数理解析研究所講究録
第 886 巻 1994 年 1-9

The Multiplicative Group of Rationals Generated by the Shifted Primes

P.D.T.A. Elliott (Colorado University, USA)

1. I begin with three conjectures.

Conjecture 1. Every positive rational r has a representation

$$r = \frac{p+1}{q+1}, \quad p, q \text{ prime}.$$

Conjecture 2. There is a k so that every positive rational r has a representation

$$r = \prod_{j=1}^{k} (p_j + 1)^{\varepsilon_j}, \quad p_j \text{ prime}, \ \varepsilon_j = +1 \text{ or } -1.$$

Conjecture 3. Every positive rational r has a representation

$$r = \prod_{j=1}^{k_r} (p_j + 1)^{\varepsilon_j}, \quad p_j \text{ prime}, \ \varepsilon_j = +1 \text{ or } -1.$$

Let Q^* be the multiplicative group of positive rationals, Γ the subgroup generated by the $p+1, p$ prime, $G = Q^*/\Gamma$ the quotient group. Conjecture 3 asserts the triviality of G.

Clearly the validity of Conjecture 1 implies that of Conjecture 2, and so of Conjecture 3. Actually Conjectures 2 and 3 are equivalent, although that is not at all obvious. Moreover, G is known to be finite.

That G is finite follows from early work of Kátai, and Elliott; not realised at the time. A documented account of their results, related results of Elliott, Wirsing, Dress and Volkmann, Wolke, Meyer, and a proof of the equivalence of Conjectures 2 and 3 may be found in Elliott, [2], Chapters 15 and 23.

Let $|H|$ denote the order of a finite group H.

Theorem 1. *There is a positive integer k such that every positive rational r has a representation*

$$r^{|G|} = \prod_{j=1}^{k} (p_j + 1)^{\varepsilon_j}, \quad p_j \text{ prime } \varepsilon_j = +1 \text{ or } -1.$$

Theorem 2. $|G| \leq 4$.

2. The equivalence of Conjectures 2 and 3 obtained in Elliott [2], Chapter 23, elaborates to give Theorem 1. I sketch a proof of Theorem 2 that suggests an approach to a sharper bound.

Let U be the multiplicative group of complex numbers that are roots of unity. Let $\widehat{G}$ be the dual group generated by the group homomorphisms $g : G \to U$. In particular, $|\widehat{G}| = |G|$.

We can extend the definition of a g in $\widehat{G}$ to Q^*, by

$$Q^* \to Q^*/\Gamma \to U,$$

employing the canonical homomorphism from Q^* to G. Thus g is typically a completely multiplicative function, with values in U, and which is identically 1 on the shifted primes.

Let $g_1, \dots, g_t$ be extensions of elements in $\widehat{G}$ (we might view them as characters on Q^*), and define the arithmetic function

$$w(n) = \left| \sum_{j=1}^{t} g_j(n) \right|^2 .$$

For real $x \geq 0$, let

$$S = \sum_{p+1 \leq x} w(p+1).$$

Our hypothesis ensures that

$$S \geq (1 + o(1)) \frac{t^2 x}{\log x}, \quad x \to \infty,$$

and we seek an upper bound for S.

We do not currently possess a method to give sharp upper bounds for sums

$$\sum_{p+1 \leq x} h(p+1),$$

when h is multiplicative, constrained only by $|h(n)| \leq 1$; so we argue indirectly.

Let $1 \leq z \leq x$; R the product of primes not exceeding z; λ_d real numbers for each divisor d of R which does not exceed z, $\lambda_1 = 1$. Following Selberg's sieve method

$$\begin{aligned} S &\leq \sum_{n+1 \leq x} \left(\sum_{d \mid n} \lambda_d \right)^2 w(n+1) + t^2 z \\ &= \sum_{d_1, d_2} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{m \leq x \\ m \equiv 1 \ (\mathrm{mod}\ [d_1, d_2])}} w(m) + \mathit{small}. \end{aligned}$$

Here *small* indicates that we shall choose z so that the missing term is $o(x/\log x)$ as $x \to \infty$. In order to proceed we seek an estimate for

$$\sum_{i,j=1}^{t} \sum_{\substack{m \leq x \\ m \equiv 1 \ (\mathrm{mod}\ D)}} g_i(m) \overline{g_j(m)},$$

with the positive integer D as large as possible compared to x.

Let $0 < \varepsilon < 1/2$. For the moment assume an analogue of the extended Riemann Hypothesis: that for any multiplicative function h with values in the complex unit disc,

$$\sum_{\substack{m\le x\\ m\equiv 1 \pmod D}} h(m) \approx \frac{1}{\phi(D)} \sum_{\substack{m\le x\\ (m,D)=1}} h(m) \approx \frac{1}{D}\sum_{m\le x} h(m),$$

uniformly for D up to $x^{\frac{1}{2}-\varepsilon}$. Here $\approx$ indicates that the difference of the two expressions approximately equated is to have a negligible effect in our subsequent calculations. The second part of the hypothesis, a tricky point, is employed only to simplify the exposition of the argument. Granted a suitable validity to this generalized hypothesis

$$S \le \sum_{d_1,d_2} \frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]} \sum_{m\le x} w(m) + \textit{small}, \ x\to\infty.$$

Quite generally, if the series

$$\sum_p p^{-1}(1-\operatorname{Re} h(p)p^{i\tau}),$$

taken over the prime numbers, diverges for every real τ, then a 1968 theorem of Halász asserts that

$$x^{-1}\sum_{m\le x} h(m) \to 0, \quad x\to\infty.$$

In our case, typically either

$$x^{-1}\sum_{m\le x} g_\ell(m)\overline{g_j(m)} \to 0, \quad x\to\infty,$$

or

$$\sum_p p^{-1}(1-\operatorname{Re} g_\ell(p)\overline{g_j(p)}p^{i\tau}) \tag{1}$$

converges for some real τ. The latter ensures that $g_\ell(m)\overline{g_j(m)}m^{i\tau}$ is 'usually near to 1' on integers m; hence $g_\ell(p+1)\overline{g_j(p+1)}(p+1)^{i\tau}$ is 'usually near to 1. Since every $g_j(p+1)=1$, $1\le j\le t$, $(p+1)^{i\tau}$ is 'usually near to 1. In stages, this forces $\tau = 0$, $g_\ell\bar{g}_j$ near to 1, $g_\ell\bar{g}_j$ identically one. I explicate this part of the argument below.

Accordingly,

$$\sum_{m\le x} w(m) = \sum_{\ell,j=1}^{t}\sum_{m\le x} g_\ell(m)\overline{g_j(m)} = \sum_{\ell=1}^{t} |g_\ell(m)|^2 + o(x), \ x\to\infty,$$

can be assumed.

Following the classical method of Selberg, we choose the λ_d so that

$$\sum_{d_1,d_2}\frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]} \le \frac{1}{\log z}. \tag{2}$$

Altogether

$$S \le \frac{(1+o(1))tx}{\log z}, \quad x \to \infty.$$

The best that we can do with our current hypotheses is set $z^2 = x^{\frac{1}{2}-\varepsilon}$. Since $\varepsilon > 0$ may be otherwise arbitrary,

$$S \le (4t + o(1))\frac{x}{\log x}, \quad x \to \infty.$$

Combining the upper and lower asymptotic bounds for S gives $t^2 \le 4t$, $t \le 4$, $|\widehat{G}| \le 4$. Theorem 2 is so established.

3. How can we obviate our generalized Riemann Hypothesis? The example of h a non-principal Dirichlet character (mod 3) shows that our extended hypothesis is in general false. Disregarding this objection we might try for an analogue of the Bombieri–Vinogradov theorem on primes in arithmetic progression; a result of the form

$$(3) \qquad \sum_{D \le x^{\frac{1}{2}-\varepsilon}} \phi(D) \max_{(r,D)=1} \left| \sum_{\substack{m \le x \\ m \equiv r \ (\mathrm{mod}\ D)}} h(m) - \frac{1}{\phi(D)} \sum_{\substack{m \le x \\ (m,D)=1}} h(m) \right|^2 \ll x^2 (\log x)^{-A},$$

valid for each fixed positive A, would suffice. Standard methods, such as Motohashi, [6], require that the function $h(p)\log p$ satisfy an analogue of the Siegel–Walfisz theorem for primes in arithmetic progression; a condition not necessarily satisfied at the outset of our argument.

In [4], [5], I proved that a general result of the type (3) is available provided that h is replaced by $h - h' - h''$, where $h'(m) \approx h(m)/\log m \approx h(m)/\log x$; $h''(m) \approx$
$h(p)\log p/\log x$, supported on the primes. Thus, besides $w(n)$, we have to consider sums

$$\sum_{\substack{n \le x \\ n \equiv 1 \ (\mathrm{mod}\ D)}} g'_\ell(n)\overline{g_j(n)},$$

and so on. This leads to extra terms. Typically we proceed

$$\begin{aligned}
\left| \sum_{n \le x} \Bigl(\sum_{d|n} \lambda_d \Bigr)^2 g_\ell(n+1)\overline{g''_j(n+1)} \right| &\le \sum_{n \le x} \Bigl(\sum_{d|n} \lambda_d \Bigr)^2 |g''_j(n+1)| \\
&\ll \sum_{p \le x} \Bigl(\sum_{d|(p-1)} \lambda_d \Bigr)^2 \frac{\log p}{\log x} + \mathit{small} \\
&\ll \sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{p \le x \\ p \equiv 1 \ (\mathrm{mod}\ [d_1,d_2])}} \frac{\log p}{\log x} + \mathit{small}.
\end{aligned}$$

To this last multiple sum we apply the standard theorem of Bombieri and Vinogradov, and obtain a bound

$$\ll \frac{x}{\log x} \sum_{d_1,d_2} \frac{\lambda_{d_1}\lambda_{d_2}}{\phi([d_1,d_2])} + \textit{small}. \tag{4}$$

In practice we need to choose the λ_d to make five quadratic forms simultaneously small; the forms appearing in (2) and (4) typical.

Note that the denominator $[d_1, d_2]$ of (2) is replaced by $\phi([d_1, d_2])$ in (4). To allow a choice of the λ_d we take for R not the product of all primes up to z, but the product of all primes in an interval $((\log x)^{c_1}, z]$, where c_1 is a constant, of value about 4. We so reach

$$S \leq \frac{v}{\phi(v)\log z} \sum_{\substack{m \leq x \\ (m-1,v)=1}} w(m) + \textit{small}, \tag{5}$$

where v denotes the product of the omitted primes, those not exceeding $(\log x)^{c_1}$.

4. The integer v in (5) is sufficiently small relative to R that the corresponding condition $(m-1, v) = 1$ can be dealt with directly.

Lemma 1. *Let* $0 < \beta < 1$, $0 < \varepsilon < 1/8$, $2 \leq \log M \leq Q \leq M$. *Then*

$$\sum_{\substack{n \leq x \\ n \equiv r \pmod D}} g(n) = \frac{1}{\phi(D)} \sum_{\substack{n \leq x \\ (n,D)=1}} g(n) + O\left(\frac{x}{\phi(D)} \left(\frac{\log Q}{\log x}\right)^{\frac{1}{8}-\varepsilon}\right)$$

holds for $M^\beta \leq x \leq M$, *all* $(r, D) = 1$, *all* $D \leq Q$ *save possibly for the multiples of a* $D_0 > 1$.

There are absolute constants B, c *and attached to each exceptional modulus a non-principal character* χ *with the following properties: For* $\tau, |\tau| \leq Q^B$,

$$\sum_{Q<p\leq M} p^{-1}(1 - Re\, g(p)\chi(p)p^{i\tau}) < \frac{1}{4} \log\left(\frac{\log M}{\log Q}\right) - c.$$

Moreover, the characters are induced by the same primitive character $(\mathrm{mod}\, D_0)$.

This result is the substance of [3].

We can largely evaluate $w(m)$ over the integers m which satisfy $(m-1, v) = 1$ by means of the representations

$$\sum_{m \leq x} w(m) \sum_{d|(m-1,v)} \mu(d) = \sum_{d|v} \mu(d) \sum_{\substack{m \leq x \\ m \equiv 1 \pmod d}} w(m).$$

The contribution to the double sums arising from those d exceeding $\exp((\log x)^{\varepsilon_0})$ for a small, fixed, positive ε_0, may be neglected. The remaining d give rise to the main term. Effectively we apply Lemma 1 with $Q = \exp((\log x)^{\varepsilon_0})$, so that $(\log Q/\log x)^{1/10} \ll (\log x)^{-(1-\varepsilon_0)/10}$ is suitably small. This introduces a factor

$$\approx \sum_{d|v} \frac{\mu(d)}{d} = \frac{\phi(v)}{v},$$

which cancels the related factor in (5).

The upshot of the argument is a result of the same quality as that which we can achieve by assuming a Riemann Hypothesis analogue for multiplicative functions with values in the complex unit disc.

To improve the bound of Theorem 2 it would suffice to be able to choose a value $z^2 = x^\gamma$ with $\gamma > 1/2$. To this end we might treat the error term in the application of Selberg's sieve with more care.

The foregoing is an abbreviated account of the lecture with which I opened the conference in Analytic Number Theory, held at the Institute of Mathematics, Kyoto, Japan, in October 19–22, 1993.

In the following sections I substantiate the sketched steps.

5. A valid version of (3) is established as Lemma 6 of [5].

Let g be multiplicative, with values in the complex unit disc. Define an exponentially multiplicative function g_1 by $g_1(p^k) = g(p)^k/k!$, $k = 1, 2, 3, \ldots$; and the multiplicative h by convolution: $g = h * g_1$.

For $B \geq 0$ define

$$\beta_1(n) = \sum_{\substack{ump=n \\ u \leq (\log x)^B \\ p \leq b}} \frac{h(u)g_1(m)g(p)\log p}{\log mp}, \quad \beta_2(n) = \sum_{\substack{urp=n \\ u \leq (\log x)^B \\ r \leq b}} \frac{h(u)g_1(r)g(p)\log p}{\log rp},$$

and set $\beta(n) = g(n) - \beta_1(n) - \beta_2(n)$.

Lemma 2. *Let $B \geq 0$, $A \geq 0$, $b = (\log x)^{6A+15}$, $0 < \delta < 1/2$. Then*

$$\sum_{D_1 D_2 \leq x^\delta} \max_{(r, D_1 D_2)=1} \left| \sum_{\substack{n \leq x \\ n \equiv r \pmod{D_1 D_2}}} \beta(n) - \frac{1}{\phi(D_2)} \sum_{\substack{n \leq x, (n, D_2)=1 \\ n \equiv r \pmod{D_1}}} \beta(n) \right|$$

$$\ll x(\log x)^{-A}(\log\log x)^2 + \omega^{-1} x(\log x)^{2A+8}(\log\log x)^2 + \omega^{-1/2} x (\log x)^{5/2} \log\log x$$

$$+ x(\log x)^{\frac{1}{2}(5-B)},$$

where D_1 is confined to those integers whose prime factors do not

exceed ω, and D_2 to integers whose prime factors exceed ω. The implied constant depends at most upon A, B.

In the argument following (3) the rôles of h', h'' are played by β_1, β_2 respectively. An appropriate application of Lemma 2 is embodied in the following result, which is a particular case of [5], Lemma 7.

Lemma 3. *In the notation of Lemma 2 set* $B = 2A + 5$. *Let* $(\log x)^{3A+8} \le \omega \le \exp(\sqrt{\log x})$. *Let* P *be a product of primes which do not exceed* ω. *Then*

$$\sum_{\substack{D \le x^{\delta} \\ p|D \Rightarrow p > \omega}} \left| \sum_{\substack{n \le x, (n-1,P)=1 \\ n \equiv 1 \pmod D}} \beta(n) - \frac{1}{\phi(D)} \sum_{\substack{n \le x, (n-1,P)=1 \\ (n,D)=1}} \beta(n) \right| \ll x(\log x)^{1-A}.$$

In our application of Lemma 3, $P = v$.

In the application of Lemma 1 to the estimation of

$$\sum_{\substack{n \le x \\ (n-1,P)=1}} g(n)$$

It may be necessary to separate off terms of the form

$$\frac{\phi(P)}{P} \frac{\mu(D_0)}{D_0} \prod_{p|D_0} \left(1 - \frac{2}{p}\right)^{-1} \sum_{\substack{n \le x \\ n \text{ odd}}} \chi(n) g(n) \prod_{p|n} \left(\frac{p-1}{p-2}\right).$$

A detailed example of such a procedure occurs in Lemma 11 of [5]. As a consequence, the convergence of the sum (1) is replaced by that of

$$\sum_p p^{-1}(1 - \operatorname{Re} g_\ell(p)\overline{g_j(p)}\chi(p)p^{i\tau}) \tag{6}$$

for a Dirichlet character χ.

6. To deduce the coincidence of the characters g_j, g_ℓ from the convergence of the series (6), the following suffices.

Lemma 4. (Proximity Lemma) *Let* g *be a character on* Q^*. *Suppose that for some Dirichlet character* χ *and real* τ *the series*

$$\sum p^{-1}|1 - g(p)\chi(p)p^{i\tau}|^2,$$

taken over the prime numbers, converges. Suppose further that $g(p+1) = 1$ *for all sufficiently large primes. Then* g *is identically 1.*

Proof. For any unimodular complex number α, and positive integer m, $|1 - \alpha^m| \le m|\alpha - 1|$. If χ has order m, then the series

$$\sum p^{-1}|1 - g(p)^m p^{mi\tau}|^2$$

also converges. This is the particular case with χ replaced by the identity.

If $0 < \varepsilon < 1$, then $\sum q^{-1}$, taken over the primes q for which $|g^m(q)q^{i\tau - 1}| > \varepsilon$, converges. Given $\eta > 0$, there is a prime p in the interval $(x, x(1+\eta)]$, such that $(p+1)/2$ has at most c prime factors, none of them an exceptional q. Here c is independent of ε and η, although x may need to be sufficiently large in terms of ε, η. That there are many suitable primes p can be shown using sieve methods, as in [1]; see also [2], Chapter 12, Chapter 23, problem 62. Since $g(p+1) = 1$,

$$\overline{g(2)^m} = g\left(\frac{p+1}{2}\right)^m = \left(\frac{p+1}{2}\right)^{i\tau} + O(\varepsilon) = \left(\frac{x}{2}\right)^{i\tau} + O(\varepsilon + \eta),$$

and $x^{i\tau} = 2^{i\tau}\overline{g(2)^m} + O(\varepsilon + \eta)$. If τ is non-zero, then the choice $x = \exp(2\pi n\tau^{-1} + 2\pi\alpha)$ with α real, $n = 1, 2, \ldots$, gives $x^{i\tau} \to e^{2\pi i\tau\alpha}$. Letting $\eta \to o+$, $\varepsilon \to o+$ we see that $e^{2\pi i\tau\alpha} = 2^{i\tau}\overline{g(2)^m}$ is valid for all real α. The choice $\alpha = 0$ shows that the right hand side of this equation is 1. Another suitable value for α gives $\tau = 0$, and a contradiction.

Thus $\tau = 0$. Let χ be a character (mod δ). Let D be a positive integer. We can carry out a similar application of sieves to get a representation $p + 1 = 2Dr$ where r has again a bounded number of prime factors, none of which is a q for which $|\chi(q)g(q) - 1| > \varepsilon$. Then

$$\begin{aligned} 1 &= g(p+1) = g(2D)g(r) = g(2D)(\chi(r) + O(\varepsilon)) \\ &= g(2D)\chi\left(\frac{p+1}{2D}\right) + O(\varepsilon). \end{aligned} \tag{7}$$

If $(2Dt - 1, \delta) = 1$ for some integer t, then $(2Dt - 1, 2D\delta) = 1$. If, further, $(t, \delta) = 1$, then we can demand that the prime p in (7) satisfy $p \equiv 2Dt - 1 \pmod{2D\delta}$. The conditions on t allow Dirichlet's theorem on primes in arithmetic progression to be applied. For such primes, $(p+1)/(2D)$ will have the form $(2D)^{-1}(2Dt + 2Dm\delta) = t + m\delta$ for some integer m. Letting $\varepsilon \to o+$ then gives $1 = g(2D)\chi(t)$.

If a further integer D_1 satisfies $D_1 \equiv D \pmod{\delta}$ then *for the same* t, $(2D_1t - 1, \delta) = 1$. Hence $1 = g(2D_1)\chi(t)$ as well. The value of $g(D + m\delta)$ is independent of m. From [2], Chapter 19, Lemma 19.3, g is a Dirichlet character (mod δ) on the integers prime to δ.

In order for g to be a Dirichlet character (mod δ) on the integers prime to δ it will therefore suffice to find a t such that $(t(2Dt-1), \delta) = 1$. Let $\delta = 2^\nu\delta_1$ where δ_1 is odd. Then $(2Dt - 1, \delta) = (2Dt - 1, \delta_1)$. We can solve $2Dt \equiv 2 \pmod{\delta_1}$ and the t will automatically satisfy $(t, \delta_1) = 1$. If t is odd, then $(t, \delta) = 1$. If t is even, then $t + \delta_1$ will be odd, $(t + \delta_1, \delta) = 1$.

Insofar as it can be, g is a Dirichlet character (mod δ).

We mop up. Given any D prime to δ, there are infinitely many primes p for which $p + 1 = 2\delta Dm$, $m \equiv 1 \pmod{\delta}$. This only needs $p \equiv -1 + 2\delta D \pmod{2\delta^2 D}$. For all large enough such primes

$$1 = g(p+1) = g(2\delta D)\chi(1) = g(2\delta D).$$

Therefore $g(D)g(2\delta) = 1$. The choice $D = 1$ shows that $g(2\delta) = 1$. Hence $g(D) = 1$ for all D prime to δ.

Given any positive D, an infinity of primes p for which $p+1 = 2Dm$ with $(m, \delta) = 1$ can be arranged. Then $1 = g(p+1) = g(2D)g(m) = g(2D)$. The choice $D = 1$ shows that $g(2) = 1$. Therefore $g(D) = 1$ for all $D \geq 1$.

A careful examination of this proof shows that g need not be completely multiplicative. It will suffice that it satisfy the standard condition: $g(ab) = g(a)g(b)$ whenever $(a, b) = 1$.

7. The argument sketched in the lecture may be applied to the more general sums

$$\sum_{p+1\leq x} \left| \sum_{j=1}^{t} z_j g_j(p+1) \right|^2, \quad z_j \in \mathbb{C},$$

and their duals:

$$\sum_{j=1}^{t} \left| \sum_{p+1\leq x} g_j(p+1) y_p \right|^2, \quad y_p \in \mathbb{C}.$$

A (somewhat lengthy) further argument then removes the need for Lemma 4. This allows an interesting weakening of the hypothesis in Theorem 2. Let P be a collection of primes for which

$$\limsup_{x\to\infty} \frac{\log x}{x} \sum_{\substack{p\leq x \\ p\in P}} 1 = 1.$$

Then the group G_1, defined in a manner analogous to G but employing only the shifted primes $p+1$ with p in P, also satisfies $|G_1| \leq 4$.

References

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

[2] ______________. *Arithmetic Functions and Integer Products*, Grund. der math. Wiss. **272**, Springer–Verlag, New York, Berlin, Heidelberg, Tokyo, 1985.

[3] ______________. Multiplicative functions on arithmetic progressions VI: More Middle Moduli, *Journal of Number Theory*.

[4] ______________. Additive functions on shifted primes, *Bulletin (New Series) of the American Mathematical Society*, **27** (2) (1992), 273–278.

[5] ______________. The concentration function of additive functions on shifted primes; to appear in *Acta Math.*, Mittag Leffler, 1994.

[6] Motohashi, Y. An induction principle for the generalization of Bombieri's prime number theorem, *Proc. Japan. Acad.* **52** (1976), 273–275.

Boulder, January 1994