Advanced Studies in Pure Mathematics 49, 2007
Probability and Number Theory — Kanazawa 2005
pp. 69–77

The ramifications of a shift by 2

Peter Elliott

Abstract.

Harmonic analysis and the elementary geometry of Hilbert spaces enable the representation of rationals by quotients of doubly-shifted primes. These representations offer an approach to lower bounds on the gaps between successive primes.

§1. Introduction

If F is a free abelian group, A its subgroup generated by a sequence of elements $a_1, a_2, \ldots$, and B its subgroup generated by the sequence $a_{j+1}a_j^{-1}$, $j = 1, 2, \ldots$, then what is the relation of the quotient group F/B to F/A?

For example, elementary group theory shows that F/B is finite if and only if F/A and A/B are finite. Here A/B is finitely generated, so will be the direct sum of its finite torsion group and of a free group of rank at most 2. In particular, it will be finite if and only if there is a positive integer m so that a_1^m and a_2^m belongs to B.

Whilst every denumerable abelian group has a presentation in the form F/A, there may be differing choices for the elements a_j. Whether some power of a_1 belongs to B need not be at all evident.

The following result shows that with an appropriate choice of the a_j the initial question becomes number-theoretically interesting.

Let $p_1 < p_2 < \cdots$ be the rational primes.

Theorem 1. *There is a positive integer k, so that given any further positive integer t, each positive rational r has a representation*

$$r^k = \prod_{j \in I} \left(\frac{p_{j+2} + 1}{p_j + 1} \right)^{d_j}$$

Received September 10, 2005.
Revised October 30, 2006.
2000 *Mathematics Subject Classification.* Primary 11N99; Secondary 11N05.

where I is a finite set of integers, the exponents d_j are integers, possibly negative, and every prime exceeds t.

I shall show the theorem to be valid for some k not exceeding 8.

Taking logarithms,

$$k \log r \leq \Omega(r,t) \max_{d_j>0} \log\left(\frac{p_{j+2}+1}{p_j+1}\right),$$

where $\Omega(r,t)$ denotes the sum of the positive d_j. Since $\log(1+y) < y$ for positive y,

$$\frac{k\log r}{\Omega(r,t)} \leq \max_{p_i>t}\left(\frac{p_{i+2}-p_i}{p_i}\right).$$

Typically $y = (p_i+1)^{-1}(p_{i+2}-p_i)$, which the prime number theorem shows to approach zero as p_i becomes unbounded. Our replacement of $\log(1+y)$ by y is not too wasteful.

In particular, an upper bound on $\Omega(r,t)$ gives a lower bound on gaps between primes.

A conjecture of Dickson from 1904, [1], would imply that every positive rational has a representation in the form $(q+1)^{-1}(p+1)$ with primes p, q. For example, if we consider the possible primality of $19(q+1)-1$ as q runs through the sequence of primes, then the first occurrence gives $19 = (5+1)^{-1}(113+1)$. Employing telescopes

$$p_j + 1 = \left(\frac{p_j+1}{p_{j-2}+1}\right)\left(\frac{p_{j-2}+1}{p_{j-4}+1}\right)\cdots,$$

together with

$$2+1 = \left(\frac{5+1}{2+1}\right)^{-1}\left(\frac{17+1}{11+1}\right), \quad 3+1 = \left(\frac{5+1}{2+1}\right)^{2},$$

we obtain a representation of the type asserted in the theorem where $r = 19$, $k = 1$, $t = 1$ and $\sum |d_j| = 19$.

The next occurrence gives $19 = (7+1)^{-1}(151+1)$, and the interval $(7, 151)$ contains 31 primes, enabling a single telescope to reach from 151 + 1 to 7 + 1. There is a corresponding representation for 19 of the type in the theorem with $k = 1$, $t = 1$ every $d_j \geq 0$ and $\sum d_j = 16$.

However, trial and error discovers

$$19 = \left(\frac{11+1}{5+1}\right)^{2}\left(\frac{13+1}{7+1}\right)\left(\frac{17+1}{11+1}\right)\left(\frac{19+1}{13+1}\right)\left(\frac{37+1}{29+1}\right)$$

where every exponent is positive and there are only six terms.

From a number-theoretical point of view it is desirable to obtain product representations of the type in the theorem that use as few terms as possible. Once the restriction $p_j > t$ is required, simple telescoping is not adequate to the situation.

I approach the theorem group theoretically. Let Q^* be the multiplicative group of positive rationals, Γ_t the subgroup of it generated by the ratios of shifted primes $(p_j+1)^{-1}(p_{j+2}+1)$, where each p_j exceeds t. In the notation of the introduction, F is Q^* and the rôle of the a_i is played by the p_j+1 with $p_j > t$. The validity of the theorem with $k=1$ would then amount to the assertion that the quotient groups Q^*/Γ_t are all trivial.

Consider a typical group $G = Q^*/\Gamma_t$. We may compose each character on G with the canonical homomorphism $Q^* \longrightarrow Q^*/\Gamma_t$ and obtain a function g with values in the unit circle of the complex plane, satisfying $g(ab) = g(a)g(b)$ for every pair of positive rationals a, b and $g((p_j+1)^{-1}(p_{j+2}+1)) = 1$ if $p_j > t$. This last asserts that for primes $p > t$, $g(p+1)$ is periodic, of period at most 2.

Given k characters on G, with extensions, $g_1, \ldots, g_k$, the points $(g_1(p+1), \ldots, g_k(p+1))$ in $\mathbb{C}^k$ are ultimately periodic. If $(c_1, \ldots, c_k)$ is a further point in $\mathbb{C}^k$, then the inner-product

$$c_1\overline{g_1(p+1)} + \cdots + c_k\overline{g_k(p+1)}$$

is also ultimately periodic, period at most 2.

To continue, we pursue upper and lower bounds on a collection of partially known inner products.

§2. Upper bound

Lemma 1. *The inequality*

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

with

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

holds uniformly for $x \ge 3$, g_j multiplicative functions with values in the complex unit disc, complex c_j, $j = 1, \ldots, k$, The inner maximum runs over Dirichlet characters to squarefree moduli.

Lemma 1 is Theorem 3 of [2]. A version with the constant 4 replaced by another, strictly less than 4, may be derived from Lemma 15 of the same reference. No doubt the constant should be 1, and that would improve the bound $k \leq 8$ attached to the theorem to $k \leq 2$.

Lemma 1 relates the values of a multiplicative function g on the shifted primes to the values on the natural numbers of the multiplicative functions obtained by braiding g with varous Dirichlet characters.

In turn we may relate the values of a multiplicative function on the natural numbers to its values on the primes themselves by a result of Halász, cf. [3], Lemma 6.10.

Lemma 2. *The inequality*

$$x^{-1} \sum_{n \leq x} g(n) \ll T^{-1/4} + \exp\left(-\frac{1}{4} \min_{|\tau| \leq T} \sum_{p \leq x} \frac{1}{p}(1 - Re\, g(p)p^{i\tau}) \right)$$

holds uniformly for all multiplicative functions g with values in the complex unit disc, real $x \geq 2$ and $T \geq 2$. Here τ is confined to real values.

§3. Lower bound

I assume that $\sum_{j=1}^{k} |c_j|^2 = 1$, and introduce a renormalisation

$$\frac{1}{\sqrt{k}}(g_1(p+1), \ldots, g_k(p+1)).$$

Lemma 3. *For any r points ω_j of unit length in a Hilbert space, there is a further unit point z such that*

$$|(z, \omega_j)| \geq \sqrt{2\pi}(3r^{3/2})^{-1}, \qquad j = 1, \ldots, r.$$

The space may be real or complex

The lower bound in this result is not best possible.

As a sample argument consider r points in the real space $\mathbb{R}^t$. Let $Y_1, \ldots, Y_t$ be independent random variables, each normally distributed, mean zero and variance 1. If $\omega_1 = (s_1, \ldots, s_t)$ in a unit point in $\mathbb{R}^t$, then $s_1 Y_1 + \cdots + s_t Y_t$ is also normally distributed, mean zero, variance

$$\sum_{j=1}^{t} var(s_j Y_j) = s_1^2 + \cdots + s_t^2 = 1.$$

For any real $\theta \geq 0$,

$$P(|s_1 Y_1 + \cdots + s_t Y_t| \leq \theta) = \frac{1}{\sqrt{2\pi}} \int_{-\theta}^{\theta} e^{-u^2/2} du \leq \frac{2\theta}{\sqrt{2\pi}}.$$

Arguing simply, for any $w > 0$,

$$P(Y_1^2 + \cdots + Y_t^2 > w) \le w^{-1} E\left(\sum_{j=1}^{t} Y_j^2\right) = w^{-1}t.$$

If $r\theta(2/\pi)^{1/2} + w^{-1}t < 1$, then the unit vector

$$z = (Y_1^2 + \cdots + Y_t^2)^{-1/2}(Y_1, \ldots, Y_t)$$

satisfies

$$\min_{1\le j\le t} |(z, \omega_j)| > \theta w^{-1/2}.$$

Bearing in mind that the unit sphere in $\mathbb{R}^t$ is compact in the usual topology, we see that our best choices are $\theta = r^{-1}(\pi/2)^{1/2}(1 - w^{-1}t)$ and $w = 3t$. The minimum is then at least $(2\pi)^{1/2}(3rt^{1/2})^{-1}$.

It transpires that within a constant multiple a natural form for the lower bound is $(rt^{1/2})^{-1}$ when the space is real, $(tr^{1/2})^{-1}$ when the space is complex.

If $r = 2$, then the best possible lower bound is $1/\sqrt{2}$, whether the space is real or complex. In our application there are complex numbers c_j, $j = 1, \ldots, k$, $\sum_{j=1}^{k} |c_j|^2 = 1$, so that for all primes $p > t$,

$$\left|\sum_{j=1}^{k} c_j g_j(p+1)\right| \ge (k/2)^{1/2}.$$

If $k > 8$, then Lemmas 1 and 2 guarantee the existence of j, ℓ, $1 \le j < \ell \le k$, a Dirichlet character χ_δ to a squarefree modulus δ, and a real τ, so that the series

$$\sum p^{-1}(1 - \operatorname{Re} g_j(p)\overline{g_\ell(p)}p^{i\tau}\chi_\delta(p)),$$

taken over the primes, converges.

Lemma 4 (Proximity Lemma). *If on the shifted primes $p+1$ the unimodular multiplicative function g assumes finitely many values, and if the series $\sum p^{-1}(1 - \operatorname{Re} g(p)p^{i\tau}\chi_\delta(p))$ converges, then $g(2m\delta)\chi_\delta(t)$ belongs to the set of values $g(p+1)$ of infinite multiplicity, uniformly for $(t, \delta) = 1$ and all positive integers m*

A proof of this result may be adapted from that for Lemma 13 of [2], there concerned with the case that $g(p+1) = 1$ holds for all but finitely many primes. I confine myself to two remarks.

If χ_δ has order h, then the inequality $1-\operatorname{Re} w^h \le h^2(1-\operatorname{Re} w)$, valid for $|w|\le 1$, shows that the series $\sum p^{-1}(1-\operatorname{Re} g(p)^h p^{i\tau h})$ converges. The initial argument of [2], Lemma 13, using a sieve to localise primes p for which $p+1$ has a bounded number of factors, then shows that for any real α, $g(2)2^{i\tau}\exp(2\pi i\alpha\tau)$ belongs to the finite value set of the $g(p+1)$. This is only feasible if $\tau = 0$.

Refinement of the argument employs the asymptotic uniform distribution of the primes in reduced residue classes.

As an application, suppose that $g(p+1)$ assumes at most d values. Choosing $t=1$ in Lemma 4 we see that the powers $g(m)^j$, $j=1,\ldots,d+1$ cannot be distinct. Each $g(m)$ is a root of unity, of order at most d.

As a corollary, the values of g on the positive *integers* form a group.

As a further corollary the set of $g(p+1)$-values of infinite multiplicity also form a group, W, say.

In our case W has order at most 2. If W has order 2, then $g(p+1)$ must ultimately assume values $+1,-1,+1,-1,\ldots$. In particular,

$$\sum_{\substack{p\le x\\ g(p+1)=y}} 1 = \frac{1}{2}\pi(x) + O(1), \qquad x\ge 2,$$

holds for $y = 1,-1$. An estimation of this accuracy is scarcely credible!

Lemma 5. *Let g be a unimodular completely multiplicative function for which the series*

$$\sum_{g(p)\ne\chi_\delta(p)} p^{-1}$$

converges. Then

$$\lim_{x\to\infty}\pi(x)^{-1}\sum_{p\le x} g(p+1)$$

exists and is non-zero.

The limit may be evaluated as an Euler product involving the Dirichlet character χ_δ. If g is assumed only to be multiplicative, $g(ab) = g(a)g(b)$ when $(a,b)=1$, then the limit can be zero.

In our case, W can have exact order 2 only if g has mean-value zero on the shifted primes, a possibility excluded by Lemma 5. The extended characters g_j, g_ℓ on Q^* coincide.

The group dual to G is finite, of order at most 8. The second dual of G and, since G can be embedded in it, G itself are finite. All three groups are isomorphic, of order at most 8.

Proof of the theorem. As t increases, the subgroups Γ_t form a decreasing chain, ordered by inclusion. For $s > t$ there is a natural homomorphism from Q^*/Γ_s onto Q^*/Γ_t, and $(Q^*/\Gamma_s)/(\Gamma_t/\Gamma_s)$ is isomorphic to Q^*/Γ_t. In particular

$$|Q^*/\Gamma_s| = |Q^*/\Gamma_t| \prod_{j=t}^{s-1} |\Gamma_j/\Gamma_{j+1}|.$$

Since the orders $|Q^*/\Gamma_s|$ are uniformly bounded, from some value of t onwards the Γ_j coincide and the groups Q^*/Γ_t are isomorphic.

The common group, which I denote by G_∞, is again of order at most 8. The assertion of the theorem is valid with $k = |G_\infty|$.

§4. Further results

It is natural to seek an analog of the theorem employing ratios $(p_j + 1)^{-1}(p_{j+3} + 1)$ with a shift by 3.

The k-tuples $(g_1(p + 1), \ldots, g_k(p + 1))$, ultimately periodic, may have a period of 1 or 3. Lemma 3 will then provide c_j, $j = 1, \ldots, k$, $\sum_{j=1}^k |c_j|^2 = 1$, for which the uniform but not necessarily best possible, lower bound

$$\left| \sum_{j=1}^{k} c_j g_j(p+1) \right| \geq k^{1/2}/(3\sqrt{3})$$

holds.

If $k > 108$, then we gain a pair of extended characters g_j, g_ℓ, $1 \leq j < \ell < k$, and a real τ for which the function $n \mapsto g_j(n)\overline{g_\ell(n)}n^{i\tau}$ is in an appropriate sense close to a Dirichlet character.

The proximity Lemma gives for the group W, of ultimate values attached to the $(g_j\bar{g}_\ell)(p + 1)$, a bound $|W| \leq 3$.

If $|W| = 3$, then W consists of $1, \rho, \rho^2$, with a cube root of unity ρ, $\rho \neq 1$. The periodic values of $(g_j\bar{g}_\ell)(p + 1)$ sum to zero and an appeal to Lemma 5 will yield the desired contradiction.

There remains the possibility that $|W| = 2$, so that the $(g_j\bar{g}_\ell)(p+1)$ ultimately assume one of the periodic patterns $1, -1, -1$ or $1, 1, -1$, with a corresponding mean-value $\pm 1/3$.

I conjecture that if $g(p + 1)$ assumes finitely many values, then for any y, an estimate

$$\sum_{\substack{p \leq x \\ g(p+1)=y}} 1 = A\pi(x) + O(1), \quad x \geq 2,$$

with $A \neq 0, 1$, is impossible.

It seems that it is the irregularities in the distribution of primes in residue classes that force finer structure upon the $g(p+1)$, and thus the groups generated by ratios of shifted primes.

Lacking a suitable variant of Lemma 5, we operate with the subgroup of squares in G, rather than with G itself. In this way we conclude the existence of an integer K, $K \leq 216$, for which the analog of the theorem holds with representations of the form

$$r^K = \prod_{j \in I} \left(\frac{p_{j+3}+1}{p_j+1} \right)^{d_j},$$

but we have not proved the corresponding groups Q^*/Γ_t to be finite.

It seems likely that if we replace the ratios $(p_j+1)^{-1}(p_{j+2}+1)$ by $(p_j+1)^{-1}(p_{j+m}+1)$, for any fixed $m \geq 1$ then the corresponding groups Q^*/Γ_t are all trivial.

All inequalities in this account may be made explicit.

It might be mentioned that in pursuit of a lower bound for gaps between primes we may not only choose the represented rational r, but consider product representations using shifted primes $p_j + a$, where a is allowed to vary.

The method of this paper is quite general and may be applied to study products and gaps formed by any sequence b_j, $j = 1, 2, \ldots$ for which the values $g(b_j)$ for characters g on Q^*, or some other appropriate group, exhibit suitable cancellation.

The foregoing account closely follows the lecture, under the same title, that I gave at the International Conference on Probability and Number Theory, held in Kanazawa, Japan, June 20–24, 2005.

With great pleasure I thank the organizers of the conference for their kind invitation to speak and for their financial support.

References

[1] L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, Messenger Math., **33** (1904), 155–161.

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

[3] P. D. T. A. Elliott, Probabilistic Number Theory I: Mean-Value Theorems, Grundlehren Math. Wiss., **239**, Springer-Verlag, Berlin, Heidelberg, New York, 1979.

Department of Mathematics
University of Colorado
Boulder, Colorado 80309–0395
USA