JOURNAL OF NUMBER THEORY **63**, 325–338 (1997)
ARTICLE NO. NT972108

A New Characteristic of the Identity Function

Jean-Marie De Koninck*

Département de Mathématiques et de Statistique, Université Laval, Québec G1K 7P4, Canada

and

Imre Kátai† and Bui Minh Phong

Computer Algebra Department, Eötvös Loránd University, Müzeum krt. 6–8, 1088 Budapest, Hungary

Received March 4, 1996; revised November 5, 1996

In 1992, C. Spiro [7] showed that if f is a multiplicative function such that $f(1)=1$ and such that $f(p+q)=f(p)+f(q)$ for all primes p and q, then $f(n)=n$ for all integers $n \geqslant 1$. Here we prove the following:

THEOREM. *Let f be a multiplicative function such that $f(1)=1$ and such that*

$$f(p+m^2)=f(p)+f(m^2) \qquad \text{for all primes } p \text{ and integers } m \geqslant 1, \tag{1}$$

then $f(n)=n$ for all integers $n \geqslant 1$.

Proof. First we show that

$$f(p^2)=f(p)^2. \tag{2}$$

Indeed, using (1) and the fact that f is multiplicative, we have

$$\begin{aligned} f(p)+f(p^2) &= f(p+p^2)=f(p(1+p))=f(p)\,f(p+1^2) \\ &= f(p)(f(p)+1)=f(p)^2+f(p), \end{aligned}$$

from which (2) follows immediately.

We now show that

$$f(n)=n \qquad \text{for all positive integers } n \leqslant 12. \tag{3}$$

* Research partially supported by Grants from NSERC of Canada and FCAR of Québec.
† Research partially supported by the Hungarian Research Foundation (OTKA).

0022-314X/97 $25.00

Repeated use of (1) gives $f(3)=f(2+1)=f(2)+f(1)=f(2)+1$ and thus $f(4)=f(3+1)=f(3)+1=f(2)+2$. Then $f(6)=f(4)+f(2)=f(2)+2+f(2)=2+2f(2)$, $f(7)=f(4)+f(3)=3+2f(2)$, $f(8)=1+f(7)=4+2f(2)$, $f(9)=f(4)+f(5)=f(2)+2+f(5)$. Moreover $f(11)=f(4)+f(7)=5+3f(2)$, while also $f(11)=f(9)+f(2)=f(4)+f(5)+f(2)=2+2f(2)+f(5)$. Finally $f(12)=f(4)\,f(3)=f(11)+1=6+3f(2)$, which implies that $(2+f(2))\,f(3)=6+3f(2)$, that is $2f(3)+f(6)=6+3f(2)$ and therefore $(2+2f(2))+(2+2f(2))=6+3f(2)$, from which we deduce that $f(2)=2$. It easily follows from this that $f(n)=n$ successively for $n=3$, 4, 6, 7, 8, 11, 5, 9, 10, 12. This proves (3).

It is clear that the Theorem will follow if we can prove the following:

$$\text{If } T \text{ is an integer such that } f(n)=n \text{ for all } n<T, \text{ then } f(T)=T. \tag{4}$$

Because of (3), we can assume that $T>12$.

We proceed by contradiction. Hence assume that (4) is false for a certain $T>12$, that is that $f(n)=n$ for each positive integer $n<T$, but that $f(T)\neq T$.

We first show that in such a case, T must be a prime power. Suppose indeed that T is not a prime power. We may thus write $T=AB$ with $1<A<B<T$ and $(A,B)=1$, in which case we have $f(T)=f(AB)=f(A)\,f(B)=AB=T$, a contradiction.

We also show that T cannot be a prime. Assume that it is. Then

$$f(T+1)=f(T)+1\neq T+1. \tag{5}$$

Clearly $T+1$ is composite. Letting $P^*(n)$ denote the largest prime power which divides n, then either $T+1$ is a prime power or else $T+1=AB$ with $1<A<B<T+1$, $(A,B)=1$, $P^*(A)<T$, $P^*(B)<T$. In the former case, since $T+1$ is even, we must have $T+1=2^\beta$ and thus $T=2^\beta-1$. It follows from this that

$$\begin{aligned} f(T+9)&=f(2^\beta-1+9)=f(2^\beta+8)=f(8(2^{\beta-3}+1))\\ &=f(8)\,f(2^{\beta-3}+1)=8(2^{\beta-3}+1)=T+9, \end{aligned}$$

a relation which is contradicted by the fact that

$$f(T+9)=f(T+3^2)=f(T)+f(9)=f(T)+9\neq T+9.$$

In this latter case, we have $f(T+1)=f(AB)=f(A)\,f(B)=AB=T+1$ which contradicts (5). We also have that T cannot be the square of a prime. In fact, this follows immediately from (2).

We must therefore have that

$$T=q^\alpha, \qquad \text{with } \alpha\geqslant 3 \text{ and some prime } q.$$

We also note that α must be an odd number. Indeed, if α is even, then

$$f(q^\alpha + q) = f(q(q^{\alpha-1} + 1)) = f(q)\, f(q^{\alpha-1} + 1) = q(q^{\alpha-1} + 1) = q^\alpha + q, \qquad (6)$$

while on the other hand

$$f(q^\alpha + q) = f(q^\alpha) + f(q) = f(q^\alpha) + q \neq q^\alpha + q,$$

which contradicts (6).

With the help of a computer, we found all those prime powers $r^k \leqslant 10^6$, with $k \geqslant 3$, which cannot be written as $r^k = p + m^2$ (p is a prime, m an integer), namely 2^6, 5^4, 2^{10}, 3^8, 5^6, 2^{14}, 3^{10}, 2^{16}, 7^6, 19^4, 2^{18}, 23^4, 3^{12}, 29^4 and 31^4. Using the results established above including the induction hypothesis and the fact that each of these 15 numbers r^k have an even exponent k, it follows that $T > 10^6$.

Our next step is to prove three important lemmas.

Lemma 1. *Assume that $T > 10^6$. Then for all primes $p < T^2/2$, we have $f(p) = p$.*

Proof of Lemma 1. Let p be the smallest prime, if any, for which $f(p) \neq p$ and assume that $T < p < T^2/2$, and consider the integers

$$\ell_v = p + v^2 \qquad (v = 1, 3, 5, ..., [\sqrt{p}],\ v \text{ odd}).$$

Our plan is to show that there exists an odd integer $v \leqslant [\sqrt{p}]$ satisfying both $f(\ell_v) = \ell_v$ and $f(v^2) = v^2$. For such a v, it will follow that $f(\ell_v) = f(p) + f(v^2) = f(p) + v^2 \neq p + v^2$ since $f(p) \neq p$, thereby contradicting the fact that $f(\ell_v) = \ell_v = p + v^2$, thus establishing the proof that $f(p) = p$.

By definition,

$$\ell_v < 2p, \qquad (7)$$

the inequality being strict because $\sqrt{p}$ is not an integer. Now write

$$\ell_v = A_v \cdot B_v, \qquad \text{where } A_v \text{ is the largest prime power dividing } \ell_v. \qquad (8)$$

We first look for v's such that $f(\ell_v) = \ell_v$. First consider the case where A_v is a prime. It is clear that we cannot have $A_v \geqslant p$; indeed, since B_v is even, it would follow from (7) that $2 \leqslant B_v = \ell_v / A_v < 2p/p = 2$, a non sense. Hence $A_v < p$, in which case $f(A_v) = A_v$ due to the minimal choice of p. If $A_v < T$, then $P^*(B_v) < A_v < T$ and thus $f(\ell_v) = f(A_v)\, f(B_v) = A_v B_v = \ell_v$. On the other hand, if $T \leqslant A_v < p$, then $B_v = \ell_v / A_v < 2p/T < T$, which again implies that $f(\ell_v) = f(A_v)\, f(B_v) = A_v B_v = \ell_v$. On the other hand, if A_v is a prime power, say $A_v = Q^\beta$, with $\beta \geqslant 2$, then first consider the case where $\beta = 2$:

using (7), we have $Q^2 < 2p < T^2$, and thus $Q < T$. It follows from (2) that $f(Q^2) = f^2(Q) = Q^2$ and thus that $f(A_v) = A_v$ and $f(B_v) = B_v$, from which it follows as above that $f(\ell_v) = \ell_v$. If $\beta \geqslant 3$, consider the set

$$\mathscr{H} := \{v \colon 1 \leqslant v \leqslant \sqrt{p},\ v \text{ odd},\ A_v = Q^\beta = \text{prime power} \geqslant T,\ \beta \geqslant 3\}.$$

Observe that, since $p + v^2 \equiv 0 \pmod{Q^\beta}$ is a quadratic congruence, it has at most two solutions modulo Q^β if Q is odd and at most 4 if $Q = 2$, and in fact there are no more solutions located in the range $1 \leqslant v \leqslant [\sqrt{p}]$ since $\sqrt{p} < T \leqslant Q^\beta$.

Rosser and Schoenfeld [6] have shown that $\pi(x)$, the number of prime numbers up to x, satisfies

$$\frac{x}{\log x} < \pi(x) < \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right) \qquad (x \geqslant 59).$$

On the other hand, one can verify that

$$\frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right) < (1+\eta)\frac{x}{\log x} \qquad \text{with} \quad \eta = \frac{1}{10} \quad (x > 3.3 \times 10^6)$$

and also, using a computer, that

$$\pi(x) < (1+\eta)\frac{x}{\log x} \qquad (10^6 < x < 3.3 \times 10^6).$$

It follows that

$$\frac{x}{\log x} < \pi(x) < (1+\eta)\frac{x}{\log x}, \qquad \eta = \frac{1}{10}, \quad (x > 10^6) \tag{9}$$

and since the largest integer β such that $Q^\beta < p$, for $\beta \geqslant 3$, satisfies $\beta < \log p / \log Q$, we may thus conclude that

$$\begin{aligned} \#\mathscr{H} &< 4 \sum_{\substack{2^\beta < p \\ \beta \geqslant 3}} 1 + 2 \sum_{\substack{Q^\beta < p \\ Q > 2,\ \beta \geqslant 3}} 1 \\ &< 4\left(\frac{\log p}{\log 2} - 2\right) + 2\left(\pi(p^{1/3}) + \pi(x^{1/4})\frac{\log p}{\log 3}\right) \\ &< 4\left(\frac{\log p}{\log 2} - 2\right) + 2(1+\eta)\left(\frac{3p^{1/3}}{\log p} + \frac{4p^{1/4}}{\log 3}\right). \end{aligned} \tag{10}$$

Since we have already shown that, if $v \notin \mathscr{H}$, then $f(\ell_v) = \ell_v$, we now look for odd v's not exceeding $\sqrt{p}$ with the property $f(v^2) = v^2$. We call such a v a *good* v; the other ones being called *bad* v's. Certainly those v's for which each prime power π^δ dividing exactly v is such that $\delta = 1$ or $\pi^\delta < \sqrt{T}$ are good. Possible bad v's must therefore have a prime power $\pi^\delta \geqslant \sqrt{T}$ (with $\delta \geqslant 2$). Hence the number N_{bad} of bad v's up to $\sqrt{p}$ is small, indeed it is

$$N_{bad} < \sum_{\substack{\sqrt{T} \leqslant \pi^\delta < T \\ \delta \geqslant 2}} \left[\frac{\sqrt{p}}{\pi^\delta} \right] < \sqrt{p} \sum_{\substack{\sqrt{T} \leqslant \pi^\delta < T \\ \delta \geqslant 2}} \frac{1}{\pi^\delta}. \tag{11}$$

Now, for each integer $\delta \geqslant 2$, real $R \geqslant 2$, using Stieltjes integral, then integration by parts and finally (9), we obtain

$$\begin{aligned}
\sum_{\pi^\delta > R} \frac{1}{\pi^\delta} &= \sum_{\pi > R^{1/\delta}} \frac{1}{\pi^\delta} \\
&= \int_{R^{1/\delta}}^{\infty} \frac{d\pi(t)}{t^\delta} \\
&= \frac{\pi(t)}{t^\delta} \bigg|_{R^{1/\delta}}^{\infty} + \delta \int_{R^{1/\delta}}^{\infty} \frac{\pi(t)}{t^{\delta+1}}\, dt \\
&< -\frac{\pi(R^{1/\delta})}{R} + \delta(1+\eta) \int_{R^{1/\delta}}^{\infty} \frac{dt}{t^\delta \log t} \\
&< -\frac{\delta}{R^{1-1/\delta} \log R} + \frac{\delta^2(1+\eta)}{(\delta-1)\, R^{1-1/\delta} \log R}.
\end{aligned} \tag{12}$$

Note that in the case $\delta = 2$, we have

$$\sum_{\pi^2 > R} \frac{1}{\pi^2} < -\frac{2}{R^{1/2} \log R} + \frac{4(1+\eta)}{R^{1/2} \log R} = \frac{2+4\eta}{R^{1/2} \log R}.$$

Observe also that, for $\delta \geqslant 3$, we have

$$-\delta + \frac{\delta^2(1+\eta)}{\delta-1} < \frac{3}{2} + 2(\delta+1)\, \eta. \tag{13}$$

By treating separately the two cases $\delta = 2$ and $\delta \geqslant 3$, we have

$$\sum_{\delta \geqslant 2} \sum_{R < \pi^\delta < R^2} \frac{1}{\pi^\delta} = \sum_{R < \pi^2 < R^2} \frac{1}{\pi^2} + \sum_{\delta \geqslant 3} \sum_{R < \pi^\delta < R^2} \frac{1}{\pi^\delta}$$
$$< \frac{2 + 4\eta}{R^{1/2} \log R} + \sum_{3 \leqslant \delta \leqslant 2 \log R/\log 2} \frac{(3/2) + 2(\delta + 1)\,\eta}{R^{1 - 1/\delta} \log R}$$
$$< \frac{2 + 4\eta}{R^{1/2} \log R} + \frac{2((3/2) + 8\eta)}{R^{2/3} \log 2}$$

Letting $R = \sqrt{T}$, we obtain

$$\sum_{\delta \geqslant 2} \sum_{\sqrt{T} < \pi^\delta < T} \frac{1}{\pi^\delta} < \frac{2(2 + 4\eta)}{T^{1/4} \log T} + \frac{2((3/2) + 8\eta)}{T^{1/3} \log 2}. \tag{14}$$

Hence, using (14), inequality (11) can be written as

$$N_{bad} < \sqrt{p} \left(\frac{8 + 16\eta}{p^{1/8} \log p} + \frac{3 + 16\eta}{p^{1/6} \log 2} \right). \tag{15}$$

Hence, combining (10) and (15), and if $p > 10^6$, it follows that

$$[\sqrt{p}] > N_{bad} + \#\mathscr{H},$$

which proves that there exists at least one odd integer $v \leqslant [\sqrt{p}]$ such that $f(v^2) = v^2$ and $f(\ell_v) = \ell_v = p + v^2$ while $f(\ell_v) = f(p) + f(v^2) = f(p) + v^2$. Hence if $f(p) \neq p$, it would follow that $f(\ell_v) = f(p) + v^2 \neq p + v^2 = f(\ell_v)$, a non sense. The proof of Lemma 1 is thus completed.

LEMMA 2. *Let π be a prime and Δ a positive integer such that $\pi^\Delta < T$, then*

$$f(\pi^{2\Delta}) = \pi^{2\Delta}. \tag{16}$$

Proof of Lemma 2. First assume that π is odd. Then, for each prime $2 < p < T^2/2$, set

$$h_p := p + \pi^{2\Delta} = E_p \cdot F_p,$$

where E_p is the highest prime power dividing h_p. Observe that $h_p < \frac{3}{2} T^2$. Clearly, by Lemma 1,

$$f(h_p) = f(p) + f(\pi^{2\Delta}) = p + f(\pi^{2\Delta}). \tag{17}$$

If $E_p < T$, then $f(h_p) = h_p = p + \pi^{2\Delta}$, an equality which combined with (17) proves (16). Hence assume that $E_p \geqslant T$.

First consider the case where E_p is a prime with $E_p \geqslant T$. Clearly $2 \mid F_p$. Since $h_p < \frac{3}{2}T^2$, then $F_p < \frac{3}{2}T$. There are two possibilities:

- $F_p = U \cdot V$, where $(U, V) = 1$, $1 < P^*(U) < T$ and $1 < P^*(V) < T$, in which case $f(F_p) = F_p$. Therefore $F_p \geqslant 6$. Since $E_p \leqslant (3T^2/2)/6 = T^2/4$, it follows by Lemma 1 that $f(E_p) = E_p$. This implies that

$$f(h_p) = f(E_p)\, f(E_p) = E_p F_p = h_p = p + \pi^{2\Delta},$$

which combined with (17) proves (16).

- F_p is a prime power, which implies, since F_p is even, that $F_p = 2^\beta$ for some integer $\beta \geqslant 2$ with $T < 2^\beta < \frac{3}{2}T$. Then $h_p = Q \cdot 2^\beta$ for some prime Q. The number M_T of such p's is

$$M_T < \pi\left(\frac{T^2}{2};\, -\pi^{2\Delta}, 2^\beta\right),$$

where $\pi(x; k, \ell) = \#\{r \leqslant x, r \text{ prime: } r \equiv k \pmod{\ell}\}$. Using the sieve result (see Halberstam and Richert [1], formula (4.10), p. 110)

$$\pi(x; k, \ell) < \frac{3x}{\phi(k) \log(x/k)} \qquad (1 \leqslant k < x, (k, \ell) = 1),$$

we conclude that, since $\phi(2^\beta) = 2^{\beta-1} > T/2$,

$$M_T < 3\,\frac{T^2}{2}\,\frac{1}{\log(T^2/2 \cdot 2^\beta)}\,\frac{1}{\phi(2^\beta)} < \frac{3T}{\log(T^2/2 \cdot (3/2)\,T)} = \frac{3T}{\log T/3} < \frac{4T}{\log T}. \tag{18}$$

On the hand, assume that $E_p = Q^\beta$ for some prime $Q > 2$ and integer $\beta \geqslant 2$ and satisfying $T < Q^\beta < \frac{3}{4}T^2$. First consider the case $\beta = 2$; then $Q^2 < \frac{3}{4}T^2$, that is $Q < T$ and therefore $f(Q) = Q$, in which case $f(Q^2) = f^2(Q) = Q^2$, and since $F_p < T$, $f(F_p) = F_p$, implying that $f(h_p) = h_p = p + \pi^{2\Delta}$, which combined with (17) implies (16). For $\beta \geqslant 3$, count the number N_T of those primes $p \leqslant T^2/2$ such that $Q^\beta \mid p + \pi^{2\Delta}$, $Q^\beta > T$ and $\beta \geqslant 3$. This number N_T satisfies

$$N_T < \frac{3}{2}\,T^2 \sum_{\substack{T < Q^\beta < 3T^2/4 \\ \beta \geqslant 3}} \frac{1}{Q^\beta},$$

which, in view of (12) and (13) and observing that β runs in the range $3 \leqslant \beta < 3 \log T$, gives

$$N_T < \frac{3}{2} T^2 \cdot \frac{33}{T^{2/3}}. \tag{19}$$

Using (18) and (19), and if T is large enough, we certainly have that

$$\pi\left(\frac{T^2}{2}\right) > \frac{1}{2} \frac{T^2/2}{\log(T^2/2)} > M_T + N_T,$$

which implies that there exists at least one prime $p < T^2/2$ satisfying $f(h_p) = h_p$, in which case, as we saw above, (16) follows.

It remains to consider the case $\pi = 2$. Then, for each prime p satisfying $2 < p < T^2/2$ and $p \equiv 2 \pmod 3$, define h_p as above, noticing that (17) is still valid. If $E_p < T$, then $f(h_p) = h_p = p + 2^{2\Delta}$, an equality which combined with (17) proves (16). Hence assume that $E_p \geqslant T$. We now analyse separately two possibilities: E_p is not a power of 3, or else it is. In the first case, we must have $3 \mid F_p$ and thus $E_p < \frac{3}{2} T^2/3 = T^2/2$ which implies that $E_p = Q^\gamma$ with $\gamma \geqslant 2$. If $\gamma = 2$, then $E_p = Q^2$ with $Q < T$, in which case $f(E_p) = f(Q^2) = f(Q)^2 = Q^2$ and since $F_p < T$, we have $f(F_p) = F_p$ and therefore $f(h_p) = h_p = p + 2^{2\Delta}$, which combined with (17) implies (16). For $\gamma \geqslant 3$, we proceed as above and obtain that the number N_T of those primes $p \leqslant T^2/2$ such that $Q^\gamma \mid p + 2^{2\Delta}$, $Q^\gamma > T$ and $\gamma \geqslant 3$, satisfies (19).

On the other hand, if $E_p = 3^\gamma \geqslant T$ for some $\gamma \geqslant 3$, we then have $p + 2^{2\Delta} = 3^\gamma F_p$. Let γ_0 be the smallest integer satisfying $3^{\gamma_0} > T$. But the number M_T of primes p satisfying $3^{\gamma_0} \mid p + 2^{2\Delta}$ is

$$M_T < \pi\left(\frac{T^2}{2}; -2^{2\Delta}, 3^{\gamma_0}\right),$$

and as previously we obtain that

$$M_T < \frac{4T}{\log T}.$$

Now, since (see McCurley [4]) $\theta(x; 2, 3) := \sum_{p \leqslant x,\, p \equiv 2 \pmod 3} \log p \geqslant 0,49042x$ holds for $x \geqslant 3761$, it follows that $(\log x)\, \pi(x; 2, 3) > 0,49x$ in the same range. Hence it is enough to prove that

$$\frac{0,49T^2/2}{\log(T^2/2)} > \frac{99}{2} T^{2-2/3} + \frac{4T}{\log T} \qquad (T \geqslant 10^6).$$

This clearly holds if

$$0,245 > \frac{50}{T^{2/3}} \log\left(\frac{T^2}{2}\right) + \frac{4\log(T^2/2)}{T\log T} \qquad (T \geqslant 10^6). \tag{20}$$

But the right hand side of (20) is certainly non increasing for $T \geqslant 10^6$ and, on the other hand in that range,

$$\frac{50}{T^{2/3}} \log\left(\frac{T^2}{2}\right) < 50\,\frac{\log 10^{12}}{10^4} = \frac{6}{100}\log 10 < 0,14$$

while

$$\frac{4\log(T^2/2)}{T\log T} < \frac{8}{T} < \frac{1}{10^5},$$

thereby proving (20). This ends the proof of Lemma 2.

As will be seen below, a crucial element in the proof of the Theorem rests on the fact that, given an odd prime q, there exists a prime number $p < q^3$ such that $(-p/q) = 1$. Better results exist concerning the size of the smallest prime quadratic residue modulo q. However, these results either involve non-effective constants or effective constants which are very large. Hence we state and prove the following lemma.

LEMMA 3. *Let q be an odd prime. Then there exists at least one prime $p < q^3$ such that $(-p/q) = 1$.*

Proof. Clearly if $q \equiv 3 \pmod 4$, the result follows easily. Since the result is true for $q = 3$, we may assume that $q \equiv 1 \pmod 4$. On the other hand, since $q = 5$ satisfies the conclusion, we may also assume that $q \geqslant 13$. To prove the lemma, we assume that the conclusion is false, that is that $(p/q) = -1$ for all primes $p < q^3$.

First define the real character $\chi(n) = (n/q)$ and the L-series $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$, and let

$$W := \max_{u < v} \left| \sum_{u \leqslant n \leqslant v} \chi(n) \right|.$$

It is known (see Polya [5]) that

$$W \leqslant \sqrt{q}\log q. \tag{21}$$

Further set

$$f(n) := \prod_{\pi^\alpha \parallel n} (1+\chi(\pi)+\chi(\pi^2)+ \cdots +\chi(\pi^\alpha)) = \sum_{d \mid n} \chi(d).$$

Observe that f is a multiplicative function and that, if $f(n) \neq 0$, then for each $\pi < q^3$, $\pi \neq q$, $\pi^\gamma \parallel n$ implies that γ is even.

Given an integer x, let $S = S(x) = \sum_{n \leqslant x} f(n)$. We write S as follows:

$$S = \sum_{d \leqslant x} \chi(d) \left[\frac{x}{d}\right] = \sum_{d \leqslant x} \chi(d)\frac{x}{d} - \sum_{d \leqslant x} \chi(d) \left\{\frac{x}{d}\right\} = E - J,$$

say. Furthermore write E as

$$E = x\sum_{d=1}^{\infty} \frac{\chi(d)}{d} - x\sum_{d>x} \frac{\chi(d)}{d} = xL(1,\chi) - x\sum_{d>x} \frac{\chi(d)}{d} \tag{22}$$

and define

$$S_x(v) := \sum_{x<n<v} \chi(n).$$

We have

$$\sum_{d>x} \frac{\chi(d)}{d} = \int_x^\infty \frac{1}{u}\,\mathrm{d}\,S_x(u) = \frac{S_x(u)}{u}\bigg|_x^\infty + \int_x^\infty \frac{S_x(u)}{u^2}\,\mathrm{d}\,u$$

$$= 0 + \int_x^\infty \frac{S_x(u)}{u^2}\,du < \int_x^\infty W\frac{du}{u^2} < \frac{W}{x}.$$

So far, we have thus established, in view of (22), that

$$|E - xL(1,\chi)| < W. \tag{23}$$

To estimate J, we let $y < x$ (y will be determined later) and write

$$J = \sum_{d \leqslant y} \chi(d) \left\{\frac{x}{d}\right\} + \sum_m L_m,$$

where in L_m we sum over those $d > y$ such that $[x/d] = m$. From this it follows that

$$|J| \leqslant y + \sum_{m \leqslant (x/y)} |L_m|. \tag{24}$$

Now let $I_m = \{d > y\colon [x/d] = m\}$, and let d_0 be the smallest $d \in I_m$ and d_1 be the largest $d \in I_m$. We write

$$L_m = \sum_{d \in I_m} \chi(d) \left(\frac{x}{d} - \frac{x}{d_1}\right) + \left\{\frac{x}{d_1}\right\} \sum_{d \in I_m} \chi(d) = A + B,$$

say. First

$$\begin{aligned} A &= \int_{d_1}^{d_0} \left(\frac{x}{u} - \frac{x}{d_1}\right) \mathrm{d}\, S_{d_1}(u) \\ &= S_{d_1}(u) \left(\frac{x}{u} - \frac{x}{d_1}\right) \Bigg|_{d_1}^{d_0} - x \int_{d_1}^{d_0} \frac{S_{d_1}(u)}{u^2}\, du \leqslant W + Wx \left(\frac{1}{d_0} - \frac{1}{d_1}\right) \leqslant 2W. \end{aligned}$$

From this estimate and the fact that $B \leqslant W$, it follows that $L_m \leqslant 3W$. Using this estimate, (24) becomes

$$|J| < y + 3W \frac{x}{y}. \tag{25}$$

We now set $x = q^3$, in which case and in view of the remark made above on f, we may write S as

$$S = \#\{n\colon n^2 \leqslant q^3\} + \#\{n\colon n^2 q \leqslant q^3\} = [q^{3/2}] + q. \tag{26}$$

It follows from (23), (25) and (26) that

$$|L(1, \chi)\, q^3| \leqslant q + W + y + 3W \frac{x}{y} + q^{3/2}. \tag{27}$$

We now look for an optimal choice for y, namely one for which $y = 3W(x/y)$, which means that $y = \sqrt{3Wx}$. Hence, from (27), we get

$$|L(1, \chi)\, q^3| \leqslant q + W + 2\sqrt{3}\, q^{3/2} \sqrt{W} + q^{3/2},$$

which implies using (21) that

$$|L(1, \chi)| < \frac{2\sqrt{3}\sqrt{\log q}}{q^{5/4}}. \tag{28}$$

We now look for a lower bound for $L(1, \chi)$ which will contradict (28). First observe that, since $q \equiv 1 \pmod 4$, it follows that $(-1)^{(q-1)/2} = 1$ and hence that

$$\chi(n) = \left(\frac{n}{q}\right) = \left(\frac{q}{n}\right).$$

This implies that, as is mentioned in Davenport [1], the discriminant q is positive.

On the other hand, from the Dirichlet class number formula, we have that

$$h(q) = \frac{\sqrt{q}}{\log \varepsilon} L(1, \chi),$$

where $h(q)$ is the class number of the field $\mathbb{Q}(\sqrt{q})$ with discriminant q (>0) and where $\varepsilon = \frac{1}{2}(t_0 + u_0\sqrt{q})$ is the smallest solution (with $t_0 > 0$ and $u_0 > 0$) of the Pell equation $t^2 - qu^2 = 4$. Since $\varepsilon > \frac{1}{2}(1 + \sqrt{q})$ and since $h(q)$ is an integer $\geqslant 1$, it follows that

$$L(1, \chi) \geqslant \frac{\log \varepsilon}{\sqrt{q}} > \frac{\log\{\frac{1}{2}(1 + \sqrt{q})\}}{\sqrt{q}},$$

which contradicts (28), since we have assumed that $q \geqslant 13$.

This ends the proof of Lemma 3.

We may now complete the proof of the Theorem.

For the moment, let us assume that q is odd, and let p be a prime smaller than q^3 such that $(-p/q) = 1$. Clearly, if $q > 3$, one can show that such a prime exists by Lemma 3. It means in particular that there exists $u_0 \in [1, q/2]$ such that

$$-p \equiv u_0^2 \pmod{q}.$$

One can then show that, for each $\alpha \geqslant 2$, there exists an integer $v_p \in [1, q^\alpha/2]$ such that

$$-p \equiv v_p^2 \pmod{q^\alpha}. \tag{29}$$

If $q = 3$, then (29) has a solution for $\alpha = 2$, and then consequently for each $\alpha \geqslant 2$. Hence, in any case, there exists an integer m_p such that

$$v_p^2 + p = m_p q^\alpha. \tag{30}$$

First we note that

$$m_p < q^\alpha. \tag{31}$$

This is true because

$$m_p < \left(\frac{q^{2\alpha}}{4} + q^\alpha\right)\frac{1}{q^\alpha} = \frac{q^\alpha}{4} + 1 < q^\alpha.$$

Then write

$$\begin{aligned}(q^{\alpha}-v_p)^2+p &= q^{2\alpha}-2q^{\alpha}v_p+v_p^2+p\\ &= q^{2\alpha}-2q^{\alpha}v_p+m_p q^{\alpha}\\ &= q^{\alpha}(q^{\alpha}-2v_p+m_p)=M_p q^{\alpha},\end{aligned} \tag{32}$$

say. Similarly it can be shown that

$$M_p < q^{\alpha}.$$

Observing that it follows from (30) and (32) that

$$M_p q^{\alpha}-m_p q^{\alpha}=q^{\alpha}(q^{\alpha}-2v_p),$$

that is

$$M_p-m_p=q^{\alpha}-2v_p$$

and hence, since $(q, v_p)=1$, we obtain that at least one of m_p or M_p is coprime to q.

If $(m_p, q)=1$, then

$$f(m_p q^{\alpha})=f(p)+f(v_p^2). \tag{33}$$

Similarly, if $(M_p, q)=1$, then

$$f(M_p q^{\alpha})=f(p)+f((q^{\alpha}-v_p)^2). \tag{34}$$

By hypothesis, we have $f(p)=p$, and, because of (31), we have that $f(m_p)=m_p$. Since v_p and $q^{\alpha}-v_p$ are smaller than T, then by Lemma 2, we have $f(v_p^2)=v_p^2$, and similarly, if (33) holds,

$$f((q^{\alpha}-v_p)^2)=(q^{\alpha}-v_p)^2.$$

Assume that (33) holds, then, since we assumed that $f(q^{\alpha})\neq q^{\alpha}$, we have

$$f(m_p q^{\alpha})=f(m_p)\, f(q^{\alpha})=m_p\, f(q^{\alpha})\neq m_p q^{\alpha},$$

which contradicts the fact that

$$f(m_p q^{\alpha})=f(p)+f(v_p^2)=p+v_p^2=m_p q^{\alpha}.$$

This implies that $f(q^{\alpha})=q^{\alpha}$, as we wanted to establish.

To complete the proof of the Theorem, it remains to consider the case $q=2$. We know that -7 is a quadratic residue modulo 2^{α} and therefore that for each $\alpha>3$, there exists $v_{\alpha}\in[0, 2^{\alpha-1}]$ such that $7+v_{\alpha}^2\equiv 0 \pmod{2^{\alpha}}$, and consequently, $7+(v_\alpha+2^{\alpha-1})^2\equiv 0 \pmod{2^\alpha}$. Define m_α and M_α by $7+v_\alpha^2=m_\alpha 2^\alpha$, and $7+(v_\alpha+2^{\alpha-1})^2=M_\alpha 2^\alpha$. We easily deduce from these two equations that

$$M_\alpha - m_\alpha = v_\alpha + 2^{\alpha-2}.$$

It follows from this relation and the fact that 2 does not divide v_α that v_α cannot both be even or odd at the same time, it follows that one of m_α or M_α is odd, that is that we either have $(m_\alpha, 2)=1$ or $(M_\alpha, 2)=1$, and the rest of the proof can thus be handled similarly as for the case "q odd" and we thus omit it.

REFERENCES

1. H. Davenport, "Multiplicative Number Theory," Lectures in Advanced Mathematics, Markham, Chicago, 1967.
2. H. Halberstam and H. E. Richert, "Sieve Methods," Academic Press, New York, 1974.
3. G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 4th ed., Clarendon Press, Oxford, 1960.
4. K. S. McCurley, Explicit estimates for $\theta(x; 3, \ell)$ and $\psi(x; 3, \ell)$, *Math. Comp.* **42** (1984), 287–296.
5. G. Polya, Über die Verteilung der quadratischen Reste und Nichtreste, *Göttinger Nachr.* (1918), 116–141.
6. J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.
7. C. Spiro, Additive uniqueness sets for arithmetic functions, *J. Number Theory* **42** (1992), 232–246.