<table>
<thead>
<tr>
<th>Title</th>
<th>The Multiplicative Group of Rationals Generated by the shifted Primes (Analytic Number Theory)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Elliott, P.D.T.A.</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (1994), 886: 1-9</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1994-09</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/84319">http://hdl.handle.net/2433/84319</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
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

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

Conjecture 3. Every positive rational $r$ has a representation

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

Let $Q^*$ be the multiplicative group of positive rationals, $\Gamma$ 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

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

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 $\hat{G}$ be the dual group generated by the group
homomorphisms $g : G \to U$. In particular, $|\hat{G}| = |G|$. We can extend the definition of a $g$ in $\hat{G}$ 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 $g_1, \ldots, g_t$ be extensions of elements in $\hat{G}$ (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 $z$; $\lambda_d$ real numbers for each divisor $d$ of $R$ which does not exceed $z$, $\lambda_1 = 1$. Following Selberg's sieve method

$$ S \leq \sum_{n+1 \leq x} \left( \sum_{d|n} \lambda_d \right)^2 w(n+1) + t^2 z \leq \sum_{d_1,d_2} \lambda_{d_1} \lambda_{d_2} \sum_{m \leq x, m \equiv 1 (\mod \{d_1,d_2\})} w(m) + \text{small}. $$

Here $\text{small}$ 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

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

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

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

$$\sum_{m \leq x \atop m \equiv 1 \pmod{D}} h(m) \approx \frac{1}{\varphi(D)} \sum_{m \leq x \atop (m, D) = 1} h(m) \approx \frac{1}{D} \sum_{m \leq x} h(m),$$

uniformly for $D$ up to $x^{1-\epsilon}$. 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

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

Quite generally, if the series

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

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

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

In our case, typically either

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

or

(1)

$$\sum_p p^{-1} (1 - \text{Re} g\ell(p) \overline{g_j(p)} p^{i\tau})$$

converges for some real $\tau$. 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 $g_j(p+1) = 1, 1 \leq j \leq t$, $(p+1)^{i\tau}$ is 'usually near to 1. In stages, this forces $\tau = 0, g\ell \overline{g_j}$ near to 1, $g\ell \overline{g_j}$ identically one. I explicate this part of the argument below.

Accordingly,

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

can be assumed.

Following the classical method of Selberg, we choose the $\lambda_d$ so that

(2)

$$\sum_{d_1, d_2} \frac{\lambda_{d_1} \lambda_{d_2}}{[d_1, d_2]} \leq \frac{1}{\log z}.$$
Altogether

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

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

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

Combining the upper and lower asymptotic bounds for $$S$$ gives $$t^2 \leq 4t, \ t \leq 4, \ |\hat{G}| \leq 4$$. 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

$$(3) \quad \sum_{D \leq x^{1-\epsilon}} \phi(D) \max_{(r,D)=1} \left| \sum_{m \leq x, (m,D)=1} h(m) - \frac{1}{\phi(D)} \sum_{m \leq x} h(m) \right|^2 \ll x^2 (\log x)^{-A},$$

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

$$\sum_{n \leq x, n \equiv 1 (mod D)} g_{\ell}'(n) \overline{g_{j}'(n)},$$

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

$$\left| \sum_{n \leq x, (d | n)} \left( \sum_{d | n} \lambda_d \right)^2 g_{\ell}'(n+1) \overline{g_{j}'(n+1)} \right| \leq \sum_{n \leq x} \left( \sum_{d | n} \lambda_d \right)^2 |g_{\ell}'(n+1)| \ll \sum_{p \leq x} \left( \sum_{d | (p-1)} \lambda_d \right)^2 \frac{\log p}{\log x} + \text{small}$$

$$\ll \sum_{d_1, d_2} \lambda_{d_1} \lambda_{d_2} \sum_{p \leq x, p \equiv 1 (mod [d_1, d_2])} \frac{\log p}{\log x} + \text{small}.$$
To this last multiple sum we apply the standard theorem of Bombieri and Vinogradov, and obtain a bound

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

In practice we need to choose the $\lambda_d$ 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 $\lambda_d$ 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

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

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 $0 < \beta < 1$, $0 < \epsilon < 1/8$, $2 \leq \log M \leq Q \leq M$. Then

$$ \sum_{n \equiv T (\text{mod } D)} g(n) = \frac{1}{\phi(D)} \sum_{n \leq x, (n, D) = 1} g(n) + O \left( \frac{x}{\phi(D)} \left( \frac{\log Q}{\log x} \right)^{1-\epsilon} \right) $$

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 $\chi$ with the following properties: For $r, |r| \leq Q^B$,

$$ \sum_{Q < p \leq M} p^{-1} (1 - \text{Reg}(p) \chi(p)p^r) < \frac{1}{4} \log \left( \frac{\log M}{\log Q} \right) - c. $$

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

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

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

The contribution to the double sums arising from those $d$ exceeding $\exp((\log x)^{\epsilon_0})$ for a small, fixed, positive $\epsilon_0$, may be neglected. The remaining $d$ give rise to the main term. Effectively we apply Lemma 1
with $Q = \exp((\log x)^{\epsilon_{O}})$, so that $(\log Q/\log x)^{1/10} \ll (\log x)^{-1/10 - \epsilon_{O}}$ 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 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

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

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

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

$$\sum_{D_1, D_2 \leq x^\delta} \max_{(r, D_1D_2) = 1} \sum_{n \equiv r \pmod{D_1D_2}} \beta(n) - \frac{1}{\phi(D_2)} \sum_{n \equiv r \pmod{D_1}} \beta(n) \ll x(\log x)^{-A} (\log \log x)^2 + \omega^{-1} x(\log x)^{2A+8} (\log \log x)^2 + \omega^{-1/2} x(\log x)^{5/2} \log \log x$$

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

where $D_1$ is confined to those integers whose prime factors do not exceed $\omega$, and $D_2$ to integers whose prime factors exceed $\omega$. The implied constant depends at most upon $A, B$.

In the argument following (3) the roles of $h', h''$ are played by $\beta_1, \beta_2$ 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 $(\log x)^{3A+8} \leq \omega \leq \exp(\sqrt{\log x})$. Let $P$ be a product of primes which do not exceed $\omega$. Then

$$\sum_{D \leq \delta^4} \left| \sum_{n \leq \varepsilon(n-1,p) = 1 \mod (n,D)} \beta(n) - \frac{1}{\phi(D)} \sum_{n \leq \varepsilon(n-1,p) = 1} \beta(n) \right| \ll x(\log x)^{1-A}.$$

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

In the application of Lemma 1 to the estimation of

$$\sum_{n \leq \varepsilon \mod (n-1,p) = 1} g(n)$$

It may be necessary to separate off terms of the form

$$\frac{\phi(P)}{P} \frac{\mu(D_0)}{D_0} \prod_{p \mid D_0} \left( 1 - \frac{2}{p} \right)^{-1} \sum_{n \leq \varepsilon \ mod \ n \ odd} \chi(n)g(n) \prod_{p \mid n} \left( \frac{p-1}{p-2} \right).$$

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

(6) $$\sum_p p^{-1}(1 - \text{Re} \ g(p)\overline{g_j(p)}\chi(p)p^{i\tau})$$

for a Dirichlet character $\chi$.

6. To deduce the coincidence of the characters $g_j, g_\ell$ 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 $\chi$ and real $\tau$ 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 $\alpha$, and positive integer $m$, $|1 - \alpha^m| \leq m|\alpha - 1|$. If $\chi$ has order $m$, then the series

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

also converges. This is the particular case with $\chi$ replaced by the identity.

If $0 < \epsilon < 1$, then $\sum q^{-1}$, taken over the primes $q$ for which $|g^m(q)q^{m\tau-1}| > \epsilon$, 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 \( \varepsilon \) and \( \eta \), although \( x \) may need to be sufficiently large in terms of \( \varepsilon, \eta \). 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 \( g(p + 1) = 1, \)

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

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

Thus \( \tau = 0 \). Let \( \chi \) be a character \( (\mod \delta) \). 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

\[
1 = g(p + 1) = g(2D)g(r) = g(2D)(\chi(r) + O(\varepsilon))
\]

(7)

\[
g = g(2D)\chi \left( \frac{p + 1}{2D} \right) + O(\varepsilon).
\]

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 \( \varepsilon \to 0+ \) 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 \( (\mod \delta) \) on the integers prime to \( \delta \).

In order for \( g \) to be a Dirichlet character \( (\mod \delta) \) on the integers prime to \( \delta \) it will therefore suffice to find a \( t \) such that \( (t(2Dt - 1), \delta) = 1 \). Let \( \delta = 2^m \delta_1 \) where \( \delta_1 \) 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 \( (\mod \delta) \).

We mop up. Given any \( D \) prime to \( \delta \), 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 \( \delta \).
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

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

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


Boulder, January 1994