u_j + b_1 \equiv 0\ (\mathrm{mod}\,\ell_j^{\beta_j})$, $1 \leqslant j \leqslant v$. Similarly if $A_1n + B_1 \equiv 0\ (\mathrm{mod}\,d_2)$.

Then

$$\chi\left(\frac{a_1n+b_1}{d_1}\right) = \prod_{j\leqslant v} \chi_j\left(\frac{a_1n+b_1}{d_1}\right),$$

where χ_j is a Dirichlet character $(\mathrm{mod}\,\ell_j^{\alpha_j})$.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

In particular,

$$\chi_j\left(\frac{a_1n+b_1}{d_1}\right)=\chi_j\left(\frac{\sum_{r\leqslant v}(a_1u_r+b_1)L_r}{d_1}\right)$$

since $\sum_{r\leqslant v}L_r\equiv 1 \pmod{\delta[d_1,d_2]}$.

Hence

$$\chi_j\left(\frac{a_1n+b_1}{d_1}\right)=\chi_j\left(\frac{a_1u_j+b_1}{d_1}\right)=\chi_j\left(\frac{a_1u_j+b_1}{\ell_j^{\beta_j}}\right)\overline{\chi}_j(d_{1j})$$

where $d_{1j}=\ell_j^{-\beta_j}d_1$, $1\leqslant j\leqslant v$; for L_r/d_1 is divisible by $\ell_j^{\alpha_j}$ if $r\neq j$.

Define $\widehat{\chi}_j(\ell_j^{\beta_j})$ to be $\prod_{1\leqslant r\leqslant v, r\neq j}\overline{\chi}_r(\ell_j^{\beta_j})$, $1\leqslant j\leqslant v$, dual analogue of Tate's lift of a Dirichlet character to a character on the rational idèles.

The sum $S(g,\chi)$ becomes

$$g(\rho)\prod_{j=1}^{v}\sum_{\substack{\beta_j\geqslant 0\\ \gamma_j\geqslant 0}}\frac{g(\ell_j^{\beta_j})\widehat{\chi}_j(\ell_j^{\beta_j})\overline{g}(\ell_j^{\gamma_j})\overline{\widehat{\chi}}_j(\ell_j^{\gamma_j})}{\ell_j^{\max(\beta_j,\gamma_j)}}\eta_j$$

where

$$\ell_j^{\alpha_j}\eta_j=\ell_j^{\alpha_j}\eta_j(\beta_j,\gamma_j)=\sum_{u_j \pmod{\ell_j^{\alpha_j+\max(\beta_j,\gamma_j)}}}{}'\chi_j\left(\frac{a_1u_j+b_1}{\ell_j^{\beta_j}}\right)\overline{\chi}_j\left(\frac{A_1u_j+B_1}{\ell_j^{\gamma_j}}\right),$$

it understood that $a_1u_j+b_1\equiv 0 \pmod{\ell_j^{\beta_j}}$, $A_1u_j+B_1\equiv 0 \pmod{\ell_j^{\gamma_j}}$, and $\ell_j^{\min(\beta_j,\gamma_j)}\mid\Delta_1$, $1\leqslant j\leqslant v$.

Since $g(\ell_j^{\beta})=g(\ell_j)^{\beta}$, χ^{β} are periodic in β, period $2\phi(\delta)$, a typical innersum becomes a polynomial in $g(\ell_j)\widehat{\chi}_j(\ell_j)$, of degree at most $2\phi(\delta)-1$, with coefficients that are linear forms in $2\phi(\delta)$th roots of unity (values of χ) that in turn have coefficients that are essentially geometric progressions, indeed rational numbers.

The values of the $g(p)$, $p\nmid(a_1,A_1)$, together with that of $g(\rho)$, that fulfill conditions (ii) and (iii) may therefore be ascertained recursively.

Theorem 1 is established. □

Remark. For any prime ℓ and integers $\alpha\geqslant 1$, $\beta\geqslant 0$, $\gamma\geqslant 0$, the sum

$$\tilde{\eta}(\beta,\gamma)=\ell^{-\alpha}\sum_{\substack{u \pmod{\ell^{\alpha+\max(\beta,\gamma)}}\\ \ell^{\beta}\parallel(a_1u+b_1),\ \ell^{\gamma}\parallel(A_1u+B_1)}}1,$$

i.e. a typical η_j with χ_j the principal character $\pmod{\ell}$, represents the asymptotic density of the integers n for which $\ell^{\beta}\parallel(a_1n+b_1)$, $\ell^{\gamma}\parallel(A_1n+B_1)$. In particular,

$$\sum_{\beta\geqslant 0,\gamma\geqslant 0}\tilde{\eta}(\beta,\gamma)=1.$$

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

In absolute value, each term in the above product representing $S(g, \chi)$ does not exceed 1. In order for $|S(g, \chi)| = 1$ to hold it is necessary and sufficient that every term in the product have absolute value 1. In particular, each η_j must satisfy $|\eta_j(\beta_j, \gamma_j)| = \tilde{\eta}(\beta_j, \gamma_j)$ with respect to the appropriate prime $\ell = \ell_j$.

§4. *Further practical matters.* Let k be a positive integer. The foregoing argument reduces the determination of the multiplicative group generated by the rationals $(an + b)/(An + B)$ with $n \geqslant k$ to a calculation in a polynomial ring over a cyclotomic extension of the rational field.

The following results may accelerate this process.

Example. The groups $\mathbb{Q}^*/\Gamma_k$ attached to the ratios $(3n+1)/(5n+2)$, $n \geqslant k$, introduced in the first author's volume on arithmetic functions and integer products [**8**], were there shown, via homomorphisms into the positive reals, to be finite.

After Theorem 2 each character g on $\mathbb{Q}^*/\Gamma_k$ coincides, on the primes p that do not divide 30, with a product of Dirichlet characters $\chi_2\chi_3\chi_5$ to moduli 2, 3^2 and 5^2 respectively.

For $\chi = \chi_3$, a typical sum

$$\eta(\beta, \gamma) = \sum_{\substack{u \pmod{3^{2+\max(\beta,\gamma)}} \\ 3^\beta \| (3u+1),\ 3^\gamma \| (5u+2)}}{}' \chi\left(\frac{3u+1}{3^\beta}\right)\overline{\chi}\left(\frac{5u+2}{3^\gamma}\right)$$

necessarily has $\beta = 0$ and, if $5u_0 + 2 \equiv 0 \pmod{3^\gamma}$ with $\gamma \geqslant 2$, $u = u_0 + 3^\gamma k$, a representation

$$\chi(3u_0 + 1) \sum_{k=1}^{3^2} \overline{\chi}(5k + 3^{-\gamma}(5u_0 + 2))$$

that vanishes unless the character χ_3 is principal.

The character χ_5 is likewise principal.

The character g on $\mathbb{Q}^*$ is principal on all primes save possibly 2, 3 and 5, and by Lemma 4 on these also.

The groups $\mathbb{Q}^*/\Gamma_k$ are trivial. Each positive rational r has infinitely many representations

$$r = \prod_j \left(\frac{3n_j + 1}{5n_j + 2}\right)^{\varepsilon_j}, \quad \varepsilon_j = \pm 1,$$

with the n_j as large as desired. In the notation of the preface to the volume [**8**], we may take $v = 1$.

Rationalizing the denominators establishes the following.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

Multiplicity lemma. Let the integers $a_j > 0, b_j$, $j = 1, 2$, *satisfy* $\Delta_0 = a_1b_2 - a_2b_1 \neq 0$, *and the integers* s, n, n', $(s, (a_2n + b_2)(a_2n' + b_2)) = 1$.

Then

$$\frac{a_1n + b_1}{a_2n + b_2} \equiv \frac{a_1n' + b_1}{a_2n' + b_2} \pmod{s}$$

if and only if $\Delta_0(n - n') \equiv 0 \pmod{s}$.

Example. Consider the group $\mathbb{Q}_5^*/\Gamma$, where $\mathbb{Q}_5^*$ denotes the multiplicative positive rationals not divisible by 5 and Γ its subgroup generated by all but finitely many fractions of the form $(5n + 1)/(5n - 1)$. It was established in the first author's volume [**8**] that $\mathbb{Q}_5^*/\Gamma$ is finite. Reduction $\pmod 5$ shows 2 not to belong to Γ, hence that $\mathbb{Q}_5^*/\Gamma$ is not trivial.

According to the main result of the present paper, on the primes that do not divide 30 each character g on $\mathbb{Q}_5^*/\Gamma$ coincides with a product of Dirichlet characters, $\chi_2\chi_3\chi_5$, to moduli 2^4, 3 and 5^8 respectively.

For $\chi = \chi_3$, a typical sum

$$\eta(\beta, \gamma) = \sum_{\substack{u \pmod{3^{1+\max(\beta,\gamma)}} \\ 3^\beta \| (5u+1),\ 3^\gamma \| (5u+2)}}{}' \chi\left(\frac{5u+1}{3^\beta}\right)\overline{\chi}\left(\frac{5n-1}{3^\gamma}\right)$$

with $\gamma = 0$, $\beta \geqslant 1$, if $5u_0 + 1 \equiv 0 \pmod{3^\beta}$, has a representation

$$\overline{\chi}_3(5u_0 - 1)\sum_{k=1}^{3} \chi_3(5k + 3^{-\beta}(5u_0 + 1))$$

that vanishes unless χ_3 is principal.

A similar argument shows that χ_2 is principal.

It follows from the multiplicity lemma that the ratios $(30n + 1)/(30n - 1)$ cover 5^7 distinct residue classes $\pmod{5^8}$, five times each. From what we have proved so far, if $\chi = \chi_5$ has order t, then $5^7 \leqslant t^{-1}\phi(5^8)$; $t = 1, 2$ or 4.

Since 3 is a primitive root for all reduced residue class groups $\pmod{5^r}$, $r = 1, 2, \ldots$, and the representative exponents of a given integer $\pmod 5$ and $\pmod{5^8}$ differ by a multiple of 4, we may assume χ to be defined $\pmod 5$. Then $\chi(3)^2 = \chi(3^2) = \chi(-1) = 1$, and χ_5 has order 1 or 2.

An application of Lemma 4 to $g\overline{\chi}_5$ shows that g coincides with χ_5 on the primes 2 and 3.

The group $\mathbb{Q}^*/\Gamma$ generated by the ratios $(5n+1)/(5n-1)$ has the single free generator, 5, and a torsion group of order 2 determined by its dual through the quadratic Dirichlet character $\pmod 5$.

There are infinitely many representations

$$57^2 = \prod_j \left(\frac{5n_j + 1}{5n_j - 1}\right)^{\varepsilon_j}, \quad \varepsilon_j = \pm 1,$$

but no such representation is available to 57 itself.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

Note that the group $G = \mathbb{Q}_5^\times / \Gamma$, with $\mathbb{Q}_5^\times$ the multiplicative rationals prime to 5, Γ its subgroup generated by the ratios $(5n-1)/(-5n+1)$, $n > k$, has order 4.

In the basic condition (iii) $S(g, \chi)$ is replaced by $g(-1)S(g, \chi)$ where g is a unitary character on $\mathbb{Q}_5^*$ extended to $\mathbb{Q}_5^\times$ by setting $g(-1) = 1$ or -1. As a consequence the dual group of G is generated by a quartic character $\pmod 5$ with $g(-1) = -1$.

There is a representation

$$57^4 = \prod_j \left(\frac{5n_j + 1}{-5n_j + 1} \right)^{\varepsilon_j}, \quad n_j > k,$$

but no similar representation for 57^2.

Remark. A short elementary proof that a complex-valued multiplicative function constant on all sufficiently large members of a progression $an + b$, $a > 0$, coincides with a Dirichlet character $\pmod a$, on the integers prime to a, may be found as [**8**, Lemma 19.3, pp. 334–335].

§5. *Further results. Two dimensional product representations.* Let $\mathbb{Q}_2 = \mathbb{Q}^* \oplus \mathbb{Q}^*$ be the direct sum of two copies of the multiplicative positive rationals, Γ_2 its subgroup generated by the pairs $(an+b) \oplus (An+B)$, $n > k$. Simultaneous representations of the form

$$r_1 = \prod_{j=1}^m (an_j + b)^{\varepsilon_j}, \qquad r_2 = \prod_{j=1}^m (An_j + B)^{\varepsilon_j}, \quad \varepsilon_j = \pm 1,$$

may be studied through the offices of the quotient group $\mathbb{Q}_2 / \Gamma_2$. A typical character on that group amounts to a pair of completely multiplicative functions g_1, g_2, with values in the complex unit circle, and that satisfy

$$g_1(an + b) g_2(An + B) = 1, \quad n > k.$$

We may reduce this two-dimensional problem to a one-dimensional problem by means of the following argument, given in an equivalent form in [**8**, Ch. 19]. For ease of notation we shall assume, as we clearly may, that $b > 0$, $B > 0$.

Replacing n by bBn,

$$g_1(aBn + 1) g_2(Abn + 1) = c_1 \neq 0.$$

Replacing n by $(aB + 1)n + 1$,

$$g_1(aBn + 1) g_2(Ab[(aB + 1)n + 1] + 1) = c_2 \neq 0.$$

Eliminating between these relations,

$$g_2(Ab(aB + 1)n + 1) \overline{g}_2(Abn + 1) = c_3 \neq 0,$$

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

to which we can apply Theorem 2. The functions g_2 and g_1 are essentially Dirichlet characters and we may follow the treatment for a single function.

Variant proof of Theorem 1. There is an alternative procedure in Steps 2 and 3 that avoids appeal to the results of Step 1 and may more readily generalize to higher dimensional problems. Once Step 2 guarantees the existence of a real α for which the series $\sum p^{-1}(1-\operatorname{Re} g(p)^k p^{-i\alpha})$ converges, Lemma 5 is applied to the completely multiplicative function h defined by $p \to h(p) = g(p)^k p^{-i\alpha}$. We arrive at an asymptotic estimate

$$\lim_{x\to\infty} x^{-1} \sum_{n\leqslant x} h(an+b)\overline{h}(An+B) = \prod_p w_p$$

where the w_p may now depend upon the parameter α. Following the argument of Step 3, $g(p)^k = p^{i\alpha}$ on all but finitely many primes.

Bearing in mind the two cases considered in Constraints, typically, on a suitable residue class $(g(an+b)\overline{g}(An+B))^k$ will coincide with $((an+b)/(An+B))^{i\alpha}$.

A simple analogue of Theorem 2 then suffices to guarantee that $\alpha = 0$.

LEMMA 7. *If integers $u_j > 0$, v_j, $j = 1, 2$, $\Delta = u_1v_2 - u_2v_1 \neq 0$, satisfy*

$$\left(\frac{u_1 n + v_1}{u_2 n + v_2}\right)^{i\alpha} = c$$

for all n sufficiently large, then $\alpha = 0$ and $c = 1$.

Proof of Lemma 7. Since $(u_j n+v_j)^{i\alpha} = (u_j n)^{i\alpha}(1+i\alpha v_j(u_j n)^{-1}+O(n^{-2}))$, $j = 1, 2$,

$$c = \left(\frac{u_1}{u_2}\right)^{i\alpha}\left(1 + \frac{i\alpha\Delta}{u_1u_2n} + O\left(\frac{1}{n^2}\right)\right), \quad n \to \infty.$$

This forces $(u_1/u_2)^{i\alpha} = c$, $\alpha = 0$, $c = 1$ in turn.

We may now continue as before until reaching the section on constraints. To once again avoid applying Step 1, choice of an appropriate residue class for n will, for example, for a given prime p arrange infinitely many representations

$$1 = g\left(\frac{an+b}{An+B}\right) = g(p)\chi\left(\frac{an+b}{p(An+b)}\right)$$

with $p\|(an+b)$, $(p^{-1}(an+b)(An+B), \delta) = 1$, where χ is a Dirichlet character $(\mathrm{mod}\,\delta)$.

In particular, $g(p)$ will be a value of the character χ, and $g(p)^k = 1$ with k the order of χ. □

Altogether, this variant argument obviates appeal to the Fourier analysis, involving estimates for Kloosterman sums, that is given in [**8**, Chs 2 and 4]. It does not deliver, for the moment at least, the upper bound on the number of

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

terms sufficient to represent group theoretically a typical positive rational, r, or the underlying recursive argument by which such a bound is obtained there. Moreover, the attendant inequalities on the additive functions in [8, Ch. 10], are strongly localized.

§6. *Closing remarks (by the first author).* In anticipation of the validity of an appropriate version of the conjecture that correlations of multiplicative functions with values in the complex unit circle could only satisfy

$$\limsup_{x\to\infty} x^{-1}\left|\sum_{n\leqslant x} g_1(an+b)g_2(An+B)\right| > 0, \quad \Delta \neq 0,$$

if there are reals τ_j and Dirichlet characters χ_j so that the series

$$\sum p^{-1}(1-\operatorname{Re} g_j(p)\chi_j(p)p^{i\tau_j}), \quad j=1,2,$$

taken over the prime numbers converge, a particular case of Conjecture II mentioned in the Introduction, Jonathan Kish and I were already in possession of a detailed version of Step 4 in the proof of Theorem 2 by mid 2010—putting the cart before the horse is sometimes helpful.

The conjecture has a root in the probabilistic theory of numbers. In the early 1970s, when studying asymptotic behaviour of additive arithmetic functions with unbounded renormalizations:

$$[x]^{-1}\sum_{\substack{n\leqslant x\\ f(n)-\alpha(x)\leqslant z\beta x}} 1 \qquad , \quad x(\text{real})\to\infty.$$

I felt that the Erdős–Kac realization of an additive function as a sum of independent random variables, in general not valid, might be restored provided a suitable (moving) obstruction were removed from f.

Where to find such an obstruction? In the event, cf. [5, 6], perturbation of the underlying probability models, somewhat in the style of the perturbation of planetary orbits within the circle of ideas of the Hamilton–Jacobi equation, led to a satisfactory outcome, the renormalizing functions $\alpha(x)$, $\beta(x)$ classified according to their behaviour under the group of transformations $x\to x^y$, $y>0$, fixed.

The same point of view could be applied to frequencies involving the sums $f_1(an+b)+f_2(An+B)$ of two (or more) possibly distinct additive functions, $aB-Ab\neq 0$, cf. [7].

The respective characteristic functions of the corresponding frequencies have the form

$$[x]^{-1}\sum_{n\leqslant x} g(n), \qquad [x]^{-1}\sum_{n\leqslant x} g_1(an+b)g_2(An+B),$$

where the functions $g(n)=\exp(itf(n))$, $g_j(n)=\exp(itf_j(n))$, t, t_j real, are multiplicative.

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

Besides the many experiences in probabilistic number theory, there is the further experience of the Hardy–Ramanujan–Littlewood circle method. One may view that method as resting on the approximation of continuous characters $\alpha \to \exp(2\pi i k\alpha)$, $k = 0 \pm 1, \pm 2, \ldots$, on the group $\mathbb{R}/\mathbb{Z}$ dual to the additive group of integers, by the discrete characters $a/q \to \exp(2\pi i ka/q)$, (usually effected with $(a, q) = 1$) on the additive (reduced) group $\mathbb{Z} \pmod{q\mathbb{Z}}$.

For this and other reasons the Dirichlet characters suggested themselves as obstructions in the dual group of the positive rationals under multiplication, the direct product of denumerably many copies of $\mathbb{R}/\mathbb{Z}$, and in which, in a certain sense, they are dense, cf. [**16**, Ch. 12, Exercise 7]. The role of reduced rationals a/q is then played by primitive characters.

Whilst the Stone–Weierstrass theorem might offer other approximating functions, the connections between special functions and group representations also suggests the application of associated group characters.

Conjecture III of [**14**, p. 65], that there is a positive absolute constant c such that

$$x^{-1}\sum_{n\leqslant x} g(n)h(n+1) \ll \left(T^{-1} + \exp\left(-\min_{\chi}\min_{|\tau|\leqslant T}\sum_{p\leqslant x} p^{-1}(1-\operatorname{Re} g(p)\chi(p)p^{i\tau})\right)\right)^{c}$$

uniformly for $x \geqslant 2$, and multiplicative functions g, h with values in the complex unit disc, modified by the requirement that the characters χ be to moduli not exceeding T, as noted in the author's Cambridge Tract [**16**, Ch. 34, p. 315], may well be applied to $g(an+b)h(An+B)$, $aB - Ab \neq 0$.

It is clear that some restriction must be made upon the size of the defining moduli of the characters χ, since the application of Kronecker's theorem that shows the χ to be dense in the dual of $\mathbb{Q}^*$ for a given value of x shows the minimum over χ in Conjecture III to be arbitrarily close to zero.

Although the ultimate aim was for a fixed obstruction, experience in Probabilistic Number Theory showed that the variable τ might be allowed to float far past x in size yet be retrieved, cf. [**10**, **19**]. Moreover, cf. [**9**, **13**], I was aware that for considerable ranges of τ and the modulus D, at most one generalized character $n \to \chi(n)n^{i\tau}$, $\chi \pmod{D}$, could be near to a given multiplicative function. To this extent the obstruction would be isolated (just as it is in the case of a single renormalized additive function).

Ultimately, one would expect the study of quotient groups of $\mathbb{Q}^*$ to embrace integration over appropriate subgroups of the dual group of $\mathbb{Q}^*$.

An extensive survey of problems and results attached to many dimensional product representations of rationals by the values of polynomials on the integers or on the primes, together with a discussion of their attendant groups and $\mathbb{Q}^*$-character sums, may be found in [**18**].

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press

Acknowledgements. We thank the referee for a careful reading of the text and have implemented as many of their suggestions as exigencies of publication will allow.

References

1. P. Berrizbeitia and P. D. T. A. Elliott, On products of shifted primes. *Ramanujan J.* **2**(1–2) (1998), 219–223. Paul Erdős memorial volume.

2. J. L. Britton, Solution of the word problem for certain types of groups I. *Proc. Glasgow Math. Assoc.* **3** (1956), 45–54.

3. F. Dress and B. Volkmann, Ensembles d'unicité pour les fonctions arithmétiques additives ou multiplicatives. *C. R. Acad. Sci. Paris Sér. A-B* **287**(2) (1978), A43–A46.

4. P. D. T. A. Elliott, A conjecture of Kátai. *Acta Arith.* **26**(1) (1974/75), 11–20.

5. P. D. T. A. Elliott, The law of large numbers for additive arithmetic functions. *Math. Proc. Cambridge Philos. Soc.* **78**(1) (1975), 33–71.

6. P. D. T. A. Elliott, General asymptotic distributions for additive arithmetic functions. *Math. Proc. Cambridge Philos. Soc.* **79**(1) (1976), 43–54.

7. P. D. T. A. Elliott, Sums and differences of additive arithmetic functions in mean square. *J. Reine Angew. Math.* **309** (1979), 21–54.

8. P. D. T. A. Elliott, *Arithmetic Functions and Integer Products* (*Grundlehren Math. Wiss.* **272**), Springer (New York, 1985).

9. P. D. T. A. Elliott, Multiplicative functions on arithmetic progressions. *Mathematika* **34**(2) (1987), 199–206.

10. P. D. T. A. Elliott, A localized Erdős–Wintner theorem. *Pacific J. Math.* **135**(2) (1988), 287–297.

11. P. D. T. A. Elliott, Multiplicative functions $|g| \leqslant 1$ and their convolutions: an overview. In *Séminaire de Théorie des Nombres, Paris 1987–88* (*Progress in Mathematics* **81**) (ed. C. Goldstein), Birkhäuser (Boston, 1990), 63–73.

12. P. D. T. A. Elliott, On the correlation of multiplicative functions. *Notas Soc. Mat. Chile* **11**(1) (1992), 1–11.

13. P. D. T. A. Elliott, Multiplicative functions on arithmetic progressions. VI. More middle moduli. *J. Number Theory* **44**(2) (1993), 178–208.

14. P. D. T. A. Elliott, On the correlation of multiplicative and the sum of additive arithmetic functions. *Mem. Amer. Math. Soc.* **112**(538) (1994), viii+88.

15. P. D. T. A. Elliott, The multiplicative group of rationals generated by the shifted primes, I. *J. Reine Angew. Math.* **463** (1995), 169–216.

16. P. D. T. A. Elliott, *Duality in Analytic Number Theory* (*Cambridge Tracts in Mathematics* **122**), Cambridge University Press (Cambridge, 1997).

17. P. D. T. A. Elliott, The multiplicative group of rationals generated by the shifted primes, II. *J. Reine Angew. Math.* **519** (2000), 59–71.

18. P. D. T. A. Elliott, Product representations by rationals. In *Number Theoretic Methods: Future Trends, Proceedings of the Second China–Japan Seminar, Iizuka, Japan, March 12–16, 2001* (*Dev. Math.* **8**) (eds S. Kanemitsu and C. Jia), Kluwer Academic Publishers (Dordrecht, 2002), 119–150.

19. P. D. T. A. Elliott, The value distribution of additive arithmetic functions on a line. *J. Reine Angew. Math.* **642** (2010), 57–108.

20. I. Kátai, On sets characterizing number-theoretical functions. *Acta Arith.* **13**(3) (1968), 315–320.

21. J. Meyer, Ensembles d'unicité pour les fonctions additives. Étude analogue dans le cas des fonctions multiplicatives. In *Proceedings of the Journées de Théorie Analytique et Elémentaire des Nombres, Université de Paris-Sud, Orsay, France, June 2–3, 1980*, Vol. 81 (*Publ. Math. Orsay* **1**), Université de Paris-Sud (Orsay, 1981), 19–29.

22. G. Stepanauskas, The mean values of multiplicative functions, V. In *Analytic and Probabilistic Methods in Number Theory, Proceedings of the Third International Conference in Honour of J. Kubilius, Palanga, Lithuania, 24–28 September, 2001* (eds A. Dubrickas, A. Laurinčikas and E. Manstavičius), TEV (Vilnius, 2002), 272–281.

23. J. Stillwell, The word problem and the isomorphism problem for groups. *Bull. Amer. Math. Soc. (N.S.)* **6**(1) (1982), 33–56.

24. T. Tao, The logarithmic averaged Chowla and Elliott conjectures for two-point correlations. *Preprint*, 2015, arXiv:1509.05422v2.

25. D. Wolke, Bemerkungen über Eindeutigkeitsmengen additiver Funktionen. *Elem. Math.* **33**(1) (1978), 14–16.

P. D. T. A. Elliott,
Department of Mathematics,
University of Colorado Boulder,
Boulder, Colorado 80309-0395,
U.S.A.
E-mail: pdtae@euclid.colorado.edu

Jonathan Kish,
Department of Applied Mathematics,
University of Colorado Boulder,
Boulder, Colorado 80309-0526,
U.S.A.
E-mail: jonathan.kish@colorado.edu

https://doi.org/10.1112/S0025579317000304 Published online by Cambridge University Press