Periodica Mathematica Hungarica Vol. 43 (1–2), (2001), pp. 81–91

ON THE GREATEST PRIME FACTOR OF INTEGERS OF THE FORM $ab+1$

C. L. Stewart (Waterloo)

Dedicated to Professor András Sárközy on the occasion of his 60th birthday

Abstract

Let N be a positive integer and let A and B be dense subsets of $\{1,\dots,N\}$. The purpose of this paper is to establish a good lower bound for the greatest prime factor of $ab+1$ as a and b run over the elements of A and B respectively.

1. Introduction

Let N be a positive integer and let A and B be subsets of $\{1,\dots,N\}$. A basic question of combinatorial number theory is the following. What can be deduced about the arithmetical character of integers of the form $a+b$ with a in A and b in B from information about the cardinalities of A and B? There is an extensive literature addressing this problem, see, for example, [1, 2, 3, 4, 5, 10, 16, 17, 21, 22, 23, 24], with the work of Sárközy being of central importance.

For any set X let $|X|$ denote the cardinality of X and for any integer n, larger than one, let $P(n)$ denote the greatest prime factor of n. Let ε be a positive real number and suppose that

$$|A|>\varepsilon N \quad \text{and} \quad |B|>\varepsilon N. \tag{1}$$

For example, in 1986, Sárközy and Stewart [22] proved, by means of the Hardy–Littlewood method, that there is a positive number $C(\varepsilon)$, which is effectively computable in terms of ε, such that if (1) holds then there exist integers a in A and b in B with

$$P(a+b)>C(\varepsilon)N. \tag{2}$$

In 1992 Ruzsa [17] gave a different proof of (2). Notice that $a+b$ is at most $2N$ and so estimate (2) is best possible up to a determination of $C(\varepsilon)$.

Research supported in part by Grant A3528 of the Natural Sciences and Engineering Research Council of Canada.

Mathematics subject classification numbers: primary 11N36; secondary 11L05.

Key words and phrases: greatest prime factor, Selberg's sieve, Kloosterman sums.

0031-5303/01/\$5.00 *Akadémiai Kiadó, Budapest*

Kluwer Academic Publishers, Dordrecht

The multiplicative analogue of our original question is one in which integers of the form $a+b$ are replaced by integers of the form $ab+1$. Recently there has been much work on this question, see, for example, [9, 19, 20, 25]. For the additive case $a+b$ is at most $2N$, whereas in the multiplicative case $ab+1$ may be as large as N^2+1. In [25], Sárközy and Stewart made the following conjecture.

Conjecture. *For each positive real number ε there are positive real numbers $N_0(\varepsilon)$ and $C_1(\varepsilon)$ such that if N exceeds $N_0(\varepsilon)$ and (1) holds, then there are a in A and b in B with*

$$P(ab+1) > C_1(\varepsilon)N^2.$$

We were not able to prove the conjecture. However we were able to prove the following result by means of an argument related to those used by Gallagher [7], Ruzsa [17], and Chebyshev [15].

Put

$$Z = \min(|A|, |B|). \tag{3}$$

For each positive real number ε there are numbers $N_1(\varepsilon)$ and $C_2(\varepsilon)$ which are effectively computable in terms of ε such that if N exceeds $N_1(\varepsilon)$ and

$$Z > C_2(\varepsilon)\frac{N}{\log N}, \tag{4}$$

then there are a in A and b in B such that

$$P(ab+1) > (1-\varepsilon)Z\log N. \tag{5}$$

The main purpose of this paper is to show that we can strengthen (5) considerably provided that we restrict the range given by (4) for Z.

Theorem 1. *Let N be a positive integer, let A and B be subsets of $\{1,\ldots,N\}$ and put $Z = \min(|A|,|B|)$. There are effectively computable positive numbers c_1, c_2 and c_3 such that if N exceeds c_1 and*

$$Z > c_2\frac{N}{\sqrt{(\log N)/\log\log N}}, \tag{6}$$

then there are a in A and b in B such that

$$P(ab+1) > N^{1+c_3(Z/N)^2}. \tag{7}$$

Our proof of Theorem 1 will employ a strategy first introduced by Hooley for his proof [13] that $P(n^2+1)$ exceeds $n^{11/10}$ for infinitely many integers n. In particular we will make use of estimates for Kloosterman sums as well as Selberg's upper bound sieve. Our application of Selberg's upper bound sieve will be similar to that of Greaves [8] in that we will be sieving a subset of $\mathbb{Z}\times\mathbb{Z}$ and not a set of integers; here $\mathbb{Z}$ denotes the set of integers.

For positive integers N and t we put

$$U_t(N) = \{(m,n)\in\mathbb{Z}\times\mathbb{Z} \mid 1\le m\le N,\ 1\le n\le N,\ t\mid mn+1\}.$$

Our plan is to sieve sets of the form $U_t(N)$ and so we require a sharp estimate for the cardinality of such sets. Of course if t divides N then we may decompose $\{(m,n) \mid 1 \le m,\ n \le N\}$ into $(N/t)^2$ blocks consisting of the Cartesian product of two complete sets of residues modulo t. Thus if t divides N, $|U_t(N)| = \varphi(t)(N/t)^2$. In general we deduce that

$$|U_t(N)| = \varphi(t)\left(\frac{N}{t} + O(1)\right)^2 = \frac{\varphi(t)}{t^2}N^2 + O(N). \tag{8}$$

However, such a result is not sufficiently precise for our purpose. To obtain a sharper estimate we appeal to Weil's estimates for Kloosterman sums [27]. For any positive integer n let $d(n)$ denote the number of divisors of n.

Theorem 2.

$$|U_t(N)| = \frac{\varphi(t)}{t^2}N^2 + O\left(t^{1/2}d(t)^{3/2}(\log t)^2 + \frac{Nd(t)\log t}{t}\right). \tag{9}$$

The above improvement on (8) allows us to sieve $U_t(N)$ when t is as large as N. For the proof of Theorem 1 it would have sufficed to establish (9) with $t^{1/2}$ in the O-term replaced by t^β for any real number β with $\beta < 1$.

2. Proof of Theorem 2

Denote $e^{2\pi i x}$ by $e(x)$. For each integer a

$$t^{-1} \sum_{-\frac{t}{2} < g \le \frac{t}{2}} e(ga/t) = \begin{cases} 1 & \text{if } t \mid a, \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$|U_t(N)| = \frac{1}{t^2} \sum_{-\frac{t}{2} < g,h \le \frac{t}{2}} \sum_{\substack{1 \le a,b \le t \\ ab \equiv -1 \,(\mathrm{mod}\, t)}} \sum_{1 \le m,n \le N} e\left(\frac{g(m-a) + h(n-b)}{t}\right).$$

For each integer a coprime with t let $\overline{a}$ denote the integer from $\{1, \ldots, t\}$ for which $a\overline{a} \equiv 1 \pmod t$. We have

$$|U_t(N)| = \frac{1}{t^2} \sum_{-\frac{t}{2} < g,h \le \frac{t}{2}} \sum_{\substack{a=1 \\ (a,t)=1}}^{t} \sum_{1 \le m,n \le N} e\left(\frac{g(m-a) + h(n+\overline{a})}{t}\right). \tag{10}$$

For integers g and h we put

$$S(g,h;t) = \sum_{\substack{a=1 \\ (a,t)=1}}^{t} e\left(\frac{ga + h\overline{a}}{t}\right). \tag{11}$$

It follows from (10) and (11) that

$$|U_t(N)| = \frac{1}{t^2} \sum_{-\frac{t}{2}<g,h\le\frac{t}{2}} S(-g,h;t) \sum_{1\le m,n\le N} e\left(\frac{gm+hn}{t}\right). \tag{12}$$

The terms with $g = h = 0$ contribute $N^2\varphi(t)/t^2$ to the right hand side of (12). Thus, we have

$$|U_t(N)| - N^2\varphi(t)/t^2 = L_1(N,t) + L_2(N,t) + L_3(N,t) \tag{13}$$

where

$$L_1(N,t) = \frac{1}{t^2}\left(\sum_{\substack{-\frac{t}{2}<g,h\le\frac{t}{2}\\ gh\neq 0}} S(-g,h;t) \sum_{1\le m,n\le N} e\left(\frac{gm+hn}{t}\right)\right),$$

$$L_2(N,t) = \frac{N}{t^2}\left(\sum_{\substack{-\frac{t}{2}<g\le\frac{t}{2}\\ g\neq 0}} S(-g,0;t) \sum_{1\le m\le N} e\left(\frac{gm}{t}\right)\right)$$

and

$$L_3(N,t) = \frac{N}{t^2}\left(\sum_{\substack{-\frac{t}{2}<h\le\frac{t}{2}\\ h\neq 0}} S(0,h;t) \sum_{1\le n\le N} e\left(\frac{hn}{t}\right)\right).$$

Employing the inequality

$$\sum_{1\le m\le N} e\left(\frac{gm}{t}\right) = O\left(\frac{t}{|g|}\right) \quad \text{for } 1\le |g| \le \frac{t}{2}$$

we deduce that

$$\begin{aligned} L_1(N,t) &= \frac{1}{t^2}\left(\sum_{\substack{-\frac{t}{2}<g,h\le\frac{t}{2}\\ gh\neq 0}} S(-g,h;t)\left(\sum_{1\le m\le N} e\left(\frac{gm}{t}\right)\sum_{1\le n\le N} e\left(\frac{hn}{t}\right)\right)\right)\\ &= O\left(\sum_{\substack{-\frac{t}{2}<g,h\le\frac{t}{2}\\ gh\neq 0}} \frac{|S(-g,h;t)|}{|g||h|}\right),\\ L_2(N,t) &= O\left(\frac{N}{t}\sum_{1\le|g|\le\frac{t}{2}} \frac{|S(-g,0;t)|}{|g|}\right) \end{aligned}$$

and

$$L_3(N,t) = O\left(\frac{N}{t}\sum_{1\le |h|\le \frac{t}{2}} \frac{|S(0,h;t)|}{|h|}\right).$$

It follows from a result of Estermann [6], based on the estimates of Weil [27] and a result of Salié [18] that

$$|S(-g,h;t)| \le d(t)t^{1/2}((h,t))^{1/2},$$

see, for example, (70) of [14]. Thus

$$\begin{aligned} L_1(N,t) &= O\left(\sum_{\substack{-\frac{t}{2}<g,h\le\frac{t}{2}\\ gh\neq 0}} \frac{d(t)t^{1/2}(h,t)^{1/2}}{|g||h|}\right) \\ &= O\left(d(t)t^{1/2}\log t \sum_{\substack{-\frac{t}{2}<h\le\frac{t}{2}\\ h\neq 0}} \frac{(h,t)^{1/2}}{|h|}\right). \end{aligned}$$

Since

$$\begin{aligned} \sum_{1\le h\le\frac{t}{2}} \frac{(h,t)^{1/2}}{h} &= \sum_{d|t}\sum_{\substack{1\le h\le\frac{t}{2}\\ (h,t)=d}} \frac{\sqrt{d}}{h} \le \sum_{d|t}\sum_{1\le k\le\frac{t}{2d}} \frac{1}{\sqrt{d}k} \\ &= O\left(\sum_{d|t}\frac{\log t}{\sqrt{d}}\right) = O\left(\log t\sum_{n=1}^{d(t)}\frac{1}{\sqrt{n}}\right) \\ &= O(d(t)^{1/2}\log t), \end{aligned}$$

we find that

$$L_1(N,t) = O(t^{1/2}d(t)^{3/2}(\log t)^2). \tag{14}$$

By Theorem 272 of [12], $|S(-g,0;t)| \le (g,t)$ and so

$$L_2(N,t) = O\left(\frac{N}{t}\sum_{g=1}^{t}\frac{(g,t)}{g}\right).$$

We have

$$\begin{aligned} \sum_{g=1}^{t}\frac{(g,t)}{g} &= \sum_{d|t}\sum_{\substack{g=1\\ (g,t)=d}}^{t}\frac{d}{g} \\ &\le \sum_{d|t}\sum_{k=1}^{\frac{t}{d}}\frac{1}{k} = O(d(t)\log t). \end{aligned}$$

Therefore

$$L_2(N,t) = O\left(\frac{N d(t)\log t}{t}\right). \tag{15}$$

In a similar fashion we deduce that

$$L_3(N,t) = O\left(\frac{N d(t)\log t}{t}\right). \tag{16}$$

Theorem 2 now follows from (13), (14), (15) and (16).

3. Preliminary lemmas

Let N be a positive integer, let A and B be subsets of $\{1,\ldots,N\}$ and put $Z = \min(|A|,|B|)$. Define E by

$$E = \prod_{a\in A,\ b\in B} (ab+1) \tag{17}$$

and put

$$E_1 = \prod_{p\le N} p^{\operatorname{ord}_p E}, \tag{18}$$

where the product is taken over primes p up to N and ord_p denotes the p-adic order.

Lemma 1. *Let $\varepsilon > 0$. There exists a positive number $N_0(\varepsilon)$, which is effectively computable in terms of ε, such that for $N > N_0(\varepsilon)$,*

$$\log E_1 < (1+\varepsilon) Z^2 \log N.$$

Proof. This follows from the proof of Theorem 2 of [25], see 4.14 of [25].

Let t be a positive integer. We define $f_t(d)$ for each positive integer d by

$$f_t(d) = \frac{d}{\prod\limits_{\substack{p\mid d\\ p\nmid t}} \left(1-\frac{1}{p}\right)}.$$

Observe that $f_t(d)$ is multiplicative and, for each positive integer n, put

$$g_t(n) = f_t(n)\prod_{p\mid n}\left(1-\frac{1}{f_t(p)}\right).$$

Since

$$f_t(p) = \begin{cases} p & \text{if } p \mid t \\ \frac{p^2}{p-1} & \text{if } p\nmid t, \end{cases}$$

we see that

$$g_t(n) = n \prod_{\substack{p\mid n \\ p\mid t}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p\mid n \\ p\nmid t}} \left(1 + \frac{1}{p(p-1)}\right). \tag{19}$$

For each integer z with $z \geq 2$ and each positive integer t, we put

$$V_t(z) = \sum_{n \leq z} \frac{\mu^2(n)}{g_t(n)}. \tag{20}$$

Let t and N be positive integers and let z be an integer with $1 \leq z \leq N$. We put $U_t(N, z) = \{(m, n) \mid 1 \leq m \leq N,\ 1 \leq n \leq N,\ t \mid mn + 1$, all prime factors of $(mn + 1)/t$ exceed $z\}$.

Lemma 2. *Let ε be a positive real number and let N, t and z be positive integers with $t > N^{2/3}$ and $z \geq 2$. Then*

$$|U_t(N, z)| \leq \frac{N^2 \varphi(t)}{V_t(z) t^2} + O_\varepsilon\left((t^{1/2} z^3)^{1+\varepsilon}\right).$$

Proof. We shall estimate $|U_t(N, z)|$ by means of Selberg's upper bound sieve [26], (see also [11] and [14]). We shall follow the approach taken in Chapter 1, Section 2 of [14].

For each real number z with $z \geq 2$ we sieve the set $U_t(N)$ by the primes p up to z. In other words, for each prime p we remove the pairs (m, n) from $U_t(N)$ for which p divides $(mn + 1)/t$. The set remaining is $U_t(N, z)$.

Note that by Theorem 2, for each positive integer d,

$$|U_{td}(N)| = \frac{|U_t(N)|}{f_t(d)} + R_d$$

where, since $t > N^{2/3}$,

$$R_d = O_\varepsilon\left((td)^{1/2+\varepsilon}\right). \tag{21}$$

Take

$$\lambda_d = \frac{f_t(d)}{V_t(z)} \sum_{sd \leq z} \frac{\mu(s)\mu(sd)}{g_t(sd)},$$

for $1 \leq d \leq z$. By Selberg's upper bound sieve, see (11), (15) and (16) of Chapter 1 of [14],

$$|U_t(N, z)| \leq \frac{|U_t(N)|}{V_t(z)} + O\left(\sum_{d_1, d_2 \leq z} |\lambda_{d_1}||\lambda_{d_2}||R_{[d_1, d_2]}|\right), \tag{22}$$

where $[d_1, d_2]$ denotes the least common multiple of d_1 and d_2. By (18) of Chapter 1 of [14], $|\lambda_d| \le 1$ and so by (21),

$$\sum_{d_1,d_2\le z} |\lambda_{d_1}||\lambda_{d_2}||R_{[d_1,d_2]}| = O_\varepsilon\left(\sum_{d_1,d_2\le z}(td_1d_2)^{1/2+\varepsilon}\right) = O_\varepsilon\left((t^{1/2}z^3)^{1+\varepsilon}\right),$$

and the result now follows from (22).

4. Proof of Theorem 1

Let ε be a positive real number and let $N_0, N_1, \ldots$ denote positive numbers which are effectively computable in terms of ε. Define E by (17) and E_1 by (18) and put $E_2 = E/E_1$. The proof proceeds by a comparison of estimates for E.

Clearly

$$E \ge \prod_{\substack{a\in A\\ a\ge\frac{\varepsilon Z}{10}}}\prod_{\substack{b\in B\\ b\ge\frac{\varepsilon Z}{10}}}\left(\left(\frac{\varepsilon Z}{10}\right)^2+1\right) \ge \left(\frac{\varepsilon Z}{10}\right)^{2\left(|A|-\frac{\varepsilon Z}{10}\right)\left(|B|-\frac{\varepsilon Z}{10}\right)} \ge \left(\frac{\varepsilon Z}{10}\right)^{2\left(1-\frac{\varepsilon}{10}\right)^2 Z^2}.$$

Thus, by (6),

$$\log E > (2-\varepsilon)Z^2\log N,$$

for $N > N_0$. By Lemma 1

$$\log E_1 < (1+\varepsilon)Z^2\log N,$$

for $N > N_1$, hence, for $N > N_2$,

$$\log E_2 > (1-2\varepsilon)Z^2\log N. \tag{23}$$

Let P denote the greatest prime factor of E. Then

$$E_2 \le \prod_{N\le p\le P} p^{\mathrm{ord}_p G}, \tag{24}$$

where

$$G = \prod_{1\le m,n\le N}(mn+1). \tag{25}$$

Put $P = NY$ and note that

$$\sum_{N<p\le NY}\mathrm{ord}_p G\;\log p = \sum_{N<p\le NY}\sum_{\substack{1\le m,n\le N\\ p\mid mn+1}}\log p. \tag{26}$$

Observe that

$$\sum_{N<p\le NY}\ \sum_{\substack{1\le m,n\le N\\ p\mid mn+1\\ mn+1\le \frac{N^2}{(\log N)^2}}} \log p \le 2 \sum_{\substack{1\le m,n\le N\\ mn+1\le \frac{N^2}{(\log N)^2}}} \log N \tag{27}$$
$$= O(N^2) = o(Z^2 \log N),$$

and so, by (23), (24), (25), (26) and (27), for $N > N_2$,

$$\sum_{N<p\le NY}\ \sum_{\substack{1\le m,n\le N\\ p\mid mn+1\\ mn+1> \frac{N^2}{(\log N)^2}}} \log p > (1-3\varepsilon) Z^2 \log N. \tag{28}$$

Put

$$S_t(N) = \sum_{\substack{1\le m,n\le N\\ mn+1=tp\\ N<p\le NY\\ mn+1> \frac{N^2}{(\log N)^2}}} 1.$$

If $Y > N^{1/4}$ the result holds and so we may suppose that $Y \le N^{1/4}$. Then, by (28),

$$\sum_{\frac{N}{Y(\log N)^2}<t\le N} \log\left(\frac{N^2+1}{t}\right) S_t(N) > (1-3\varepsilon) Z^2 \log N,$$

and so, for $N > N_3$,

$$\sum_{\frac{N}{Y(\log N)^2}<t\le N} S_t(N) > \frac{Z^2}{3}. \tag{29}$$

For each real number z with $2 \le z \le N$,

$$S_t(N) \le |U_t(N,N)| \le |U_t(N,z)|. \tag{30}$$

Let $c_4, c_5, \ldots$ denote effectively computable positive numbers. It follows from (19) that

$$g_t(n) \le c_4 n,$$

hence, by (20), that

$$V_t(z) > c_5 \log z. \tag{31}$$

We now apply Lemma 2 with $z = N^{1/7}$ and $\varepsilon = \frac{1}{20}$ to conclude, from (30) and (31), that for $N > N_3$ and $\frac{N}{Y(\log N)^2} < t \le N$,

$$S_t(N) < c_6 \frac{N^2 \varphi(t)}{(\log N) t^2},$$

and so

$$\sum_{\frac{N}{Y(\log N)^2}<t\leq N} S_t(N) < c_6 \frac{N^2}{\log N} \sum_{\frac{N}{Y(\log N)^2}<t\leq N} \frac{1}{t} \tag{32}$$
$$< c_7 \frac{N^2}{\log N}(\log Y + \log\log N).$$

Now provided that c_2 in (6) is chosen to exceed $(6c_7)^{\frac{1}{2}}$ we find that

$$c_7 \frac{N^2 \log\log N}{\log N} < \frac{Z^2}{6}$$

and so, from (29) and (32),

$$Z^2 < 6c_7 N^2 (\log Y)/\log N.$$

Therefore

$$Y > N^{c_8 (Z/N)^2}$$

and this completes the proof since $P = NY$.

REFERENCES

[1] A. Balog and A. Sárközy, On sums of sequences of integers, I, *Acta Arith.* **44** (1984), 73–86.

[2] A. Balog and A. Sárközy, On sums of sequences of integers, II, *Acta Math. Hung.* **44** (1984), 169–179.

[3] A. Balog and A. Sárközy, On sums of sequences of integers, III, *Acta Math. Hung.* **44** (1984), 339–349.

[4] P. Erdős, H. Maier and A. Sárközy, On the distribution of the number of prime factors of sums $a + b$, *Trans. Amer. Math. Soc.* **302** (1987), 269–280.

[5] P. Erdős, C. L. Stewart and R. Tijdeman, Some diophantine equations with many solutions, *Compositio Math.* **66** (1988), 37–56.

[6] T. Estermann, On Kloosterman's sum, *Mathematika* **8** (1961), 83–86.

[7] P. X. Gallagher, A larger sieve, *Acta Arith.* **18** (1971), 77–81.

[8] G. Greaves, Large prime factors of binary forms, *J. Number Theory* **3** (1971), 35–59.

[9] K. Győry, A. Sárközy and C. L. Stewart, On the number of prime factors of integers of the form $ab + 1$, *Acta Arith.* **74** (1996), 365–385.

[10] K. Győry, C. L. Stewart and R. Tijdeman, On prime factors of sums of integers, I, *Compositio Math.* **59** (1986), 81–88.

[11] H. Halberstam and K. F. Roth, *Sequences*, Oxford University Press, 1966.

[12] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edition, Oxford University Press, 1979.

[13] C. Hooley, On the greatest prime factor of a quadratic polynomial, *Acta Math.* **117** (1967), 281–299.

[14] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge University Press, 1976.

[15] A. A. Markov, Über die Primteiler der Zahlen von der Form $1 + 4x^2$, *Bull. Acad. Sci. St. Petersburg* **3** (1895), 55–59.
[16] C. Pomerance, A. Sárközy and C. L. Stewart, On divisors of sums of integers, III, *Pacific J. Math.* **133** (1988), 363–379.
[17] I. Ruzsa, Large prime factors of sums, *Studia Sci. Math. Hungar.* **27** (1992), 463–470.
[18] H. Salié, Über die Kloostermanschen Summen $S(u, v; q)$, *Math. Z.* **34** (1931), 91–109.
[19] A. Sárközy, On sums $a + b$ and numbers of the form $ab + 1$ with many prime factors, *Grazer Math. Ber.* **318** (1992), 141–154.
[20] A. Sárközy, On the average value for the number of divisors of numbers of form $ab + 1$, *Acta Math. Hungar.* **66** (1995), 223–245.
[21] A. Sárközy and C. L. Stewart, On divisors of sums of integers, I, *Acta Math. Hungar.* **48** (1986), 147–154.
[22] A. Sárközy and C. L. Stewart, On divisors of sums of integers, II, *J. Reine Angew. Math.* **365** (1986), 171–191.
[23] A. Sárközy and C. L. Stewart, On divisors of sums of integers, IV, *Canadian J. Math.* **40** (1988), 788–816.
[24] A. Sárközy and C. L. Stewart, On divisors of sums of integers, V, *Pacific J. Math.* **166** (1994), 373–384.
[25] A. Sárközy and C. L. Stewart, On prime factors of integers of the form $ab + 1$, *Publicationes Math. Debrecen* **56** (2000), 559–573.
[26] A. Selberg, On an elementary method in the theory of primes, *Norske Vid. Selsk. Fork.* (Trondheim) **19** (1947), 64–67.
[27] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207.

(Received: April 11, 2000)

C. L. Stewart
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1
E-mail: `cstewart@watserv1.uwaterloo.ca`