ACTA ARITHMETICA
LXXXVIII.1 (1999)

Products of shifted primes: Multiplicative analogues of Goldbach's problem

by

P. D. T. A. ELLIOTT (Boulder, Colo.)

1. I begin with

CONJECTURE I. *If N is a sufficiently large positive integer, then every rational r/s with $1 \le r \le s \le \log N$, $(rs, N) = 1$, has a representation of the form*

$$\frac{r}{s} = \frac{N-p}{N-q}, \quad p, q \text{ prime},\ p < N,\ q < N.$$

The case $r = 1$ is equivalent to solving $(s-1)N = sx - y$ in positive primes x, y not exceeding N. Goldbach's problem is to correspondingly solve $N = x + y$.

CONJECTURE II. *There is a positive integer k so that in the above notation and terms there are representations*

$$\frac{r}{s} = \prod_{i=1}^{k} (N - p_i)^{\varepsilon_i}, \quad \varepsilon_i = +1 \text{ or } -1,$$

with the primes p_i not necessarily distinct.

CONJECTURE III. *There are representations of this type, but with the number, k, of factors needed possibly varying with r and s.*

An ideal method? Consider first the problem of representing 2 in the form $(p+1)(q+1)^{-1}$ with primes p, q, an analogue of the prime-pair problem.

Let Q^* denote the multiplicative group of positive rationals. The dual group $\widehat{Q^*}$ may be identified with the (direct) product of denumerably many copies of $\mathbb{R}/\mathbb{Z}$. It is rather "large". A typical character $g : Q^* \to U$ (-nit circle in $\mathbb{C}$) is, in classical parlance, a unimodular complex-valued completely multiplicative arithmetic function. There is a translation invariant Haar measure $d\mu(g)$ on $\widehat{Q^*}$ that assigns to the whole (compact) group measure 1.

1991 *Mathematics Subject Classification*: Primary 11N05; Secondary 11N99, 11L99.
Partially supported by NSF contract DMS 9530690.

We choose a weight w_p so that $S(g) = \sum w_p g(p+1)$, taken over all primes p, converges absolutely, uniformly for g in $\widehat{Q^*}$. Then there is a representation

$$\sum_{2=(p+1)/(q+1)} w_p \overline{w}_q = \int_{\widehat{Q^*}} g(2)|S(g)|^2\, d\mu(g).$$

To study the Goldbach analogue in Conjecture I we replace Q^* by Q_1, the group generated by the primes p not exceeding N, $(p,N) = 1$, and $S(g)$ by $\sum g(N-p)$ taken over the same primes. We may naturally restrict $d\mu(g)$ to $\widehat{Q}_1$, and $\int_{\widehat{Q}_1} g(2)|S(g)|^2\, d\mu(g)$ represents the number of solutions to $2 = (N-p)(N-q)^{-1}$, $p, q \le N$, $(pq, N) = 1$. In standard notation, $\widehat{Q}_1$ is $(\mathbb{R}/\mathbb{Z})^{\pi(N)-\omega(N)}$; convergence properties are not needed, but an explicit dependence of the integral upon the parameter N is introduced.

Consider the analogous representation in the Hardy–Littlewood circle method. There the rôle of Q_1 is played by $\mathbb{Z}$. $\widehat{\mathbb{Z}}$ may be identified with $\mathbb{R}/\mathbb{Z}$, and a typical character g_α on $\mathbb{Z}$ is given by $n \mapsto \exp(2\pi i\alpha n)$, where $\alpha \pmod 1$ is fixed. If $Y(\alpha) = \sum \exp(2\pi i\alpha p)$, taken over the primes $p \le N$, then $\int_{\widehat{\mathbb{Z}}} \exp(-2\pi i\alpha N) Y(\alpha)^2\, d\alpha$ is the number of solutions to $N = p+q$, with p, q prime.

We cannot currently estimate this integral satisfactorily, but its analogue with $Y(\alpha)^3$ in place of $Y(\alpha)^2$ we can. Following the standard procedure the interval $[0,1)$ (i.e., the group $\widehat{\mathbb{Z}}$) is decomposed into *major* and *minor arcs*. The *major arcs* are (small) intervals around rationals $ak^{-1} \pmod 1$, with $(a,k) = 1$, k "small compared to N". To view this group-theoretically, define a (translation invariant) metric σ on $\widehat{\mathbb{Z}}$ by $\sigma(g_\alpha, g_\beta) = \|\alpha - \beta\| = \min|\alpha - \beta - m|$, the minimum taken over all integers m. The major arcs are then the union of spheres $(g; \sigma(g, g_t) \le \delta)$ around characters g_t with t rational, of small denominator k. In particular $g_r^k = 1$, i.e. the characters g_r are *of order low compared to* N.

What remains of $\widehat{\mathbb{Z}}$ is called the *minor arcs*.

For groups other than $\mathbb{Z}$ in the present account I propose to replace *arcs* in corresponding definitions by *cells*.

Can we similarly decompose $\widehat{Q}_1, \widehat{Q^*}$? The decomposition of $\widehat{\mathbb{Z}}$ in the circle method varies according to the problem at hand. For $\widehat{Q}_1$ and problems involving shifted primes the following suggests itself.

Define a (translation invariant) metric ϱ on $\widehat{Q}_1$ by

$$\varrho(g,h) = \Big(\sum_{\substack{p \le N \\ (p,N)=1}} \frac{1}{p} |g(p) - h(p)|^2 \Big)^{1/2}.$$

For major cells we take the *tubular neighbourhoods* (“*worms*”):

$$(g;\ \inf_{|\tau|\le T} \varrho(g, h_\tau) \le \delta)$$

where h_τ is the completely multiplicative function given by $h_\tau(q) = q^{i\tau}\chi(q)$ for a real τ, and primitive Dirichlet character χ. Strictly speaking a Dirichlet character $\chi \pmod D$ does not belong to $\widehat{Q}_1$ so, contrary to classical practice, we define χ to be 1 on the primes dividing D.

That χ be primitive corresponds to the restriction $(a, k) = 1$ in the circle method. We would expect the order of χ (and the value of T) to be small compared to N. In a later section I show that under favourable circumstances these worms may be replaced by ϱ-spheres about (modified) Dirichlet characters.

What remains of $\widehat{Q}_1$ is called the *minor cells*.

I leave as a (not altogether easy) exercise to the reader that the (modified) Dirichlet characters are everywhere dense in $\widehat{Q}_1$. We shall not explicitly use this fact.

When studying $\widehat{Q^*}$, a family of metrics $(\sum p^{-\lambda}|g(p) - h(p)|^2)^{1/2}$, $\lambda > 1$, seems appropriate.

Major arcs in the circle method. Attached to the major arc about the point $ak^{-1} \pmod 1$ is the asymptotic estimate

$$\frac{1}{\pi(N)} \sum_{p\le N} e^{2\pi i a k^{-1} p} \to \frac{\mu(k)}{\phi(k)}, \qquad N \to \infty, \tag{1}$$

a result depending upon the distribution of primes in residue classes (mod k). For a general g_α in this arc

$$\frac{1}{\pi(N)} \Big| \sum_{p\le N} g_\alpha(p) \Big| \approx \frac{|\mu(k)|}{\phi(k)} \min(1, \pi(N)^{-1}\sigma(g_\alpha, g_{ak^{-1}})^{-1}), \tag{2}$$

where $\approx$ denotes “behaves like”.

Major cells in $\widehat{Q^*}$. It would appear that the multiplicative analogue of the prime p is, for problems of prime pair type, the shifted prime $p+1$. For a primitive Dirichlet character $\chi \pmod k$,

$$\frac{1}{\pi(N)} \sum_{p\le N-1} \chi(p+1) \to \frac{\mu(k)}{\phi(k)}, \qquad N \to \infty.$$

The similarity with (1) is striking.

Major cells in $\widehat{Q}_1$. Attached to a worm about the (primitive) character $\chi \pmod k$ is the estimate

$$\frac{1}{\pi(N)} \sum_{p\le N} \chi(N-p) \to \frac{\mu(k)\chi(N)}{\phi(k)}, \qquad N \to \infty.$$

Generally

$$\frac{1}{\pi(N)}\Big|\sum_{p\le N} g(N-p)\Big| \approx \frac{|\mu(k)\chi(N)|}{\phi(k)\sqrt{1+\tau^2}}\exp\big(-\tfrac{1}{2}\varrho^2(g,h_\tau)\big).$$

Compared to (2), $|S(g)|$ peaks very much less violently, indeed it falls only slowly away from an extremum. As with the circle method, we might accelerate the process by considering powers $|S(g)|^{2m}$, $m\ge 1$. This amounts to seeking a representation of the form

$$2=\prod_{i=1}^{m}(N-p_i)\prod_{j=1}^{m}(N-q_j)^{-1}.$$

We might also replace $\widehat{Q}_1$ by $(\mathbb{C}^*)^{\pi(N)-\omega(N)}$, i.e. allow $g(p)=z_p$ complex and non-zero, and work in terms of many complex variables z_p.

Vinogradov effected his proof of Goldbach's conjecture for (sufficiently large) odd numbers by providing a non-trivial upper bound for $Y(\alpha)$ on the minor arcs.

A satisfactory bound for $S(g)$ on the minor cells of $\widehat{Q}_1$ is still wanting. To establish anything non-trivial at the moment we need not only that g not lie in any (low-order worm) of the major cells, but that g^2, g^3 not lie there either. Since there are $3^{\pi(N)-\omega(N)}$ characters $g: Q_1\to U$ which satisfy $g^3=1$, there is at present a (corresponding) "third region" of $\widehat{Q}_1$ in which g is between the major and the (reliably) minor cells.

In the following sections I show that something can still be done, although for the moment I abandon control on the number of factors in the representing product and aim at Conjecture III.

2. I give the notation again. Let $0<\delta\le 1$, N a positive integer, P a set of primes not exceeding N and coprime to N,

$$|P|=\sum_{p\in P}1\ge \delta\pi(N)>0.$$

Let Q_1 be the multiplicative group generated by the positive integers n not exceeding N, $(n,N)=1$, Γ the subgroup of Q_1 generated by the $N-p$ with p in P, G_1 the quotient group Q_1/Γ.

Theorem 1. *If $N\ge N_0(\delta)$, then we may remove a set of primes q, not exceeding N and with $\sum q^{-1}\le c_1(\delta)$, such that G, the subgroup of G_1 generated by the rationals in Q_1 with no q-factor, satisfies*

(i) $|G|\le c_2(\delta)$,
(ii) *there is a subgroup L of G so that G/L is arithmic* (1),
(iii) $|L|\le 4/\delta$.

(1) The term "arithmic" is explained on the next page; see also [2], p. 392.

Conjecture. In (iii) $4/\delta$ should be $1/\delta$. Then $\delta > 1/2$ would force $|L| = 1$, and G itself would be arithmic. We may perhaps view (iii) as *singular integral as geometric obstruction*.

(ii) asserts the existence of a positive integer D and a group homomorphism $(\mathbb{Z}/D\mathbb{Z})^* \to G/L$ which makes the following diagram commute:

$$\begin{tikzcd} & (\mathbb{Z}/D\mathbb{Z})^* \arrow[dr] & \\ Q_3 \arrow[ur] \arrow[rr] & & G/L \end{tikzcd}$$

Here Q_3 is the subgroup of Q_1 when the q-factors are removed, $(D, Q_3) = 1$, $(\mathbb{Z}/D\mathbb{Z})^*$ is the multiplicative group of reduced residue classes $\pmod{D}$, the maps $Q_3 \to (\mathbb{Z}/D\mathbb{Z})^*$, $Q_3 \to G \to G/L$ are canonical. D and the $c_j(\delta)$ may be effectively determined, but not the individual q. We may perhaps view (ii) as *singular series*. It asserts that the representability of an integer by products of the $N-p$ essentially depends upon the residue class $\pmod{D}$ to which it belongs.

Corollary. *If $1 \le r < s \le N$, rs is coprime to N and not divisible by a q, and if $r \equiv s \pmod{D}$, then there is a representation*

$$\left(\frac{r}{s}\right)^{|L|} = \prod_{p \in P} (N-p)^{d_p},$$

with integer exponents d_p.

The proof of Theorem 1 is a little lengthy.

Lemma 1. *Let $c > 0$. If*

$$\sum_{\substack{q \le N \\ (q,M)=1 \\ q\ prime}} \frac{1}{q}(1 - \operatorname{Re} q^{i\tau}) \le \beta \le \tfrac{1}{8} \log\log N,$$

where $|\tau| \le N^c$, $1 \le M \le N^4$, $N \ge e^2$, then

$$\tau \log N \ll e^{\beta}.$$

Proof. Without the condition $(q, M) = 1$, a precise result of this type may be found in [3], Lemma 7.

We make three passes with our argument. Assume first that there is no condition $(q, M) = 1$. Set $\sigma = 1 + (\log N)^{-1}$ and argue with Euler products:

$$|\zeta(\sigma)\zeta(\sigma + i\tau)^{-1}| = \exp\left(\sum_{q \le N} \frac{1}{q^{\sigma}}\ (1 - \operatorname{Re} q^{i\tau}) + O(1)\right) \ll e^{\beta}.$$

Since $\zeta(\sigma+i\tau) \ll |\tau|^{-1} + (\log(2+|\tau|))^{3/4}$ (see [6], Théorème 11.1), and $(\sigma-1)\zeta(\sigma) \to 1$ as $N \to \infty$,

$$\log N \ll (|\tau|^{-1} + (\log N)^{3/4})e^{\beta} \ll |\tau|^{-1}e^{\beta} + (\log N)^{7/8}.$$

This is the first pass.

We restore the condition $(q,M)=1$ and replace the use of $\zeta(s)$ by that of $\zeta(s)\prod_{q|M}(1-q^{-s})$. This leads to a bound

$$\log N \ll \left(\frac{M}{\phi(M)}\right)^2 e^{\beta}(|\tau|^{-1} + (\log(2+|\tau|))^{3/4}).$$

Again the term involving $\log(2+|\tau|)$ may be omitted in favour of $\log N$. In particular, $\tau \ll (\log N)^{-7/8}(\log\log N)^2$. This is our second pass. It allows us to assert that

$$\sum_{q|M} \frac{1}{q}(1-\operatorname{Re} q^{i\tau}) \ll \sum_{q|M} \frac{|\tau|\log q}{q} \ll |\tau|\log\log M \ll (\log N)^{-1/2}.$$

Note that for any $y \ge 2$,

$$\sum_{q|M} \frac{\log q}{q} \ll \sum_{q\le y} \frac{\log q}{q} + \frac{\log y}{y}\sum_{\substack{q|M\\ q>y}} 1 \ll \log y + \frac{\log y}{y}\cdot\frac{\log M}{\log y},$$

and we may set $y = \log M$.

At the expense of replacing β by $\beta + O((\log N)^{-1/2})$ we may remove the condition $(q,M)=1$ from the hypothesis of the lemma and proceed as initially. This is the third pass.

Lemma 2. *Let g_j, $1 \le j \le k$, be multiplicative functions with values in the complex unit disc. The inequality*

$$\sum_{p<N}\Big|\sum_{j=1}^{k} c_j g_j(N-p)\Big|^2 \le \lambda \sum_{j=1}^{k} |c_j|^2,$$

with

$$\lambda = 4\pi(N) + \frac{\gamma_0 N}{\phi(N)\log N}\max_{1\le j\le k}\max_{\chi \,(\mathrm{mod}\, d)}\frac{d}{\phi(d)^2}\sum_{\substack{l=1\\ l\ne j}}^{k}\Big|\sum_{\substack{n<N\\ (n,N)=1}} g_j(n)\overline{g_l(n)}\chi(n)\Big|$$
$$+\, O(N(\log N)^{-21/20})$$

is valid for all complex c_j and all $N \ge e^2$. Here γ_0 is absolute and the innermost maximum runs over the Dirichlet characters to squarefree moduli d.

Proof. This is an analogue of Theorem 3 of [5], and may be obtained in the same way. No doubt a result of this type holds with 1 in place of the leading coefficient 4.

LEMMA 3. *There is a positive c so that*

$$\phi(N)^{-1}\sum_{\substack{n\le N\\(n,N)=1}} g(n)\ll T^{-c}+\exp\Bigg(-c\min_{|\tau|\le T}\sum_{\substack{q\le N\\(q,N)=1\\q\,prime}}\frac{1}{q}(1-\operatorname{Re} g(q)q^{i\tau})\Bigg)$$

uniformly for multiplicative g with values in the complex unit disc, $T\ge 1$, $N\ge e^2$.

Proof. The classical treatment of Halász, [7], needs a modification, such as that carried out in [4], Lemma 12.

3. Proof of Theorem 1, first step. Let U be the complex unit disc. Until further notice χ will revert to its classical meaning.

LEMMA 4. *If $g: Q_1\to Q_1/\Gamma\to U$ extends a character on G_1, then there is an integer m, $1\le m\le 4/\delta$, a Dirichlet character χ to a squarefree modulus d not exceeding a bound depending only upon δ, and a constant γ, also depending at most upon δ, so that*

$$\sum_{\substack{q\le N,\,(q,N)=1\\ \chi(q)g(q)^m\ne 1}}\frac{1}{q}\le\gamma.$$

REMARKS. The exceptional set of primes q may vary with g. The bound $4/\delta$ should no doubt be δ^{-1}.

Proof (of Lemma 4). We obtain upper and lower bounds for

$$S=\sum_{j=1}^{k}\Big|\sum_{p\in P}(g(N-p))^j\Big|^2,$$

where the $N-p$ belong to the set of integers generating Γ.

A lower bound is $k(\delta\pi(N))^2$.

The inequality dual to that in Lemma 2 asserts that

$$\sum_{j=1}^{k}\Big|\sum_{p\le N}a_p g_j(N-p)\Big|^2\le\lambda\sum_{p\le N}|a_p|^2$$

for all complex a_p. Setting $g_j(n)=(g(n))^j$ and choosing the a_p appropriately gives an upper bound $S\le|P|\lambda$. Combined with the lower bound this yields

$$k\delta\le 4+\gamma_1\max_{\chi\,(\mathrm{mod}\,d)}\frac{d}{\phi(d)^2}\sum_{j=1}^{k-1}\frac{1}{\phi(N)}\Big|\sum_{\substack{n<N\\(n,N)=1}}g(n)^j\chi(n)\Big| + O((\log N)^{-1/20}) \tag{3}$$

for an absolute constant γ_1.

Let $0 < 3\varepsilon < \delta$. Replacing δ by $\delta - \varepsilon$ and fixing d_0 at a sufficiently large value in terms of ε allows us to confine the maximum to the range $1 \le d \le d_0$ (still over squarefree moduli).

We estimate the innermost sum of (3) by Lemma 3. Fixing T at a value sufficiently large in terms of ε shows that

$$\begin{aligned} &k(\delta - 2\varepsilon) \\ &\quad \le 4 + \gamma_2 \sum_{j=1}^{k} \exp\Bigg(-c \min_{|\tau| \le T} \min_{\chi \,(\mathrm{mod}\, d)} \sum_{\substack{q \le N \\ (q,N)=1 \\ q \text{ prime}}} \frac{1}{q}(1 - \operatorname{Re} g(q)^j \chi(q) q^{i\tau}) \Bigg) \\ &\qquad + O((\log N)^{-1/20}). \end{aligned}$$

Again γ_2 is absolute.

This inequality holds for all positive integers k.

Denote the double minimum by m_j $(= m_j(T))$. Let B denote the sequence of positive integers j for which $m_j \le M$. This is not the M of Lemma 1. Here

$$k(\delta - 2\varepsilon - \gamma_2 \exp(-cM)) \le 4 + O((\log N)^{-1/20}) + \gamma_2 \sum_{\substack{j=1 \\ m_j \le M}}^{k} 1.$$

Fixing M large enough in terms of ε we see that the sequence B has a lower asymptotic density of at least $\delta - 3\varepsilon$. Let r be the highest common factor of the integers in B. By adjoining 1 to B and using Schnirelmann's addition theorems (cf. [1], Chapter 8; [2], Chapter 22), we see that every sufficiently large integer t has a representation $rt = j_1 + \ldots + j_s$, with r, s bounded in terms of $\delta - 3\varepsilon$.

Since

$$1 - \operatorname{Re} z_1 \ldots z_w \le \sum_{u=1}^{w} w(1 - \operatorname{Re} z_u) \tag{4}$$

for z_u in the unit disc,

$$m_{rt}(sT) = m_{j_1 + \ldots + j_s}(sT) \le s \sum_{u=1}^{s} m_{j_u}(T) \le sM.$$

The inequality

$$\min_{|\tau| \le sT} \min_{\substack{\chi \,(\mathrm{mod}\, d) \\ d \le d_0}} \sum_{\substack{q \le N \\ (q,N)=1 \\ q \text{ prime}}} \frac{1}{q}(1 - \operatorname{Re} g(q)^{rt} \chi(q) q^{i\tau}) \le sM \tag{5}$$

holds for all positive integers t.

There is an integer v, not exceeding $[d_0]!$, for which every χ^v is principal. Replacing rt, τ, s by $rtv, \tau v, v^2 s$ respectively, we may remove the character $\chi(q)$ from the last inequality. In particular

$$\sum_{\substack{q \le N \\ (q,N)=1 \\ q \text{ prime}}} \frac{1}{q}(1 - \operatorname{Re} g(q)^{vrt} q^{i\tau(t)}) \le v^2 sM + v \tag{6}$$

for a certain $\tau(t)$, not exceeding vsT in absolute value, and so bounded in terms of δ, ε.

Since $g(q)^{vrt_1} g(q)^{vrt_2} \overline{g(q)}^{vr(t_1+t_2)} = 1$, we can further argue from (4) that

$$\sum_{\substack{q \le N \\ (q,N)=1 \\ q \text{ prime}}} \frac{1}{q}(1 - \operatorname{Re} q^{iv(\tau(t_1)+\tau(t_2)-\tau(t_1+t_2))}) \le 3v(vsM + 1),$$

uniformly for all positive integers t_j. We are ready to apply Lemma 1, and conclude that for N sufficiently large in terms of δ, ε,

$$\tau(t_1) + \tau(t_2) - \tau(t_1 + t_2) \ll (\log N)^{-1},$$

uniformly in the t_j.

There is now an ω such that $\tau(t) - t\omega \ll (\log N)^{-1}$ for all positive t. This particular result goes back to Exercise 99 (Chapter 3, p. 17) of Pólya and Szegő, [8]. However, in our case the sequence $\tau(t)$ is uniformly bounded in terms of δ, ε. Thus ω must be zero, $\tau(T) \ll (\log N)^{-1}$ uniformly in t.

We return to the inequality (5) and remove the $\tau(t)$:

$$\sum_{\substack{q \le N \\ (q,N)=1 \\ q \text{ prime}}} \frac{1}{q}(1 - \operatorname{Re} g(q)^{vrt}) \ll 1, \tag{7}$$

since

$$\sum_{q \le N} \frac{|q^{i\tau(t)} - 1|}{q} \ll |\tau(t)| \sum_{q \le N} \frac{\log q}{q} \ll 1, \qquad t = 1, 2, \ldots$$

We are nearly there. For $|\theta| \le 1$,

$$\lim_{k \to \infty} \frac{1}{k} \sum_{t=1}^{k} \theta^t = \begin{cases} 1 & \text{if } \theta = 1, \\ 0 & \text{else.} \end{cases}$$

The uniformity of our inequality (7) then shows that

$$\sum_{\substack{q \le N,\, (q,N)=1 \\ g(q)^{vr} \ne 1}} \frac{1}{q} \ll 1,$$

the upper bound depending only upon δ, ε. This is the asserted result save that vr is not explicitly bounded in terms of δ.

Looking back to (3), near the beginning of this lemma, with k chosen so that $k\delta > 4$ we can find an integer j, $1 \le j \le k-1$, for which

$$\frac{1}{\phi(N)}\Big|\sum_{\substack{n<N\\(n,N)=1}} g(n)^j \chi(n)\Big| \ge y_1(\delta, k) > 0.$$

With T, d_1 sufficiently large in terms of y_1,

$$\exp\bigg(-c \min_{d \le d_1} \min_{|\tau| \le T} \sum_{\substack{q \le N\\(q,N)=1}} \frac{1}{q}(1 - \operatorname{Re} g(q)^j \chi(q) q^{i\tau})\bigg) > y_2 > 0.$$

For some d not exceeding $d_1, |\tau| \le T$,

$$\sum_{\substack{q \le N\\(q,N)=1}} \frac{1}{q}(1 - \operatorname{Re} g(q)^j \chi(q) q^{i\tau}) \le y_3(\delta, k).$$

By adjusting y_3 upwards if necessary, we can adjoin the condition $g(q)^{vr} = 1$ to the sum. Raising $g(q)^j \chi(q) q^{i\tau}$ to its vrth power, we see that $\tau \log N \ll 1$. Again we may remove τ:

$$\sum_{\substack{q \le N\\(q,N)=1}} \frac{1}{q}(1 - \operatorname{Re} g(q)^j \chi(q)) \le y_4(\delta, k).$$

If $g(q)^j \chi(q)$ is not 1, then since it is a vrth root of unity,

$$1 - \operatorname{Re} g(q)^j \chi(q) \ge \min_{\substack{(a,b)=1\\2 \le b \le vr}} (1 - \operatorname{Re} \exp(2\pi i a b^{-1})) \ge y_5 > 0.$$

Thus

$$\sum_{\substack{q \le N,\,(q,N)=1\\g(q)^j\chi(q) \ne 1}} \frac{1}{q} \le y_6(\delta, k).$$

We can choose any $k > 4\delta^{-1}$; $k = [4\delta^{-1}] + 1$ will do.

The proof was constructed assuming N to be sufficiently large in terms of δ. For the finitely many remaining values of N Lemma 4 is trivially valid.

4. Proof of Theorem 1, second step. We set out to make the exceptional set of primes q in Lemma 4 uniform in g. The notation of the previous section remains in force.

LEMMA 5. *There is a subgroup G_2 of Q_1/Γ with the property that the primes q taken by the canonical map $Q_1 \to Q_1/\Gamma$ onto any of the cosets* *outside of G_2, have the sum of their reciprocals bounded independently of N. Moreover, the order of G_2 does not exceed a value depending only upon δ.*

Remark. In particular, we may delete the character in Lemma 4, and choose a common value for the powers m, uniform in g.

Let h denote a typical character on $G_1 = Q_1/\Gamma$, and g its extension to Q_1:

$$g : Q_1 \to G_1 \xrightarrow{h} U.$$

If $t_1, \ldots, t_s$ are distinct elements of G_1, and $p \mapsto \overline{p}$ denotes the action of the canonical map $Q_1 \to G_1$, then

$$\sum_{\substack{p<N\\(p,N)=1}} \frac{1}{p}(1 - \operatorname{Re} g(p)\chi(p)) \geq \sum_j \sum_\omega (1 - \operatorname{Re} h(t_j)\omega)\beta_{j,\omega} = L(h,\chi),$$

say, where ω runs through the values assumed by χ, and $\beta_{j,\omega}$ is any real non-negative number not exceeding

$$\sum_{\substack{p<N,\,(p,N)=1\\ \overline{p}=t_j,\,\chi(p)=\omega}} \frac{1}{p}.$$

It will be convenient to choose for $\beta_{j,\omega}$ the minimum of this sum and α, with α to be fixed later. For ease of presentation set $\beta_j = \sum_\omega \beta_{j,\omega}$. Thus

$$0 \leq \beta_j \leq \sum_{\substack{p<N,\,(p,N)=1\\ \overline{p}=t_j}} p^{-1}.$$

In terms of the metric $\varrho(g,h)$ defined on $\widehat{Q}_1$ in Section 1, we have

$$\tfrac{1}{2}\varrho(g,h)^2 = \sum_{\substack{p<N\\(p,N)=1}} \frac{1}{p}(1 - \operatorname{Re} g(p)\overline{h(p)}).$$

For s large enough $L(h,\chi)$ may be considered essentially $\frac{1}{2}\varrho(g,\chi)^2$. We extend ϱ to a metric on $\mathbb{C}^{\pi(N)-\omega(N)}$ and regard $\widehat{Q}_1$ for topological purposes as a subset of $\mathbb{C}^{\pi(N)-\omega(N)}$. This loses us the translation invariance of ϱ on $\widehat{Q}_1$ but allows the choice of a standard Dirichlet character for g,h.

We wish to estimate how often the distances $\varrho(g_i, g_j\chi)$ can be small, for $1 \leq i < j \leq v$, and all (standard) χ to moduli not exceeding d_0, say. We move this question onto $\widehat{G}_1$.

Let μ be the Haar measure on $\widehat{G}_1$, normalised so that $\mu\widehat{G}_1 = 1$.

Lemma 6.

$$\mu\Big(h \in \widehat{G}_1; L(h,\chi) \leq \frac{1}{2}\sum_{j=1}^s \beta_j\Big) \leq 4\Big(\sum_{j=1}^s \beta_j\Big)^{-2} \sum_j \Big|\sum_\omega \omega\beta_{j,\omega}\Big|^2.$$

Proof. Arguing as Chebyshev would, the desired measure does not exceed

$$\mu\Big(h \in \widehat{G}_1; \operatorname{Re} \sum_{j=1}^{s} \sum_{\omega} \omega\beta_{j,\omega} h(t_j) \geq \frac{1}{2} \sum_{j=1}^{s} \beta_j\Big)$$

$$\leq \mu\Big(h \in \widehat{G}_1; \Big| \sum_{j=1}^{s} \sum_{\omega} \omega\beta_{j,\omega} h(t_j)\Big| \geq \frac{1}{2} \sum_{j=1}^{s} \beta_j\Big)$$

$$\leq 4\Big(\sum_{j=1}^{s} \beta_j\Big)^{-2} \int\limits_{h \in \widehat{G}_1} \Big| \sum_{j=1}^{s} \Big(\sum_{\omega} \omega\beta_{j,\omega}\Big) h(t_j)\Big|^2 d\mu(h)$$

$$= 4\Big(\sum_{j=1}^{s} \beta_j\Big)^{-2} \sum_{j=1}^{s} \Big| \sum_{\omega} \omega\beta_{j,\omega}\Big|^2.$$

Let $\theta(\chi)$ denote the upper bound in Lemma 6, and set

$$\theta = \sum_{d \leq d_0} \sum_{\chi \,(\mathrm{mod}\, d)} \theta(\chi),$$

the moduli d assumed squarefree.

Lemma 7 (Well-spaced functions on $\widehat{G}_1$). *If $v^2\theta < 1$, then there are functions h_j, $1 \leq j \leq v$, in $\widehat{G}_1$, such that*

$$L(h_i\overline{h}_k, \chi) \geq \frac{1}{2} \sum_{j=1}^{s} \beta_j \quad \textit{for } 1 \leq i < k \leq v,$$

for every χ (mod d), $d \leq d_0$.

Proof. Any character on G_1 will serve for h_1. Using the translation invariance of Haar measure, the previous lemma guarantees that

$$\mu\Big(h \in \widehat{G}_1; L(h_1\overline{h}, \chi) \leq \frac{1}{2} \sum_{j=1}^{s} \beta_j \text{ for some } \chi \pmod{d},\ d \leq d_0\Big)$$

does not exceed θ. There is an h for which $L(h_1\overline{h}, \chi)$ is suitably large.

We successively remove sets to obtain functions h_i inductively. Having h_i, $1 \leq i \leq k-1$, an h_k may be chosen, so that every $L(h_i\overline{h}_k, \chi)$ is suitably large, by removing from $\widehat{G}_1$ a set of μ-measure at most $(k-1)\theta$.

Since $\theta(1 + 2 + \ldots + v - 1) = \theta\frac{1}{2}(v-1)v \leq v^2\theta < 1$, v steps of this argument are possible.

We return to the group $\widehat{Q}_1$.

Lemma 8 (In a worm is in a sphere). *Suppose $T \leq N$, χ_1, χ_2 are Dirichlet characters of order $\leq b \leq N$, to moduli $\leq N$, and m is a positive integer* *not exceeding N. Then*

$$\varrho(g,\chi_1) \ll \exp(\sqrt{mb}\min_{|\tau|\le T}\varrho(g,\chi_1 p^{i\tau}) + \sqrt{b}\ \varrho(g^m,\chi_2)).$$

Proof. Choose τ to minimize $\varrho(g,\chi p^{i\tau})$ subject to $|\tau|\le T$ (the completely multiplicative function $\chi p^{i\tau}$ has value $\chi(p)p^{i\tau}$ on the prime(s) p), and let δ denote the minimum value. By (4), with the z_j equal,

$$\varrho(g^m,\chi_1^m p^{im\tau}) \le m^{1/2}\varrho(g,\chi_1 p^{i\tau}) = m^{1/2}\delta.$$

By the triangle inequality (ϱ viewed on $\mathbb{C}^{\pi(N)-\omega(N)}$),

$$\varrho(\chi_2,\chi_1^m p^{im\tau}) \le m^{1/2}\delta + \varrho(g^m,\chi_2).$$

If $\overline{\chi}_2\chi_1$ is defined (mod w), then

$$\Big(\sum_{\substack{p<N\\(p,Nw)=1}}\frac{1}{p}|1-\overline{\chi}_2\chi_1^m(p)p^{im\tau}|^2\Big)^{1/2}$$

falls under the same bound. Let $\overline{\chi}_2\chi_1^m$ have order $\varDelta$. Then again by (4),

$$\Big(\sum_{\substack{p<N\\(p,Nw)=1}}\frac{1}{p}|1-p^{im\tau\varDelta}|^2\Big)^{1/2} \le \varDelta^{1/2}(m^{1/2}\delta+\varrho(g^m,\chi_2)).$$

Note that $w\le N^2$, $\varDelta\le b^2$. We may therefore appeal to Lemma 1 of Section 2 and deduce that

$$\begin{aligned} m\tau\varDelta\log N &\ll \exp(\varDelta^{1/2}(m^{1/2}\delta+\varrho(g^m,\chi_2)))\\ &\ll \exp((bm)^{1/2}\delta + b^{1/2}\varrho(g^m,\chi_2)),\end{aligned}$$

provided the final exponent does not exceed $\frac{1}{8}\log\log N$.

Again by the triangle inequality

$$\varrho(g,\chi_1)\le\varrho(g,\chi_1 p^{i\tau})+\varrho(\chi_1 p^{i\tau},\chi_1).$$

The second of the bounding terms is

$$\ll\Big(\sum_{p<N}\frac{1}{p}|p^{i\tau}-1|^2\Big)^{1/2} \ll \Big(|\tau|^2\sum_{p<N}\frac{(\log p)^2}{p}\Big)^{1/2} \ll |\tau|\log N,$$

and the inequality of the lemma follows readily.

Otherwise $(bm)^{1/2}\delta + b^{1/2}\varrho(g^M,\chi_2) > \frac{1}{8}\log\log N$ and the asserted inequality of Lemma 8 is "trivially" valid.

Remark. According to Lemma 4, for each (extended) character g on Q_1, there is an m, $1\le m\le 4/\delta$, and a Dirichlet character χ_2 to a modulus not exceeding a function of δ, so that $\varrho(g^m,\chi_2)\ll 1$, uniformly in g,N. Since the number of possible χ_2 is bounded in terms of δ, we may take the same value of m for all the χ_2. With this value of m, Lemma 8 shows that for *any* χ_1 to a modulus not exceeding N, and of order at most b,

$$\varrho(g, \chi_1) \ll \exp((mb)^{1/2} \min_{|\tau| \le N} \varrho(g, \chi_1 p^{i\tau})).$$

This explains the subtitle of Lemma 8.

We put the results of these last two subsections together. Let $t_1, \ldots, t_s$ be elements in G_1. Suppose that $\theta < 1$, and let $v = [\theta^{-1/2}]$. If $\theta = 0$, then we can choose any positive value for v. Thus $v \ge 1$.

Let $h_1, \ldots, h_v$ be functions in $\widehat{G}_1$, guaranteed by Lemma 7, for which the $L(h_i \overline{h}_k, \chi)$ are large.

Extend the h_i to g_i on Q_1. Then

$$\begin{aligned}\exp\Big((md_0)^{1/2} \min_{|\tau| \le N} \sum_{\substack{p<N \\ (p,N)=1}} \frac{1}{p}(1 - \operatorname{Re} g_i \overline{g}_k \chi_1(p) p^{i\tau})\Big) \\ \gg \sum_{\substack{p<N \\ (p,N)=1}} \frac{1}{p}(1 - \operatorname{Re} g_i \overline{g}_k \chi_1(p)) \\ \gg L(h_i \overline{h}_k, \chi_1) \gg \sum_{j=1}^{s} \beta_j, \quad 1 \le i < k \le v,\end{aligned}$$

for all Dirichlet characters χ_1 to moduli at most d_0 $(\le N)$.

Appeal to Lemma 3 shows that for a certain positive (absolute) constant c,

$$\phi(N)^{-1} \sum_{\substack{n<N \\ (n,N)=1}} g_i \overline{g}_k \chi_1(n) \ll N^{-c} + \Big(\sum_{j=1}^{s} \beta_j\Big)^{-c(md_0)^{-1/2}}$$

uniformly for $1 \le i < k \le v$ and all χ_1 to moduli not exceeding d_0.

We render the exceptional set in Lemma 4 effectively uniform in g by estimating

$$\sum_{j=1}^{v} \Big| \sum_{p \in P} g_j(N-p) \Big|^2$$

from above and below. Again we appeal to the inequality dual to that of Lemma 2. This time

$$\begin{aligned}\delta v \le 4 + O\Big(N^{-c} + \max_{d \le d_0} \max_{\chi \,(\mathrm{mod}\, d)} \Big(\sum_{j=1}^{s} \beta_j\Big)^{-c(md_0)^{-1/2}}\Big) \\ + O(d_0^{-1/2}) + O((\log N)^{-1/20}).\end{aligned}$$

If d_0 is fixed at a value sufficiently large in terms of δ, and θ does not exceed a certain value θ_0, depending only upon δ, then the terms 4 and $O(d_0^{-1/2})$ will together not exceed $\delta v/4$. If N is large enough in terms of δ, then for some χ_1 to a modulus not exceeding d_0, $\sum_{j=1}^{s}\beta_j$ will be bounded in terms of δ alone.

However, $\theta > \theta_0$ entails

$$\Big(\sum_{j=1}^{s}\beta_j\Big)^2 < 4\theta_0^{-1}d_0^2\sum_{j=1}^{s}\Big|\sum_{\omega}\omega\beta_{j,\omega}\Big|^2$$

for some character $\chi \pmod d$, $d \le d_0$. Here $|\omega| \le 1$, $\beta_{j,\omega} \le \alpha$, so that the upper bound does not exceed $r\theta_0^{-1}d_0^2\alpha\sum_{j=1}^{s}\beta_j$. With $\alpha = \theta_0(4d_0^2)^{-1}$, $\sum_{j=1}^{s}\beta_j \le 1$ ensues.

In either case $\sum_{j=1}^{s}\beta_j$ is bounded in terms of δ alone, i.e.

$$\min_{\substack{\chi \,(\mathrm{mod}\, d)\\ d\le d_0}}\sum_{j=1}^{s}\sum_{\omega}\min\Big(\alpha,\sum_{\substack{p<N,\,(p,N)=1\\ \overline{p}=t_j\,,\,\chi(p)=\omega}}\frac{1}{p}\Big) \ll 1,$$

uniformly in s, N.

In our present circumstances we may allow the t_i to run through all the elements of G_1. Those for which the innermost minimum is α are bounded in number in terms of δ alone. They generate a subgroup G_2 of G_1 of order bounded in terms of δ.

For the remaining elements of G_1, which without loss of generality we again enumerate by t_j, $j = 1, 2, \ldots$, we see that

$$\sum_{j=1}^{\infty}\sum_{\substack{p<N,\,(p,N)=1\\ \overline{p}=t_j}}\frac{1}{p} \ll 1.$$

We have reached the following situation:

$$\begin{array}{ccccc}
0 & & 0 & & \\
\downarrow & & \downarrow & & \\
Q_2 & \longrightarrow & G_2 & \longrightarrow & 0\\
\downarrow & & \downarrow & & \\
Q_1 & \longrightarrow & G_1 & \longrightarrow & 0
\end{array}$$

where the vertical maps denote identification, and Q_2 is derived from Q_1 by stripping a set of primes q for which $\sum q^{-1}$ is bounded in terms of δ alone. We have shown that $|G_2| \le c_0(\delta)$ uniformly in N.

This establishes Lemma 5 and part of Theorem 1.

5. Proof of Theorem 1, third step. Arithmicity. We modify the above argument, with $t_1, \ldots, t_s$ running through the elements of G_2, and characters $h : G_2 \to U$ extended canonically and then by projection to $g : Q_1 \to Q_2 \to G_2 \to U$. Thus $g(q) = 1$ on a set of primes q for which $\sum q^{-1}$ converges.

Let H be the subgroup of $\widehat{G}_2$ generated by characters h that extend to a g such that for some Dirichlet character χ, to a modulus not exceeding d_1, $\sum p^{-1}$ taken over the primes $p < N$, $p \mid Q_2$, $g(p)\chi(p) \neq 1$, does not exceed c_1.

LEMMA 9. *If d_1, c_1 are fixed at sufficiently large values, depending at most upon δ, then $|\widehat{G}_2/H| \le 4/\delta$.*

Replacing 4 by 1 in Lemma 2 would replace 4 by 1 here.

Proof. If h_1, h_2 in $\widehat{G}_2$ belong to distinct cosets of H, then the corresponding extensions $g_j : Q_1 \to Q_2 \to G_2 \to U$, $j = 1, 2$, satisfy

$$\sum_{\substack{p<N\\ p\mid Q_2}} \frac{1}{p}(1 - \operatorname{Re} g_1\overline{g}_2\chi(p)) > c_1$$

for all $\chi \pmod d$, $d \le d_1$. Supposing we can find s distinct such coset representatives, then the corresponding s extensions g_j satisfy

$$\begin{aligned} s|P|^2 &= \sum_{j=1}^{s} \Big|\sum_{p\in P} g_j(N-p)\Big|^2 \\ &\le (4 + O((\log N)^{-1/20} + c_1^{-1/md_1}) + O(d_1^{-1/2}))\pi(N)|P|, \end{aligned}$$

where m may be taken to be the same value as earlier provided c_1 is fixed large enough. If d_1, c_1, N are sufficiently large (in terms of δ), then $s \le [4/\delta]$. Here we use the fact that s is an integer. This establishes the lemma.

Let J be the subgroup of G_2 on which H is trivial.

We remove from Q_2 all primes p_1 counted in a sum $\sum p_1^{-1}$, $p_1 < N$, $p \mid Q_2$, $g\chi(p_1) \neq 1$, for some g induced from H. These satisfy

$$\omega_0 \sum \frac{1}{p_1} \le |\widehat{G}_2| c_1 = |G_2| c_1 \le c_3(\delta) < \infty,$$

where

$$\omega_0 = \min_{g\chi(p)\neq 1} (1 - g\chi(p)).$$

Note that g is defined on G_2, so satisfies $g(p)^{|G_2|} = 1$. Since the modulus of χ does not exceed d_1, χ^r is principal for some r not exceeding the least common multiple of the integers up to $[d_1]$. Thus once δ is fixed, $g\chi(p)$

belongs to a fixed set of roots of unity. An explicit lower bound can be given for ω_0, depending upon δ alone.

It is convenient to also remove from Q_2 the primes not exceeding d_1. Call the resulting subgroup of Q_2, Q_3. Let G_3 be the subgroup of G_2 that it generates $\pmod{\Gamma}$.

We reach

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
Q_3 \arrow[r] \arrow[d] & G_3 \arrow[r] \arrow[d] & G_3J/J \cong G_3/L \arrow[d] \\
Q_2 \arrow[r] \arrow[d] & G_2 \arrow[r] \arrow[d] & G_2/J \\
Q_1 \arrow[r] & G_1 &
\end{tikzcd}$$

In this diagram $G_j = Q_j\Gamma/\Gamma$, $j = 2, 3$. By standard theorems in group theory, $G_3J/J \simeq G_3/G_3 \cap J = G_3/L$, say. Note that G_3/L may be viewed as a subgroup of G_2/J. In particular, $|L| = |G_3 \cap J| \le |J|$.

We have defined J so that the upper exact sequence

$$0 \longleftarrow \widehat{G}_2/H \longleftarrow \widehat{G}_2 \longleftarrow H \longleftarrow 0$$

$$0 \longrightarrow J \longrightarrow G_2 \longrightarrow G_2/J \longrightarrow 0$$

is dual to the lower exact sequence, term by term. Therefore $|J| = |\widehat{J}| = |\widehat{G}_2/H| \le 4/\delta$. Hence $|L| \le 4/\delta$.

We prove that G_3/L is arithmic.

Let h be a character on G_3/L. Since U is $\mathbb{Z}$-divisible, there is a character $h' : G_2/J \to U$ which coincides with h on G_3/L. Here we use the identification of G_3/L as a subgroup of G_2/J. We then lift h' up to Q_1 in the natural way:

$$g : Q_1 \to Q_2 \to G_2 \to G_2/J \xrightarrow{h'} U.$$

Since h' belongs to $(G_2/J)^\wedge$, i.e. to H, we may view g as "induced from H".

Attached to g there is a Dirichlet character χ, to a modulus not exceeding d_1, so that g coincides with χ on Q_3. Let D be the product of the primes not exceeding d_1. In the previous statement we may replace χ by the character it induces mod D. (Remember that the χ have squarefree moduli, although the argument could be adjusted if they did not.)

Let σ denote the composition of canonical maps $Q_3 \to G_3 \to G_3/L$.

For integers a, b dividing Q_3, and satisfying $a \equiv b \pmod{D}$, the lifting g satisfies $g(a)\overline{g(b)} = \chi(a)\overline{\chi(b)} = 1$. Otherwise expressed, $h(\sigma(a)/\sigma(b)) = h(\sigma(a))\overline{h(\sigma(b))} = 1$. Since this holds for all characters h on G_3/L, $\sigma(a)/\sigma(b)$ is the identity of G_3/L. The map $a \pmod{D} \to \sigma(a)$

$$\begin{tikzcd} & (\mathbb{Z}/D\mathbb{Z})^* \arrow[dr] & \\ Q_3 \arrow[ur] \arrow[rr, "\sigma"] & & G_3/L \end{tikzcd}$$

is well defined, and gives a commutative diagram of group homomorphisms. G_3/L is arithmic.

With $G = G_3$, Theorem 1 is established.

Proof of the Corollary to Theorem 1. If integers r, s divide Q_3 and satisfy $r \equiv s \pmod{D}$, then r/s in $Q_3 \mapsto 1$ in $(\mathbb{Z}/D\mathbb{Z})^* \mapsto$ identity in G_3/L. Under the canonical map $Q_3 \to G_3$, r/s is taken to an element in L. Therefore $(r/s)^{|L|}$ is taken to the identity of L, and so of G; $(r/s)^{|L|}$ belongs to Γ. In other terms, $(r/s)^{|L|}$ has a product representation of the asserted type.

6. Concluding remarks. Any integer m made up of primes not exceeding N, not dividing N and not among the q, has a representation

$$m^{|G|} = \prod_{p \in P} (N-p)^{e_p}, \tag{8}$$

with the e_p integral. The order of G may also be replaced by $\phi(D)|L|$, with D from the arithmicity condition of G/L.

We can determine an effective upper bound for a set of representatives for G/L in terms of δ and $\sum_{p|N} 1/p$ only. We find D. Given $(s, D) = 1$, a sufficiently strong version of Dirichlet's theorem on primes in arithmetic progression provides that

$$\sum_{\substack{p \le y,\, (p,N)=1 \\ p \equiv s \pmod{D}}} \frac{1}{p} > \frac{2 \log\log y}{3\phi(D)} - \sum_{p|N} \frac{1}{p} > c_1(\delta),$$

for $y \ge y_s = \max\left(c_0, \exp\exp\left(\frac{\phi(D)}{2} \sum_{p|N} \frac{1}{p}\right)\right)$, say. There is a prime $p < y_s$, not dividing N and not a q, which maps onto the class $s \pmod{D}$. By varying s, the arithmicity of G/L guarantees a complete set of representatives for G/L. Note that for a certain constant c_1 depending at most upon δ, $y_s \le \exp(c_1 (\log\log N)^{2\phi(D)})$ uniformly in s.

When P runs through all primes $p < N$, $(p, N) = 1$, we expect there to be no exceptional primes q. There is a reasonable hope that the representatives for G/L determined in the preceding manner all belong to Γ. In that case we could replace $|G|$ in (8) by $|L|$, which would then not exceed 4.

Let $Q(y)$ denote the number of exceptional primes q not exceeding y. From Theorem 1, an integration by parts shows that

$$\int_2^N \frac{Q(y)}{y^2}\,dy \le c_4(\delta) < \infty,$$

uniformly in N. In particular, if $0 < \gamma < 1$,

$$\min_{N^\gamma \le y \le N} \frac{Q(y)\log y}{y} \int_{N^\gamma}^N \frac{dy}{y\log y} \le c_4.$$

The integral is $-\log\gamma$, and for a suitable value of γ, independent of N, $Q(y) < y(4\log y)^{-1}$ for some y in $[N^\gamma, N]$. Then $\left(\frac{1}{2}y, y\right]$ contains at least $y(8\log y)^{-1}$ primes not dividing N, and not among the q. Let m denote their product.

For all sufficiently large N, m will lie in the interval $[\exp(N^\gamma/16), \exp 2N]$. Moreover, since each $N-p$ has at most $c_5 \log N/\log\log N$ distinct prime factors, in any representation of the form (8),

$$\sum_{p\in P} |e_p| \ge |G| y \log\log N (8c_5 \log y \log N)^{-1} > N^\gamma (\log N)^{-2}, \qquad N \ge N_2.$$

The generality of Theorem 1 militates against a reduction in the number of terms in the representing product.

Again let P contain all the primes up to N but not dividing N. To remove the exceptional primes q in Theorem 1 in this case it would suffice to show that given a positive integer d, $(d,N) = 1$, there is a prime p, not exceeding N, such that $p \equiv N \pmod{d}$, $(N-p)d^{-1}$ is not divisible by any q. Since the q might cover all primes in an interval $(N^\varepsilon, N]$, we are essentially to represent N in the form $p+n$ where every prime divisor of n is at most N^ε in size. This is a problem of independent difficulty. Of course we need only solve it for a certain fixed $\varepsilon > 0$, so there is some hope, involving much calculation.

The present paper provides the details to a lecture that I gave as the second plenary address on the first day of the international conference in analytic number theory held in Kyoto, May 19 to 25, 1996. The statement of Theorem 1 is a little complicated, and when P is the set of all primes $p < N$, $(p,N) = 1$, the presence of the exceptional primes q does not seem intrinsic. At the end of that same day, my pleasure at being in Japan combined with jet lag to relax me, and I succeeded in devising a method to remove the exceptional primes. Of the various results possible, the following may be compared with Conjecture III.

THEOREM 2. *There is an integer k so that if $c > 0$, $N > N_0(c)$, then every integer m in the range $1 \le m \le (\log N)^c$, $(m,N) = 1$, has a represen-*

tation

$$m^k = \prod_{p \le N/2} (N-p)^{d_p}$$

with integral exponents d_p.

An explicit value can be given for k.

Although the proof of Theorem 2 proceeds from Theorem 1, considerable further argument is required, and I leave it to another occasion.

It is with great pleasure that I thank the organisers, Professors Hirata-Kohno, Noriko, Motohashi, Yoichi and Murata, Leo, for the invitation to speak at this conference, for the financial help, and for their wonderful hospitality.

References

[1] P. D. T. A. Elliott, *Probabilistic Number Theory I. Mean-Value Theorems*, Grundlehren Math. Wiss. 239, Springer, New York, 1979.
[2] —, *Arithmetic Functions and Integer Products*, Grundlehren Math. Wiss. 272, Springer, New York, 1985.
[3] —, *Additive arithmetic functions on intervals*, Math. Proc. Cambridge Philos. Soc. 103 (1988), 163–179.
[4] —, *The concentration function of additive functions on shifted primes*, Acta Math. 173 (1994), 1–35.
[5] —, *The multiplicative group of rationals generated by the shifted primes*, *I*, J. Reine Angew. Math. 463 (1995), 169–216.
[6] W. J. Ellison et M. Mendès-France, *Les nombres premiers*, Hermann, Paris, 1975.
[7] G. Halász, *Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen*, Acta Math. Acad. Sci. Hungar. 19 (1968), 365–403.
[8] G. Pólya und G. Szegő, *Aufgaben und Lehrsätze aus der Analysis I*, Grundlehren Math. Wiss. 19, Springer, Berlin, 1925.

Department of Mathematics
University of Colorado at Boulder
Campus Box 395
Boulder, Colorado 80309-0395
U.S.A.
E-mail: pdtae@euclid.colorado.edu

Received on 10.11.1997 (3291)