A conjecture of Kátai

by

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

1. An arithmetic function \( f(n) \) is said to be additive if for every pair of positive coprime integers \( a \) and \( b \) the relation \( f(ab) = f(a) + f(b) \) is satisfied. If the same relation holds for every pair of positive integers, whether coprime or not, then the function is said to be completely additive.

In his paper [5] Kátai lists six conjectures. The first of these, labelled \( H_1 \), asserts that if a completely additive arithmetic function vanishes on each of the integers which are of the form \( p+1 \), \( p \) prime, then it must be identically zero. In other words, a completely additive function is determined by its values on the shifted primes. In a subsequent paper [6], he proved the existence of an absolute constant \( K \), so that if in addition we assume that \( f(p) = 0 \) for the primes \( p \) not exceeding \( K \), then \( f \) is indeed identically zero. Unfortunately, the constant \( K \) could not be effectively determined by the method that he used, so that the conjecture \( H_1 \) could not yet be settled in this way.

We shall prove two results which will, in particular, include a stronger form of the conjecture \( H_1 \).

In what follows we assume only that \( f \) is an additive arithmetic function.

**Theorem 1.** Let \( |f(p+1)| \leq A \) hold for each prime \( p \). Then the series

\[
\sum_{n \geq 1} \frac{1}{p^n}, \quad \sum_{n \geq 1} \frac{f^v(p)}{p^n}
\]

both converge.

**Theorem 2.** Let \( f(p+1) = \text{constant} \) hold for all sufficiently large primes \( p \). Then \( f(p^v) = \text{constant} \) for all integers \( v \geq 1 \), and \( f \) is zero on all other prime-powers.

**Remark.** It will be clear from the method of proof of these theorems that a weaker hypothesis than that used in Theorem 2 will lead to a similar conclusion. For example, one could restrict the primes \( p \) to lie in a fixed arithmetic progression, or consider shifted primes \( p+k \) for values of \( k \) other than \( k = 1 \).
The validity of conjecture $H_1$ follows from Theorem 2.

Acknowledgement. The author would like to thank the referee for his careful reading of the first draft of the present paper. His comments enabled the presentation to be greatly improved.

2. The proof of both theorems depends upon the following essential lemma.

Let $x$ be a positive real number. This may need to be sufficiently large in what follows. For each positive integer $d$ let $N(d, x)$ denote the number of solutions to the equation

$$p + 1 = d(q + 1)$$

where $p$ and $q$ are prime numbers restricted by the conditions

$$p < x, \quad x^{1/3} < q < x^{1/5}, \quad (d, q + 1) = 1.$$  

Lemma 1. \[\sum_{\substack{a^{1/3} < c < a^{1/6} \\
N(a, c) > 0}} d^{-1} \gg \log x.\]

In order to prove this lemma we shall make use of the following estimates which can be found as, or deduced from, standard results in the theory of numbers.

(1) For each integer $D \geq 1$:

$$\pi(x, D, 1) \overset{\text{def}}{=} \sum_{p \leq x, p(D)} 1 \leq 1 + \frac{x}{D};$$

(2) \[E^*(x, D) \overset{\text{def}}{=} \sup_{(x, 1)) \leq 1} \sup_{x < x} \pi(y, D, 1) - \frac{\text{Li}(y)}{\varphi(D)} \ll 1 + \frac{x}{\varphi(D)};\]

(3) \[\sum_{D \leq x^{1/3} \log x} E^*(x, D) \ll x(\log x)^{-1}.\]

See, for example, Bombieri [1]. A shorter proof, on different lines is given in Gallagher [4].

(4) Uniformly for all positive integers $d$ not exceeding $x^{1/6}$:

$$N(d, x) \ll \frac{x}{d(\log a)^2} \prod_{p \mid (d-1)} \left(1 - \frac{1}{p}\right)^{-1}.$$  

See, for example, Prachar [7], Kap. II, Satz 4.2, p. 45.

Proof of Lemma 1. We shall prove Lemma 1 by estimating a certain sum from above and below. We begin with the estimate from below.

From (2) and (3) we obtain

$$\sum_{a^{1/3} < c < a^{1/6}} N(d, a) \gg \sum_{a^{1/6} < c < a^{1/5}} \sum_{p \mid (d-1)} \frac{\mu(p)}{\varphi(p)} \left(1 - \frac{1}{p}\right)^{-1};$$

$$\gg \sum_{a^{1/6} < c < a^{1/5}} \sum_{p \mid (d-1)} \frac{\mu(p)}{\varphi(p)} \left(1 - \frac{1}{p}\right)^{-1};$$

where \(\pi(y)\) denotes the number of rational primes not exceeding the real number $y$. The first of these last two double sums can be estimated at once by

$$\text{Li}(x) \sum_{a^{1/3} < c < a^{1/5}} \frac{1}{g + 1} = \log \frac{6}{5} \cdot \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)$$

whilst by using (3) and (2) the second (final) double sum is

$$\ll \sum_{a^{1/6} < c < a^{1/5}} E^*(x, r(q + 1)) + \sum_{r < (\log x)^3} \left(1 + \frac{x}{\varphi(r^2)}\right) + \frac{x}{(\log x)^2}$$

$$+ x(\log x)^{-1} + x \log \log x \sum_{s < x^{1/3}} \sum_{r > (\log x)^3} \frac{1}{r^2} \ll x(\log x)^{-1}.$$  

since for all sufficiently large integers $m$ we have $\varphi(m) \gg m(\log \log m)^{-1}$. Hence we obtain the lower bound

$$\sum_{a^{1/3} < c < a^{1/6}} N(d, x) \gg \frac{x}{(\log x)^2}.$$  

In the other direction we apply the Cauchy–Schwarz inequality in the form

$$\sum_{a^{1/6} < c < a^{1/5}} N(d, x) \leq \left( \sum_{a^{1/3} < c < a^{1/6}} d^{-1/2} \right) \left( \sum_{c < a^{1/6}} dN^2(d, x) \right)^{1/2}.$$  

In view of the lower bound established above, Lemma 1 will follow if we prove that

$$\sum_{a^{1/6} < c < a^{1/5}} dN^2(d, x) \ll \frac{x^2}{(\log x)^3}.$$
To do this it is convenient to define the function
\[ e(d) = d^{-1/2} \prod_{p|d} (1 - p^{-1})^{-1}. \]

Then by the preliminary result (4) we have
\[ \sum_{1 \leq x \leq c \leq x^{1/6}} dN^2(d, x) \leq \frac{a^2}{(\log a)^8} \sum_{1 \leq x \leq c \leq x^{1/6}} e(d) e(d-1). \]

After a further application of the Cauchy–Schwarz inequality, noting that the function \( e(d) \) is multiplicative, we have
\[ \sum_{1 \leq x \leq c \leq x^{1/6}} dN^2(d, x) \leq \left( \sum_{d \leq c} e^2(d) \right)^{1/2} \left( \sum_{d \leq c} e^2(d-1) \right)^{1/2} \]
\[ \leq \prod_{p \leq c} \left( 1 + e^2(p) + e^2(p^2) + \ldots \right) \]
\[ = \prod_{p \leq c} \left( 1 + p^{-1}(1 - p^{-1})^{-1} \right) \leq \log a. \]

Gathering together the various inequalities we see that Lemma 1 is proved.

3. In this section we prove Theorem 1. We need one further preliminary result. An additive function \( f(n) \) is said to be finitely distributed if there are two positive constants \( c_1 \) and \( c_2 \), and an unbounded sequence of positive integers \( n_1 < n_2 < \ldots \) so that for each integer \( n = n_k \) we can find a further sequence of integers \( 1 < a_1 < a_2 < \ldots < a_k \leq n \) with \( k \geq c_1 n \), and for which \( |f(a_k) - f(a_{k-1})| \leq c_2 \). We shall make use of the following characterization of such functions, due to Erdős [3].

**Lemma 2.** An additive function \( f(n) \) is finitely distributed if and only if it can be expressed in the form \( c \log n + g(n) \), where \( c \) is a constant, and the additive function \( g(n) \) satisfies the conditions
\[ \sum_{|g(p)| > 1} \frac{1}{p} < \infty, \quad \sum_{|g(p)| < 1} \frac{g^2(p)}{p} < \infty. \]

**Proof.** The proof given in Erdős' original paper [3] is elementary but complicated. Another proof, based on quite different ideas, can be found in Ryavec [8].

**Proof of Theorem 1.** Let us define
\[ D(y) = \sum_{w^{1/3} < x < c^{1/6}} D(y)/y. \]

Then appealing to Lemma 1 and integrating by parts:
\[ \log a \leq \sum_{w^{1/3} < x < c^{1/6}} d^{-1} = \int_{w^{1/3}} D(y)^{-1}dy \]
\[ = X^{-1/3} \int_{w^{1/3}} D(y) y^{-2}dy \leq \beta \int_{w^{1/3}} y^{-2}dy \]
\[ = \beta (1 + (\log x)^{-1/2}). \]

From this it follows that we can find an absolute constant \( c_1 > 0 \) such that, in each interval \( x^{1/3} < y < x^{1/6} \), there exists a number \( y_0 \) for which we have \( D(y_0) > c_1 y_0 \).

We define
\[ \mathcal{D} = \{ d : w^{1/3} < d < y_0, N(d, w) > 0 \}. \]

Then each integer \( d \) in \( \mathcal{D} \) can be represented in the form \( d = (p+1)/(q+1) \) where \( (d, q+1) = 1 \), and the numbers \( p \) and \( q \) are prime and become large with \( x \). From this and the assumptions of Theorem 1 we obtain
\[ |f(d)| = |f(p+1) - f(q+1)| \leq 2A. \]

This implies that \( f \) satisfies the assumptions of Lemma 2, and therefore it can be represented in the form \( f(n) = c \log n + g(n) \) where \( g(n) \) satisfies the conditions given in Lemma 2.

To complete the proof of Theorem 1 we shall prove that the constant \( c \) has the value zero.

Let \( \varepsilon \) be a real number, \( 0 < \varepsilon < 1/10 \). Let \( P \) be chosen so large that
\[ \sum_{|g(p)| > 1} \frac{1}{p} < \varepsilon. \]

The number of integers \( m \) not exceeding \( y_0 \), and divisible by a prime \( p > P \) for which \( |g(p)| > 1 \), is then not more than
\[ \sum_{p > P \atop |g(p)| > 1} \left[ \frac{y_0}{p} \right] < \varepsilon y_0. \]

The number of integers \( m \) not exceeding \( y_0 \), and divisible by a prime-power \( p^r \) with \( r \geq y_0 = 10 - (\log x)(\log 2) \), is not more than
\[ \sum_{p \neq 1} \sum_{p^r \leq x} \left[ \frac{y_0}{p^r} \right] < y_0 \sum_{p \neq 1} \frac{1}{p^r - p^{r-1}} < 2^{-y_0+10} y_0 = \varepsilon y_0. \]
The number of integers \( m \) not exceeding \( y_0 \), and divisible by \( p^k \) for some prime \( p > 1 + \varepsilon^{-1} \), is at most

\[
\sum_{p > 1 + \varepsilon^{-1}} \left[ \frac{y_0}{p^k} \right] < y_0 \sum_{n > 1 + \varepsilon^{-1}} \frac{1}{n(n-1)} \sim y_0.
\]

Let \( \varepsilon = \min\{\frac{1}{3}, \frac{1}{3} \} \), and define

\[ S = \{ d : \sigma_0 \leq d \leq y_0, N(d, \sigma) > 0, p^k | d \Rightarrow p \leq \varepsilon^{-1} + 1, \] \[ p^k - d \Rightarrow \sigma, p | d, y(p) > 1 \Rightarrow p \leq P \}. \]

Then from these last three assertions, and what have proved concerning the set \( S \), it follows that

\[
\sum_{d \in S} 1 \geq c_1 y_0 - 3 \varepsilon y_0 \geq \frac{1}{3} c_1 y_0.
\]

Furthermore, for each integer \( b \) in \( S \)

\[
| \log b | \leq | f(b) | + | g(b) | \leq 2A + O\left( \sum_{p \leq 10} \right).
\]

Therefore

\[
| c | \sum_{r \leq 2A y_0} \log b \leq | c | \sum_{r \leq 2A y_0} \log b \leq 2A y_0 + O\left( \sum_{p \leq 10} \right)
\]

so that

\[
| c | \leq \frac{\log y_0}{\log y_0}.
\]

Since this last inequality holds for an unbounded sequence of values \( y_0 \), we have \( c = 0 \), and Theorem 1 is proved.

4. In this section we prove Theorem 2. The proof is carried out along the lines of the proof of Theorem 1. As before we define \( D(y) \) and determine an unbounded sequence of values \( y_0 \), and a positive constant \( c_1 \), so that \( D(y_0) \geq c_1 y_0 \). This time the integers \( d \) which we counted in the set \( S \) are such that

\[ f(d) = f(p+1) - f(q+1) = 0. \]

As before \( f(n) \) has the form \( \log n + o(n) \), and we can prove that \( c = 0 \). We can, however, already do better than this by applying the following result.

For each real number \( z > 0 \), and integer \( n \), set

\[ F_n(z) = n^{-z} \sum_{m=1}^{n} 1. \]

**Lemma 8.** A necessary and sufficient condition that the limiting relationship

\[ \limsup_{d \to \infty} \left| F_n(z+\delta) - F_n(z-\delta) \right| = 0 \]

should hold uniformly for all real values of \( z \) is that the series

\[ \sum_{d \to \infty} \frac{1}{d} \]

diverges.

**Proof.** This result was proved by Erdös [3], subject to the side condition \( f(p) = O(1) \). A proof along different lines, and without such a side condition, can be found in Elliott and Rávey [2].

In our present circumstances we set \( z = 0 \), so that for every \( \delta > 0 \)

\[ \limsup_{n \to \infty} | F_n(\delta) - F_n(-\delta) | \geq \limsup_{n \to \infty} | y_0 \delta D(y_0) \delta > c_1 > 0. \]

It follows at once that \( f(p) = 0 \) for almost all prime \( p \), in the sense of Lemma 3.

The remainder of the proof of Theorem 2 is straightforward, but complicated. In order to facilitate its presentation we collect here three further well-known results from the theory of numbers, of which we shall make use.

(5) **For each integer** \( D \geq 1 \)

\[ \pi(x, D, -1) = (1+o(1)) \frac{x}{\phi(D) \log x}. \]

See, for example, Prachar [7], Kap. IV, Satz 7.6, p. 138.

(6) **Uniformly for** \( D \leq x^a, 0 < a < 1, \)

\[ \pi(x, D, -1) \leq c_2(a) \frac{x}{\phi(D) \log x} \]

where the constant \( c(a) \) may depend upon \( a \).

See, for example, Prachar [7], Kap. II, Satz 4.1, p. 44.

(7) **Uniformly for** \( D \leq x^a, 0 < a < 1, \)

\[ \sum_{p \leq x, p \neq 2} \frac{1}{(\log p)^2} \leq c_1(a) \frac{x}{\phi(D)(\log x)^2}. \]

See, for example, Prachar [7], Kap. II, Satz 4.6, p. 51.

To continue with our proof of Theorem 2 let \( q_1 < q_2 < \ldots \) denote the odd primes \( q \) for which \( f(q) = 0 \). Let \( d \) be a positive integer. Let \( P \)
be a further positive integer, which we shall later choose to be in a certain sense 'large'. We shall obtain a lower bound for the number \( T(x) \) of primes \( p \), not exceeding \( x \), for which

\[
(8) \quad p + 1 = 2dk; \quad (k, 2d) = 1; \quad \forall i q_i < k; \quad \forall q \leq P, q \text{ prime}, q \nmid k; \quad \forall q > P, q \nmid (p+1).
\]

To do this choose a positive integer \( r \), and define

\[
Q = 2d \prod_{i=1}^{r} q_i \prod_{p<2d} p.
\]

Let \( \alpha \) be a real number, \( \frac{3}{4} < \alpha < 1 \). Then certainly

\[
T(x) \geq \sum_{p<2d} \sum_{q \leq Q} \sum_{q \equiv -1 (mod q_1^2)} 1 - \sum_{p \leq 2d} \sum_{q \equiv -1 (mod q_1^2)} 1 - \sum_{p \leq 2d} \sum_{q \equiv 1 (mod q_1^2)} 1
\]

\[
= \sum_{p \leq 2d} \sum_{q \equiv -1 (mod q_1^2)} \mu(q) - \sum_{p \leq 2d} \sum_{q \equiv 1 (mod q_1^2)} 1
\]

\[
= \sum_{p \leq 2d} \sum_{q \equiv -1 (mod q_1^2)} 1 - \sum_{p \leq 2d} \sum_{q \equiv 1 (mod q_1^2)} 1
\]

\[
= \Sigma_1 - \Sigma_2 - \Sigma_3 - \Sigma_4.
\]

Using (7) we can derive the estimate (for fixed \( d \)):

\[
\Sigma_1 = \frac{x}{\log x} \sum_{a \equiv 0 (mod 2)} \mu(a) - o\left( \frac{x}{\log x} \right) = (1 + o(1) \frac{x}{\log x} \cdot 2d \prod_{q \equiv 1 (mod 2)} \left( \frac{q-2}{q-1} \right).
\]

Using (8) we obtain the upper bound

\[
\Sigma_2 \leq c_0(\alpha) \frac{x}{\log x} \sum_{q} \frac{1}{q_i-1}.
\]

Using (7) we can majorise our third sum by

\[
\Sigma_3 \leq \sum_{p \equiv \alpha (mod q_1^2)} \sum_{q \equiv 1 (mod q_1^2)} 1 \leq \sum_{p \equiv \alpha (mod q_1^2)} \sum_{q \equiv 1 (mod q_1^2)} 1
\]

\[
\leq \sum_{D \equiv \alpha \equiv 1 (mod q_1^2)} \sum_{D \equiv q \equiv 1 (mod q_1^2)} \frac{x}{\log x} \sum_{D \equiv -1 (mod q_1^2)} \frac{1}{\psi(D)} \ll (1 - \alpha) \frac{x}{\log x},
\]

the implied constant being absolute.

Lastly, using (8) once again

\[
\Sigma_4 \ll \frac{x}{\log x} \sum_{q \equiv 1 (mod q_1^2)} \frac{1}{q^2} + \sum_{q \equiv 1 (mod q_1^2)} \frac{x}{P\log x} + o(x^{\theta/4}).
\]

Putting these estimates together we see that

\[
\lambda = \liminf \frac{T(x)}{x (\log x)^{-1}}
\]

\[
\geq \frac{1}{2d} \prod_{q \equiv 1 (mod 2)} \left( 1 - \frac{1}{q-1} \right) - o\left( \sum_{q \equiv 1 (mod 2)} \frac{1}{q_i-1} \right) - O\left( (1 - \alpha) - O(P^{-1}) \right).
\]

If we let \( r \rightarrow \infty \) and then \( \alpha \rightarrow 1 \), we see that we can assert that

\[
\lambda \geq \frac{1}{2d} \prod_{1 \leq q \leq P} \left( 1 - \frac{1}{q-1} \right) \prod_{1 \leq q \leq x} \left( 1 - \frac{1}{q_i-1} \right) + O(P^{-1})
\]

\[
\geq c_0(\log P)^{-1} + O(P^{-1}) > 0
\]

if we choose \( P \) suitably large, but otherwise fixed.

Since we can find infinitely many primes \( p \) which satisfy all of the hypotheses stated in (8) we can find a sufficiently large one for which

\[
f(2d) + f(k) = f(p+1) = g \quad \text{(constant)}
\]

say. Here \( k \) is square free, and has no factor of the form \( q_i \), so that \( f(k) = 0 \).

Choosing \( d = 2r, r = 0, 1, \ldots \) in turn, we see that \( f(2r) \) is constant.

Next, choosing \( d = q_i^2 \), any odd prime power, we see that \( f(q_i^2) = q - f(2) = 0 \).

This completes the proof of Theorem 2.

References

Examples of Iwasawa invariants

by

R. Gold (Columbus, Ohio)

Let \( E = \mathbb{Q}(\sqrt{-d}) \), \( d > 0 \), be a quadratic imaginary field of discriminant \(-d\) and class number \( h = h(-d)\) and let \( l \) be an odd rational prime, \( (l, d) = 1\). There is a unique \( \mathbb{Z}_l \)-extension of \( E \) which is absolutely abelian. Let \( e_n \), \( n \geq 0 \), denote the exact power of \( l \) dividing the class number of the \( n \)-th layer of the \( \mathbb{Z}_l \)-extension. Under the assumption \((A)\) \( l^{n-1} = 1(d)\), the author has given the following formulas for \( e_n - e_{n+1} \) \((1)\). Let \( \eta \) be a primitive \( l \)-th root of unity and \( 1 = (1-\eta) \) the prime ideal of \( \mathbb{Q}(\eta) \) lying over \( l \). Let \( \chi \) be the character of \( E; \chi \) is a quadratic character of conductor \( d \). Define \( \alpha(r) = \sum_{i=0}^{\infty} \chi(i) \). Let \( g \) be a primitive root modulo \( l^{n+1} \) and for all \( s \geq 0 \), \( g(s) = g^s(l^{n+1}) \), \( 0 \leq g(s) < l^{n+1} \). For any \( s \in \mathbb{Z}, r \in \mathbb{N} \), define \( s_r \) by \( s_r = s(F) \), \( 0 \leq s_r < F \). Then

\[
\begin{align*}
  e_n - e_{n+1} & = \text{ord}_l(\gamma) ; \\
  \gamma & = \sum_{i=0}^{\phi(l^n)} \gamma_i \eta^i ; \\
  \gamma_i & = \sum_{s=0}^{l-2} \left( \alpha(g(s + l^{n})) - \alpha(g(s) + i l^n + s_{n-1}) \right) .
\end{align*}
\]

Hence, the difference \( e_n - e_{n+1} \) depends on the \( l \)-order of an algebraic integer in \( \mathbb{Q}(\eta) \) whose coefficients are certain sums in \( \chi \).

For sufficiently large \( n \), \( e_n = \mu n^2 + \lambda n + o \) for fixed \( \mu, \lambda \geq 0 \), \( o \in \mathbb{Z} \) \(((4),(7))\). These \( \lambda, \mu \) are the Iwasawa invariants of the given \( \mathbb{Z}_l \)-extension. Our purpose here is to describe some computations of these invariants based on \( (1) \).

The contents of this note are as follows: in \( \S \ 1 \) we show how to alter \( (1) \) in order to dispense with the restrictive assumption \((A)\). In \( \S \ 2 \) we show that, in the case \( (-d/l) = -1 \), a knowledge of \( e_i \) for small \( i \) often suffices for the determination of \( \mu, \lambda \). Some auxiliary results for \( l = 3 \) are given in \( \S \ 3 \). A short description of the actual computations and the tabulated results are contained in \( \S \ 4 \).

I would like to thank John Coates for several useful suggestions, including, in particular, the proof of the lemma of \( \S \ 3 \).