if h is of the shape $h = 3^r n - 3^{r-1} - \ldots - 3 - 1$ for some $n = 1, 2, \ldots$ chosen minimally.

The cases $k > 2$ even are quite different essentially because $x^k \equiv x \pmod 3$ for all $x \in \mathbf{Z}$ only if k is odd. The argument of [4] is rather different, but its main result can also be obtained from transition formulae of the sort displayed at Lemma 1. Those formulae turn out to be somewhat more natural than those required here and we leave them as an exercise for the mildly energetic reader.

Cases where truncations of the product do not yield partial quotients seem more difficult.

Our indebtedness to an idea of Mills and Robbins will be evident to readers familiar with their paper [5].

References

[1] L. E. Baum and M. M. Sweet, *Continued fractions of algebraic power series in characteristic 2*, Ann. of Math. 103 (1976), 593–610.
[2] M. Mendès France and A. J. van der Poorten, *Automata and the arithmetic of formal power series*, Acta Arith. 46 (1986), 211–214.
[3] –, ––, *From geometry to Euler identities*, Theoret. Comput. Sci. 65 (1989), 213–220.
[4] –, –, *Some explicit continued fraction expansions*, Mathematika (to appear).
[5] W. H. Mills and D. P. Robbins, *Continued fractions for certain algebraic power series*, J. Number Theory 23 (1986), 388–404.
[6] G. N. Raney, *On continued fractions and finite automata*, Math. Ann. 206 (1973), 265–283.
[7] A. J. van der Poorten, *Fractional parts of the period of the continued fraction expansion of quadratic integers*, Bull. Austral. Math. Soc. 44 (1991), 155–169.

Jean-Paul Allouche and Michel Mendès France

CNRS AND UER MATHÉMATIQUES ET INFORMATIQUE
UNIVERSITÉ BORDEAUX I
351, cours de la Libération
F-33405 Talence cedex
France
allouche@frbdx11.bitnet

Alfred J. van der Poorten

SCHOOL OF MATHEMATICS, PHYSICS, COMPUTING AND ELECTRONICS
MACQUARIE UNIVERSITY NSW 2109
Australia
alf@mqcomp.mqcs.mq.oz.au

Received on 5.6.1990 (2052)

ACTA ARITHMETICA
LIX.2 (1991)

On $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ and Rosser's sieve

by

J. W. Sander (Hannover)

1. Introduction. An old conjecture of Erdős and Straus says that for any given integer $n > 1$, the equation

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \tag{1}$$

has a solution in positive integers x, y, z. For references to the huge amount of (partial) results concerning the conjecture as well as its generalizations by Sierpiński, Schinzel and others, we refer the reader to [1], problem D 11, and [9].

We just like to mention an outstanding result by Vaughan [11] which gives an upper bound for the exceptional set $E_m(N)$ of integers $n \leqslant N$ for which $m/n = 1/x + 1/y + 1/z$ has no solution ($m \geqslant 4$ is a fixed integer), namely

$$E_m(N) \ll N \exp\bigl(-c(\log N)^{2/3}\bigr),$$

where c may only depend on m.

In order to prove the conjecture it obviously suffices to solve (1) for all primes q (instead of n). Moreover, one can easily see that, if there is a solution of $4/q = 1/x + 1/y + 1/z$, then either exactly one of the numbers x, y, z is divisible by q, or exactly two of them have a divisor q. The second case, namely the equation

$$\frac{4}{q} = \frac{1}{w} + \frac{1}{gq} + \frac{1}{hq} \tag{2}$$

for a given prime q, is equivalent to the solvability of

$$(4g-1)(4h-1) = 4tq+1, \quad t \mid gh, \tag{3}$$

in positive integers g, h, t (see [9]). In [9] lower bounds for

$$V(x; k, l; t) = \operatorname{card}\{q \leqslant x:\ q \equiv l \bmod k,\ (2) \text{ unsolvable with } gh/w = t\}$$

have been given, where k and l are integers satisfying $(k, l) = 1$ (gh/w is always an integer). Only for $t = 1$, an asymptotic formula was obtained. In this paper we will improve upon these estimates by giving asymptotic formulae for all primes t.

It is known that for $n \not\equiv 1 \bmod 24$, solutions of (1) may be found constructively (with a little more effort the remaining residue class $n \equiv 1 \bmod 24$ can be reduced to an even thinner set of possible exceptions to the conjecture of Erdős and Straus). This is the reason for the condition $q \equiv l \bmod k$ in the definition of $V(x; k, l; t)$ which allows us to get results not obtainable by much simpler methods.

Throughout this paper, let p, q, t (with or without subscripts) be primes. Furthermore, let

$$G(4t) = \{a:\ 1 \leqslant a \leqslant 4t,\ (a, 4t) = 1\}$$

be the prime residue group mod $4t$. Occasionally, we will not distinguish between the element $a \in G(4t)$ and the congruence class $a \bmod 4t$. It will be shown that $G(4t)$ has exactly two subgroups U_1, U_2 satisfying

$$|U_i| = \tfrac{1}{2}|G(4t)|, \qquad -1 \notin U_i \quad (i = 1, 2).$$

For an integer m and an arbitrary subset $H \subseteq G(4t)$, we will write "$m \in H$" instead of "$m \equiv h \bmod 4t$ for some $h \in H$". By $(\cdot/t)$ we will denote the Legendre symbol mod t. Constants $c_1, c_2, \ldots, O(\ )$ and Vinogradov's $\ll$ may depend on parameters t, k, l, ε and ε', but must not depend on the real variable x.

THEOREM. *Let t be prime, $(k, l) = 1$. Let*

$$p \nmid (4tl+1) \quad \text{or} \quad (p/t) = 1, \quad p \equiv 1 \bmod 4 \tag{4}$$

for all $p \mid k$ (for $t = 2$, the condition "$(p/t) = 1$" has to be replaced by "$p \equiv 1 \bmod 8$"). Moreover, let $0 < \varepsilon < 1/6$, and $\varepsilon' > 0$. Then

$$V(x; k, l; t) = \frac{1}{\varphi(k)}\left(\frac{8t}{\pi(t-1)}\right)^{1/2}(\lambda(U_1)+\lambda(U_2))\frac{x}{(\log x)^{3/2}}(1+O(\varepsilon^{\gamma}))$$

$$+O\big(x(\log x)^{-3/2-1/(2t-2)+\varepsilon'}\big)+O(E(x, x^{1-\varepsilon})),$$

where

$$\gamma = \frac{1}{2}-\frac{1}{(2-\log 2)e}, \qquad E(X, K) = \sum_{u<K\ (v,u)=1}\max\left|\pi(X; u, v)-\frac{\operatorname{Li} X}{\varphi(u)}\right|,$$

$$\lambda(U_i) = L(1, \chi_{U_i})^{1/2}\prod_{p\in G(4t)\setminus U_i}\left(1-\frac{1}{p^2}\right)^{-1/2}\left(1-\frac{2}{p(p-1)}\right),$$

and χ_{U_i} ($i = 1, 2$) is the character mod $4t$ *defined by the subgroup U_i of $G(4t)$* (see Lemma 5 (v)).

Remark. Obviously, the condition of the theorem holds if (4) is replaced by the simpler condition "$(k, 4tl+1) = 1$". The theorem implies that an unconditional asymptotic formula would follow from the well known Halberstam conjecture (see [8], p. 137.).

2. Preliminaries.

LEMMA 1. *Let t be prime. Then*

$$(4g-1)(4h-1) = 4tq+1, \qquad t \mid gh \tag{5}$$

is unsolvable in positive integers g and h if and only if

$$d \not\equiv -1 \bmod 4t \quad \text{for all } d \mid (4tq+1). \tag{6}$$

Proof. Since t is prime, and $t \mid gh$ in (5), we may assume $t \mid g$. Hence (5) is unsolvable if and only if

$$(4tg'-1)(4h-1) = 4tq+1 \tag{7}$$

is unsolvable. Clearly, (6) implies the unsolvability of (7). Now suppose that $d \equiv -1 \bmod 4t$ for some $d \mid (4tq+1)$, $d = 4tm-1$, say, for some positive integer m. Thus there is a positive integer m' satisfying

$$4tq+1 = (4tm-1)(2m'-1).$$

This implies $2 \mid m'$. Then (7) has a solution, namely $g' = m$, $h = m'/2$.

LEMMA 2. *Let G be a finite abelian group of even order. Let $H \subseteq G$ with $|H| \geqslant \frac{1}{2}|G|+1$. Then for all $g \in G$, there are $h_1, h_2 \in H$ such that $g = h_1 h_2$.*

Proof. Clearly,

$$\operatorname{card}\{(g_1, g_2) \in G^2:\ g_1 g_2 = g\} = |G|.$$

Let $H_1 \subseteq G$, $|H_1| \geqslant 1$, and $H_2 \subseteq H_1$, $|H_2| = |H_1|-1$. If

$$\operatorname{card}\{(h_1, h_2) \in H_1^2:\ h_1 h_2 = g\} = b,$$

then

$$\operatorname{card}\{(h_1, h_2) \in H_2^2:\ h_1 h_2 = g\} \geqslant b-2.$$

By induction we get

$$\operatorname{card}\{(h_1, h_2) \in H^2:\ h_1 h_2 = g\} \geqslant |G|-2|G\setminus H| = 2|H|-|G| \geqslant 2.$$

LEMMA 3. *Let $t > 2$ be prime. Then there is $g \in G(4t)$ such that*

$$G(4t) = \{g, g^2, \ldots, g^{t-1}, -g, -g^2, \ldots, -g^{t-1}\}.$$

Proof. It is well known that, if g_1 is a primitive root mod t, then $g_2 = g_1$ is a primitive root mod $2t$ for $2 \nmid g_1$, and $g_2 = g_1+t$ is a primitive root mod $2t$

for $2|g_1$ (see [4, Theorem 3.9.1]). Thus we always have an odd primitive root $g_2 \bmod 2t$.

If $g_2^j \not\equiv -1 \bmod 4t$ for $1 \leqslant j \leqslant t-1$, then set $g = g_2$. Now suppose that $g_2^m \equiv -1 \bmod 4t$. Then $2 \nmid m$, because -1 is no square mod 4. Since g_2 and m are both odd, we have

$$(g_2+2t)^m \equiv g_2^m + 2mtg_2^{m-1} \equiv g_2^m + 2t \bmod 4t.$$

Let $g = g_2+2t$. Obviously, g is an odd primitive root mod $2t$, and

$$g^j \equiv g_2^j \bmod 2t \quad (1 \leqslant j \leqslant t-1),$$

hence $g^j \not\equiv -1 \bmod 4t$ for $1 \leqslant j \leqslant t-1$. In any case, we have a primitive root $g \bmod 2t$, $g \in G(4t)$, satisfying

$$g^j \not\equiv -1 \bmod 4t \quad (1 \leqslant j \leqslant t-1).$$

It is easily seen that the numbers

$$g, g^2, \ldots, g^{t-1}, -g, -g^2, \ldots, -g^{t-1}$$

are pairwise incongruent mod $4t$. This proves the lemma.

LEMMA 4. *Let $t > 2$ be prime. Then*
(i) *$G(4t)$ contains exactly $(t-1)/2$ squares;*
(ii) *a is a square in $G(4t)$ if and only if*

$$\left(\frac{a}{t}\right) = 1 \quad \text{and} \quad a \equiv 1 \bmod 4.$$

Proof. (i) We have

$$G(4t) = \{a: 1 \leqslant a \leqslant 4t, (a, 4t) = 1\}.$$

Clearly, for $1 \leqslant a \leqslant t$

$$a^2 \equiv (2t-a)^2 \equiv (2t+a)^2 \equiv (4t-a)^2 \bmod 4t.$$

Thus it suffices to show that we have for $1 \leqslant a_1 < a_2 \leqslant t$, $2 \nmid a_1 a_2$,

$$a_1^2 \not\equiv a_2^2 \bmod 4t.$$

Assuming $a_2^2 \equiv a_1^2 \bmod 4t$, we get

$$(a_2-a_1)(a_2+a_1) \equiv 0 \bmod t.$$

Since $0 < a_2-a_1 < t$, we have $t|(a_2+a_1)$, which implies $t = a_2+a_1$, thus $2|t$. This is a contradiction.

(ii) First let a be a square in $G(4t)$, which means that there is $b \in G(4t)$ such that

$$a \equiv b^2 \bmod 4t.$$

This implies $a \equiv b^2 \bmod t$, i.e. $(a/t) = 1$, and $a \equiv b^2 \bmod 4$, hence $a \equiv 1 \bmod 4$, since $2 \nmid a$.

Now assume that $(a/t) = 1$ and $a \equiv 1 \bmod 4$. By the above argument

$$Q := \{a: 1 \leqslant a \leqslant 4t, (a/t) = 1, a \equiv 1 \bmod 4t\} \supseteq \{a \in G(4t): a \text{ is square}\}.$$

Exactly one of the numbers d, $d+t$, $d+2t$, $d+3t$ is congruent to 1 mod 4. Therefore,

$$\operatorname{card} Q = \operatorname{card}\{a: 1 \leqslant a \leqslant t, (a/t) = 1\} = (t-1)/2.$$

By (i), the proof is finished.

LEMMA 5. *Let t be prime.*
(i) *$G(4t)$ has exactly three subgroups U_1, U_2, U_3 with*

$$|U_i| = \tfrac{1}{2}|G(4t)| = t-1 \quad (i = 1, 2, 3).$$

(ii) *U_i $(i = 1, 2, 3)$ contains all the squares of $G(4t)$.*
(iii) *For each non-square $a \in G(4t)$, there is exactly one $i \in \{1, 2, 3\}$ such that $a \in U_i$.*
(iv) *$G(4t)$ has exactly two subgroups U_1, U_2, say, with*

$$|U_i| = \tfrac{1}{2}|G(4t)| \quad \text{and} \quad -1 \notin U_i \quad (i = 1, 2).$$

(v) *The function $\chi_{U_i}: G(4t) \to \boldsymbol{C}$ defined by*

$$\chi_{U_i}(a) = \begin{cases} 1 & \text{for } a \in U_i, \\ -1 & \text{for } a \in G(4t) \setminus U_i, \\ 0 & \text{otherwise}, \end{cases} \quad (i = 1, 2, 3)$$

is a character mod $4t$.

Proof. For $t = 2$, the lemma is easily seen to be true. Therefore, we may assume $t > 2$. We use the representation of Lemma 3, namely

$$G(4t) = \{g, g^2, \ldots, g^{t-1}, -g, -g^2, \ldots, -g^{t-1}\}. \tag{8}$$

(i) By the duality principle for finite abelian groups [3, p. 213], the number of subgroups of $G(4t)$ of order $\frac{1}{2}|G(4t)|$ is equal to the number of subgroups of order 2. Since 1 is self-inverse, but of order 1, it remains to show that $G(4t)$ contains exactly four self-inverse elements.

Since g in (8) is a primitive root mod $2t$, we have

$$g^j \not\equiv 1 \bmod 4t \quad (1 \leqslant j \leqslant t-2),$$

and

$$g^{t-1} \equiv 1 \bmod 4t,$$

because there are no primitive roots mod $4t$. Thus the congruence $a^2 \equiv 1 \bmod 4t$ obviously has the four solutions $a = \pm g^{(t-1)/2}, \pm g^{t-1}$. Others do not exist by the above remark.

(ii) Suppose that $g^2 \notin U_i$, hence $g \notin U_i$. This implies that if $g^j \in U_i$ then g^{j+1}, $g^{j+2} \notin U_i$, and similarly, if $-g^j \in U_i$ then $-g^{j+1}$, $-g^{j+2} \notin U_i$. We get $|U_i| \leqslant \frac{1}{3}(2t-2)$, but $|U_i| = t-1$. Therefore, $g^2 \in U_i$, and it follows that

$$g^2, g^4, \ldots, g^{t-1} \in U_i,$$

which by Lemma 4 (i) are the $(t-1)/2$ squares of $G(4t)$.

(iii) Let $a \in U_i$ for some $i \in \{1, 2, 3\}$, a not a square. By (ii), we have g^2, $g^4, \ldots, g^{t-1} \in U_i$, hence

$$ag^2, ag^4, \ldots, ag^{t-1} \in U_i.$$

These $t-1$ numbers are pairwise incongruent mod $4t$, thus U_i is uniquely determined. Therefore, a cannot occur in more than one U_i.

By Lemma 4 (i), $G(4t)$ contains exactly $\frac{3}{2}(t-1)$ non-squares. By (ii), U_i contains $(t-1)/2$ non-squares, and these are distinct from all the non-squares in U_j, $j \neq i$. By (i), this proves the claim.

(iv) Since $a^2 \not\equiv -1 \bmod 4$ for all a, -1 is a non-square in $G(4t)$. Thus (iv) follows from (i) and (iii).

(v) We have to show that for $a, b \in G(4t)$

$$\chi_{U_i}(ab) = \chi_{U_i}(a)\chi_{U_i}(b). \tag{9}$$

This is clear except for the case $a, b \in G(4t) \setminus U_i$. But then $aU_i = bU_i$, and there is $d \in U_i$ such that $a = db$, which by (ii) implies $ab = db^2 \in U_i$, and (9) is satisfied.

LEMMA 6. *Let $n \geqslant 3$, m an arbitrary positive integer; let $1 \leqslant a_1 < a_2 < \ldots < a_m = 2n$. Let one of the following two conditions be satisfied:*

(i) $m = n$; at least one a_j is odd; $n \geqslant 4$ or $\{a_i\} \neq \{1, 5, 6\}$;

(ii) $m = n-1$; $n \geqslant 5$ or $\{a_i\} \neq \{a_1, 6\}$ $(1 \leqslant a_1 \leqslant 5)$ or $\{a_i\} \neq \{a_1, 8-a_1, 8\}$ $(1 \leqslant a_1 \leqslant 3)$.

Then there are $a_i \neq a_j$ such that for all a_k

$$a_i + a_j \not\equiv a_k \bmod 2n. \tag{10}$$

Proof. We suppose that the conclusion (10) of the lemma is wrong, i.e. for all $a_i \neq a_j$, there is a_k such that

$$a_i + a_j \equiv a_k \bmod 2n. \tag{11}$$

We have

$$a_2 + a_1 < a_3 + a_1 < \ldots < a_{m-1} + a_1 < a_m + a_1 = 2n + a_1.$$

Obviously, $a_m + a_1 \equiv a_1 \bmod 2n$, and by (11)

$$a_1 = \min\{b > 0 : b \equiv a_j + a_1 \bmod 2n,\ 2 \leqslant j \leqslant m\}. \tag{12}$$

Thus $a_{m-1} + a_1 \leqslant a_m = 2n$, because otherwise $a_{m-1} + a_1 \equiv b \bmod 2n$ for some $1 \leqslant b < a_1$, which contradicts (12). On the other hand, $a_{m-1} + a_1 < a_m$ implies $a_{m-1} + a_1 \leqslant a_{m-1}$ by (11), but $a_1 \geqslant 1$. Therefore, we have

$$a_{m-1} + a_1 = a_m.$$

By induction, we get

$$a_j + a_1 = a_{j+1} \quad (2 \leqslant j \leqslant m-1).$$

This yields

$$2n = a_m = a_{m-1} + a_1 = a_{m-2} + 2a_1 = \ldots = a_2 + (m-2)a_1. \tag{13}$$

Case 1: $m = n$. For $a_1 \geqslant 3$, we find by (13) and $n \geqslant 3$ that $a_2 \leqslant 3$, which is impossible. For $a_1 = 2$, (13) implies

$$a_j = 2j \quad (1 \leqslant j \leqslant n),$$

which contradicts (i). It remains to consider $a_1 = 1$. Then by (13)

$$a_j = n + j \quad (2 \leqslant j \leqslant n). \tag{14}$$

For $n = 3$, this yields

$$a_1 = 1, \quad a_2 = 5, \quad a_3 = 6,$$

which is excluded by (i). For $n \geqslant 4$, we have

$$a_2 + a_3 = 2n + 5 \equiv 5 \bmod 2n,$$

but $5 \notin \{a_i\}$ by (14).

Case 2: $m = n-1$. For $n = 3$ respectively $n = 4$, we get by (13) $a_1 < a_2 = 6$ respectively $a_1 < a_2 = 8 - a_1 < a_3 = 8$, which both contradict (ii). For $n = 5$, (13) yields

$$a_1 < a_2 = 10 - 2a_1 < a_3 = 10 - a_1 < a_4 = 10.$$

Obviously, $a_1 \in \{1, 2, 3\}$, but then

$$a_2 + a_3 \not\equiv a_i \bmod 10$$

for all a_i.

By the above consideration, we may assume that $n \geqslant 6$. For $a_1 \geqslant 3$, we deduce by (13) that $a_2 \leqslant 3$, which is impossible. For $a_1 = 2$, (13) implies

$$a_j = 2j + 2 \quad (2 \leqslant j \leqslant n-1),$$

but then for $n \geqslant 6$

$$a_2 + a_{n-2} \equiv 4 \not\equiv a_i \bmod 2n$$

for all a_i. Finally, for $a_1 = 1$, we have by (13)

$$a_j = n + j + 1 \quad (2 \leqslant j \leqslant n-1).$$

For $n \geqslant 6$,

$$a_2 + a_3 \equiv 7 \not\equiv a_i \bmod 2n$$

for all i. This finishes the proof.

LEMMA 7. *Let t be prime. Let $H \subseteq G(4t)$, H not a subgroup of $G(4t)$, and $|H| = \frac{1}{2}|G(4t)|$. Then one of the following conditions holds:*

(i) $-1 \in H$;

(ii) $h_1 h_2 = -1$ *for some* $h_1, h_2 \in H$;

(iii) $h_1 h_2 h_3 = -1$ *for some pairwise distinct* $h_1, h_2, h_3 \in H$;

(iv) $t = 5$; $H \in \mathscr{H}_5 := \{H_1, H_2, H_3, H_4\}$, *where* $H_1 = \{1, 3, 7, 11\}$, $H_2 = \{1, 11, 13, 17\}$, $H_3 = \{1, 3, 11, 17\}$, $H_4 = \{1, 7, 11, 13\}$;

(v) $t = 7$; $H \in \mathscr{H}_7 := \{H_5, H_6\}$, *where* $H_5 = \{1, 3, 5, 15, 17, 19\}$, $H_6 = \{1, 3, 11, 13, 19, 23\}$.

Proof. It is easily seen that for $t = 2$ and $t = 3$ either (i) or (ii) holds. Thus we may assume that $t \geqslant 5$. Moreover, we suppose that (i) and (ii) are not satisfied, i.e.

$$-1 \notin H \quad \text{and} \quad h_1 h_2 \neq -1 \quad (h_1, h_2 \in H). \tag{15}$$

We will prove that this implies (iii), (iv) or (v).

By Lemma 3, there are non-negative integers r and s with $r+s = t-1 = |H|$, and non-negative integers

$$1 \leqslant a_1 < \ldots < a_r \leqslant t-1, \quad 1 \leqslant b_1 < \ldots < b_s \leqslant t-1$$

such that

$$H = \{g^{a_1}, \ldots, g^{a_r}, -g^{b_1}, \ldots, -g^{b_s}\}.$$

Since g is a primitive root $\bmod 2t$, we have

$$g^{t-1} \equiv 1 \bmod 2t.$$

There is no primitive root $\bmod 4t$, thus

$$-g^{t-1} \equiv -1 \bmod 4t, \tag{16}$$

which yields by (15)

$$b_j < t-1 \quad (1 \leqslant j \leqslant s). \tag{17}$$

The congruence

$$g^{a_i} x \equiv -1 \bmod 4t$$

has a unique solution in $G(4t)$, namely $x = -g^{t-1-a_i}$. Now (15) implies

$$g^{a_i} \in H \Leftrightarrow -g^{t-1-a_i} \notin H. \tag{18}$$

In particular, we get by (15) and (18)

$$1 \in H, \quad \text{i.e. } a_r = t-1, \tag{19}$$

and that

$$E := \{a_1, \ldots, a_r, b_1, \ldots, b_s\}$$

satisfies

$$|\{e \in E: 2|e\}| = |\{e \in E: 2 \nmid e\}| = (t-1)/2. \tag{20}$$

Case 1: $r > s$. We may assume $s > 0$, since otherwise H would be a subgroup of $G(4t)$. First consider the case where $2 \nmid b_j$ for some j. If x and y independently run through the set $\{a_i\}$, then by the pigeon-hole principle, there are $x = a_i$, $y = a_k$ such that

$$x \equiv -b_j - y \bmod t-1,$$

thus

$$a_i + a_k \equiv -b_j \bmod t-1.$$

Since $2 \nmid b_j$, we have $a_i \neq a_k$, and by (16)

$$g^{a_i} g^{a_k} (-g^{b_j}) \equiv -1 \bmod 4t,$$

i.e. (iii) holds.

In case $2|b_j$ for all j, we have $\{1, 3, 5, \ldots, p-2\} \subseteq \{a_i\}$ by (20). Hence for $t > 5$ and $2|m$, there are $a_i \neq a_k$ such that

$$m \equiv a_i + a_k \bmod t-1, \tag{21}$$

because $2 \equiv (t-2)+3 \bmod t-1$ and $t-2 > 3$, and for $1 < n \leqslant (t-1)/2$,

$$m = 2n \equiv (2n-1)+1 \bmod t-1,$$

where $2n-1 > 1$. Setting $m = t-1-b_j$ in (21), we have $a_i \neq a_k$ such that by (16)

$$g^{a_i} g^{a_k} (-g^{b_j}) \equiv -1 \bmod 4t.$$

It remains to consider $t = 5$, where $\{a_i\} = \{1, 3, 4\}$, $b_1 = 2$. Possible values for g in Lemma 3 are $g = 3, 7, 13, 17$. This implies that $H = H_1$ or $H = H_2$, i.e. H is one of the sets in (iv).

Case 2: $r < s-1$. By (20) there exists an odd b_{j_0}. If x and y run through $\{b_j\} \setminus \{b_{j_0}\}$ independently, then the pigeon-hole principle guarantees $x = b_j$ and $y = b_k$ such that

$$x \equiv t-1-b_{j_0}-y \bmod t-1,$$

hence

$$b_j + b_k + b_{j_0} \equiv 0 \bmod t-1. \tag{22}$$

By construction, $b_j \neq b_{j_0}$ and $b_k \neq b_{j_0}$. Moreover, $b_j \neq b_k$, since $2 \nmid b_{j_0}$. Thus (22) and (16) yield (iii), namely

$$(-g^{b_j})(-g^{b_k})(-g^{b_{j_0}}) \equiv -1 \bmod 4t.$$

Case 3: $r = s$. If all the a_i's are even, then by (20) all the b_j's are odd. This implies that H is a subgroup of $G(4t)$, which contradicts the initial condition of the lemma. Thus there is an a_{i_0} with

$$2 \nmid a_{i_0}. \tag{23}$$

We apply Lemma 6 (i) with $m = n = (t-1)/2$. For $t \geqslant 11$, there are $a_i \neq a_k$ and $a \notin \{a_i\}$, $0 \leqslant a < t-1$, such that

$$a_i + a_k \equiv a \mod t-1.$$

By (18), there is b_j satisfying $b_j = t-1-a$, hence by (16)

$$g^{a_i} g^{a_k} (-g^{b_j}) \equiv -1 \mod 4t.$$

By Lemma 6 (i), the same holds for $t = 7$, except for $a_1 = 1$, $a_2 = 5$, $a_3 = 6$, which implies $b_1 = 2$, $b_2 = 3$, $b_3 = 4$ by (18). Possible values for g in Lemma 3 are $g = 5, 11, 17, 23$, thus $H \in \mathscr{H}_7$, and H is of the form (v).

For $t = 5$, we have by (23), (19) and (18) only the cases

$$a_1 = 1,\ a_2 = 4;\quad b_1 = 1,\ b_2 = 2 \quad \text{or} \quad a_1 = 3,\ a_2 = 4;\quad b_1 = 2,\ b_2 = 3.$$

Since g may take on one of the values $g = 3, 7, 13, 17$, we get $H = H_3$ or $H = H_4$, which are sets in (iv).

Case 4: $r = s-1$. We apply Lemma 6 (ii) with $n = (t-1)/2$, $m = (t-3)/2$. For $t \geqslant 11$, there are $a_i \neq a_k$ and $a \notin \{a_i\}$, $0 \leqslant a < t-1$, such that

$$a_i + a_k \equiv a \mod t-1.$$

By (18), there is b_j satisfying $b_j = t-1-a$, hence by (16)

$$g^{a_i} g^{a_k} (-g^{b_j}) \equiv -1 \mod 4t.$$

By Lemma 6 (ii), the same holds for $t = 7$, except for $1 \leqslant a_1 \leqslant 5$ and $a_2 = 6$, which by (18) implies

$$\{b_j\} = \{b:\ 1 \leqslant b \leqslant 5,\ b \neq 6-a_1\}.$$

Whenever $\{1, 2, 3\} \subseteq \{b_j\}$ or $\{3, 4, 5\} \subseteq \{b_j\}$, then there obviously are pairwise distinct b_i, b_j, b_k such that

$$b_i + b_j + b_k \equiv 0 \mod t-1,$$

hence by (16)

$$(-g^{b_i})(-g^{b_j})(-g^{b_k}) \equiv -1 \mod 4t.$$

The only remaining case is

$$a_1 = 3,\ a_2 = 6;\quad b_1 = 1,\ b_2 = 2,\ b_3 = 4,\ b_4 = 5.$$

Possible values for g are $g = 5, 11, 17, 23$, which all yield sets H of (v).

For $t = 5$, we get by (19) and (18)

$$a_1 = 4;\quad b_1 = 1,\ b_2 = 2,\ b_3 = 3.$$

The values $g = 3, 7, 13, 17$ yield sets H of (iv).

LEMMA 8. *Let $H \in \mathscr{H}_5$ respectively $H \in \mathscr{H}_7$ (as defined in Lemma 7). Then there are $h_1, h_2 \in H$, $h_1 \neq h_2$ such that*

$$h_1^2 h_2 \equiv -1 \mod 20 \quad \textit{respectively} \quad h_1^2 h_2 \equiv -1 \mod 28.$$

Proof. We have

$$3^2 \cdot 11 \equiv 13^2 \cdot 11 \equiv -1 \mod 20,$$

which proves the lemma for $H \in \mathscr{H}_5$. For $H \in \mathscr{H}_7$, we notice that

$$5^2 \cdot 19 \equiv 11^2 \cdot 3 \equiv -1 \mod 28.$$

For $H \subseteq G(4t)$, we define the following properties:

$(P_1(H))$: $p \mid (4tq+1) \Rightarrow p \in H$;

$(P_2(H))$: For every $h \in H$, there is a prime divisor p of $4tq+1$, such that $p \equiv h \mod 4t$;

(P_3): $d \mid (4tq+1) \Rightarrow d \not\equiv -1 \mod 4t$.

Then let

$$W_1(H; x; k, l; t) = \operatorname{card}\{q \leqslant x:\ q \equiv l \mod k,\ (P_1(H))\},$$

$$W_2(H; x; k, l; t) = \operatorname{card}\{q \leqslant x:\ q \equiv l \mod k,\ (P_1(H)),\ (P_2(H)),\ (P_3)\}.$$

$\mathscr{H}_5$ and $\mathscr{H}_7$ have been defined in Lemma 7. For $t \neq 5$, $t \neq 7$, let $\mathscr{H}_t = \emptyset$.

PROPOSITION 1. *Let U_1, U_2 be the two subgroups of $G(4t)$ in Lemma 5* (iv). *Then*

$$V(x; k, l; t) = \sum_{i=1}^{2} W_1(U_i; x; k, l; t) + O\Big(\sum_{\substack{H \subseteq G(4t) \\ |H| < |G(4t)|/2}} W_1(H; x; k, l; t) \Big) + O\Big(\sum_{H \in \mathscr{H}_t} W_2(H; x; k, l; t) \Big).$$

Proof. By the definition of $V(x; k, l; t)$, (2), (3) and Lemma 1,

$$\begin{aligned} V(x; k, l; t) &= \operatorname{card}\{q \leqslant x:\ q \equiv l \mod k, (3) \text{ unsolvable}\} \\ &= \operatorname{card}\{q \leqslant x:\ q \equiv l \mod k, (P_3)\} = \sum_{H \subseteq G(4t)} W_2(H; x; k, l; t). \end{aligned} \tag{24}$$

First assume that $H \subseteq G(4t)$ with $|H| \geqslant \frac{1}{2}|G(4t)| + 1$. Applying Lemma 2 for $g = -1$, there exist residue classes $h_1, h_2 \in H$ such that

$$h_1 h_2 \equiv -1 \mod 4t. \tag{25}$$

Obviously,

$$h_1 \neq h_2, \tag{26}$$

otherwise $h_1^2 \equiv -1 \bmod 4$, which is impossible. If q is counted in $W_2(H; x; k, l; t)$, then by definition $4qt+1$ has property $(P_2(H))$, i.e. $4tq+1$ has prime factors p_1 and p_2 satisfying

$$p_1 \equiv h_1 \bmod 4t, \quad p_2 \equiv h_2 \bmod 4t. \tag{27}$$

By (26), $p_1 \neq p_2$, thus $p_1 p_2 | (4tq+1)$, and by (25) and (27), $p_1 p_2 \equiv -1 \bmod 4t$, contradicting (P_3). Therefore, $|H| \geqslant \frac{1}{2}|G(4t)|+1$ implies

$$W_2(H; x; k, l; t) = 0.$$

By (24), we get

$$\begin{aligned} V(x; k, l; t) &= \sum_{\substack{H \subseteq G(4t) \\ |H| \leqslant |G(4t)|/2}} W_2(H; x; k, l; t) \\ &= \sum_{\substack{H \subseteq G(4t) \\ |H| = |G(4t)|/2}} W_2(H; x; k, l; t) + O\Big(\sum_{\substack{H \subseteq G(4t) \\ |H| < |G(4t)|/2}} W_1(H; x; k, l; t)\Big). \end{aligned} \tag{28}$$

Now let $H \subseteq G(4t)$ with $|H| = \frac{1}{2}|G(4t)|$, and H not a subgroup of $G(4t)$. Then Lemma 7 may be applied. If (i), (ii) or (iii) holds, then by the above argument, we can find a divisor $d | (4tq+1)$, and $d \equiv -1 \bmod 4t$, again contradicting (P_3). Therefore, $W_2(H; x; k, l; t) = 0$ in these cases. We are left with the cases (iv) and (v) in Lemma 7, and these are taken care of by $\mathscr{H}_5$ and $\mathscr{H}_7$. Thus (28) and Lemma 5 (iv) give

$$\begin{aligned} V(x; k, l; t) = \sum_{i=1}^{2} W_2(U_i; x; k, l; t) &+ O\Big(\sum_{\substack{H \subseteq G(4t) \\ |H| < |G(4t)|/2}} W_1(H; x; k, l; t)\Big) \\ &+ O\Big(\sum_{H \in \mathscr{H}_t} W_2(H; x; k, l; t)\Big). \end{aligned} \tag{29}$$

An easy inclusion-exclusion argument shows for $i = 1, 2$ that

$$\begin{aligned} W_2(U_i; x; k, l; t) &= \operatorname{card}\{q \leqslant x: \ q \equiv l \bmod k, (P_1(U_i)), (P_2(U_i))\} \\ &= W_1(U_i; x; k, l; t) + O\Big(\sum_{\substack{H \subseteq U_i \\ |H| < |U_i|}} W_1(H; x; k, l; t)\Big). \end{aligned}$$

This and (29) prove the proposition.

3. The main term. Iwaniec's half dimensional sieve. In this section we deal with the terms $W_1(U; x; k, l; t)$ occurring in Proposition 1, where U is a subgroup of $G(4t)$ with $|U| = \frac{1}{2}|G(4t)|$.

For a finite set $\mathscr{A}$ of positive integers, a set $\mathscr{P}$ of primes, and $z > 1$, let

$$P(z) = \prod_{\substack{p < z \\ p \in \mathscr{P}}} p, \quad S(\mathscr{A}, z) = \operatorname{card}\{a \in \mathscr{A}: \ (a, P(z)) = 1\}. \tag{30}$$

Furthermore, let $\omega(d)$ be a multiplicative arithmetic function satisfying

$$0 \leqslant \omega(p) < p, \quad \omega(p) = 0 \quad \text{for } p \notin \mathscr{P}; \tag{31}$$

$$-c_1 + \frac{1}{2}\log\frac{z}{w} \leqslant \sum_{w \leqslant p < z} \frac{\omega(p)}{p}\log p \leqslant \sum_{w \leqslant p < z} \frac{\omega(p)}{p-\omega(p)}\log p \leqslant c_2 + \frac{1}{2}\log\frac{z}{w} \tag{32}$$

for any $z > w > 1$, and some constants $c_1 > 1$, $c_2 > 1$. Define

$$\Omega(z) = \prod_{p < z}\left(1 - \frac{\omega(p)}{p}\right), \tag{33}$$

$$\mathscr{A}_d = \{a \in \mathscr{A}: \ a \equiv 0 \bmod d\}, \tag{34}$$

$$R(\mathscr{A}, d) = |\mathscr{A}_d| - \frac{\omega(d)}{d}X \tag{35}$$

for some $X = X_{\mathscr{A}} > 1$.

PROPOSITION 2. *Let U be a subgroup of $G(4t)$ with $|U| = \frac{1}{2}|G(4t)|$. Let the greatest odd divisor a' of each $a \in \mathscr{A}$ satisfy $a' \in U$. Let*

$$\mathscr{P} \subseteq \{p \in \boldsymbol{P}: \ p \in G(4t) \backslash U\},$$

and let (31) and (32) be satisfied. Then for $Q^6 < z^2 \leqslant A := \max_{a \in \mathscr{A}} a$

$$S(\mathscr{A}, z) = \Omega(z)X\left(1 + \frac{F(s)}{s} + O\left(e^{4c_2 - s}\left(\frac{c_1 + \log Q}{\log A}\right)^{\gamma}\right)\right) + \sum_{\substack{d < A/Q \\ d | P(z)}} |R(\mathscr{A}, d)|,$$

where $s = \log A/\log z$, $|\theta| \leqslant 1$, γ as in the theorem, and the function $F(s)$ as defined in § 4 of [5].

This is a straightforward generalization of Theorem 2 of [5], which can be proved in the same way. The only notable difference is the following: In [5], we have

$$a \in \mathscr{A} \Rightarrow a' \equiv 1 \bmod 4, \qquad \mathscr{P} \subseteq \{p \equiv -1 \bmod 4\},$$

which guarantees that, if $p_1 \in \mathscr{P}$ divides a, then there is a $p_2 \in \mathscr{P}$ such that $p_1 p_2 | a$. In Proposition 2, the assumptions on $\mathscr{A}$ and $\mathscr{P}$ yield the same property, since U is a group. In addition we need $h_1 h_2 \in U$ for $h_1, h_2 \in G(4t) \backslash U$. This has already been proved in Lemma 5 (v).

PROPOSITION 3. *Let U be a subgroup of $G(4t)$ with $|U| = \frac{1}{2}|G(4t)|$. For all $a \in \mathscr{A}$, let $a \in U$. Let*

$$\mathscr{P} = \{p \in \boldsymbol{P}: \ p \in G(4t) \backslash U\},$$

and let (31) *and* (32) *be satisfied. Then for* $Q^6 < A = \max_{a\in\mathscr{A}} a$, *we have*

$$S(\mathscr{A}, \sqrt{A}) = \left(\frac{8t}{\pi(t-1)} L(1,\chi_U)\right)^{1/2} \prod_{p\in\mathscr{P}} \left(1-\frac{\omega(p)}{p}\right)\left(1-\frac{1}{p^2}\right)^{-1/2}\left(1+\frac{1}{p}\right)$$
$$\times X(\log A)^{-1/2}\left(1+O\left(e^{6c_2}\left(\frac{c_1+\log Q}{\log A}\right)^{\gamma}\right)\right)+\sum_{\substack{d<A/Q\\ d\mid P(\sqrt{A})}} |R(\mathscr{A}, d)|,$$

with parameters as in Proposition 2, *and* χ_U *as defined in Lemma* 5 (v).

Proof. Applying Proposition 2 for $z = \sqrt{A}$, and reasoning as in the proof of Theorem 3 in [5] with

$$L(1,\chi_U) = \prod_{p\in\mathbf{P}}\left(1-\frac{\chi_U(p)}{p}\right)^{-1}$$

instead of $L(1,\chi_4)$, the desired result follows by Lemma 5 (v).

Remark. It should be mentioned that there is a misprint in the formulation of Theorem 3 in [5], namely the condition has to read: $\mathscr{P} = \{p \equiv -1 \pmod 4\}$.

Now we apply the half dimensional sieve to our problem. We define for arbitrary positive integers k, l with $(k,l) = 1$, primes t and q, real $x, z > 1$, and a subgroup U of $G(4t)$ with $|U| = \frac{1}{2}|G(4t)|$,

$$\mathscr{A} = \mathscr{A}_{t,k}(x) = \{4tq+1:\ q \leqslant x,\ q \equiv l \bmod k\}, \tag{36}$$

$$\mathscr{P} = \mathscr{P}_U = \{p\in\mathbf{P}:\ p\in G(4t)\backslash U\}. \tag{37}$$

Observe that in particular

$$2\notin\mathscr{P}, \quad t\notin\mathscr{P}. \tag{38}$$

Lemma 9. *For squarefree* d *satisfying* $p\in\mathscr{P}$ *for all* $p\mid d$, *there is an integer* l' *with* $(l', [d,k]) = 1$ *and*

$$|\mathscr{A}_d| = \begin{cases}\pi(x;[d,k],l') & \text{for } (d,k)\mid(4tl+1),\\ 0 & \text{otherwise.}\end{cases}$$

Proof. We consider the congruence system

$$m \equiv l \bmod k, \quad 4tm+1 \equiv 0 \bmod d \tag{39}$$

for the integer variable m. The second congruence of (39) is always solvable, since $(t,d) = 1$ by (38). Hence there is a unique solution $l' \bmod [d,k]$ of (39) satisfying $(l', [d,k]) = 1$ if and only if $(d,k)\mid(4tl+1)$ (see [2, p. 21]). This proves the lemma.

Let

$$X = \operatorname{Li} x/\varphi(k), \tag{40}$$

$$\omega(p) = \begin{cases}p/\varphi(p) & \text{for } p\in\mathscr{P},\ p\nmid k,\\ 0 & \text{otherwise,}\end{cases} \tag{41}$$

where φ denotes Euler's function, and ω is multiplicative. By the definition of $R(\mathscr{A}, d)$ and Lemma 9, we have

Lemma 10. *Let* d *be squarefree. Let*

$$p\notin G(4t)\backslash U \quad \text{or} \quad p\nmid(4tl+1) \tag{42}$$

for all $p\mid k$. *Then*

$$R(\mathscr{A}, d) = \begin{cases}\pi(x;dk,l')-\operatorname{Li} x/\varphi(dk) & \text{for } (d,k) = 1,\ p\in\mathscr{P}\ \ (p\mid d),\\ 0 & \text{otherwise.}\end{cases}$$

Proposition 4. *Let* $0 < \varepsilon < 1/6$, *and let* (42) *be satisfied. Then*

$$W_1(U;x;k,l;t) = \frac{1}{\varphi(k)}\left(\frac{8t}{\pi(t-1)}L(1,\chi_U)\right)^{1/2}\prod_{p\in\mathscr{P}}\left(1-\frac{1}{p^2}\right)^{-1/2}\left(1-\frac{2}{p(p-1)}\right)$$
$$\times \operatorname{Li} x(\log x)^{-1/2}(1+O(\varepsilon^{\gamma}))+\theta E(x, x^{1-\varepsilon}),$$

where $|\theta| \leqslant 1$, *and the other parameters as defined in the theorem.*

Proof. By (41), (31) is obviously satisfied. In order to be able to apply Proposition 3, it remains to check (32). By definition of $\omega(p)$, we have

$$\sum_{p\leqslant x}\frac{\omega(p)}{p}\log p = \sum_{\substack{p\leqslant x,\ p\in\mathscr{P}\\ p\nmid k}}\frac{\log p}{p-1} = \sum_{\substack{p\leqslant x\\ p\in\mathscr{P}}}\frac{\log p}{p-1}+c_3(k).$$

Similarly,

$$\sum_{p\leqslant x}\frac{\omega(p)}{p-\omega(p)}\log p = \sum_{\substack{p\leqslant x\\ p\in\mathscr{P}}}\frac{\log p}{p-2}+c_4(k).$$

Partial summation and Dirichlet's prime number theorem give for $j\in\{1,2\}$, $x \geqslant 3$,

$$\sum_{\substack{p\leqslant x\\ p\in\mathscr{P}}}\frac{\log p}{p-j} = \sum_{h\in G(4t)\backslash U}\ \sum_{\substack{p\leqslant x\\ p\equiv h \bmod 4t}}\frac{\log p}{p}+O(1)$$
$$= \sum_{h\in G(4t)\backslash U}\frac{1}{\varphi(4t)}\log x+O(1) = \tfrac{1}{2}\log x+O(1).$$

This yields (32) with constants c_1 and c_2 only depending on t and k.

By what was said between Propositions 2 and 3, we have

$$W_1(U; x; k, l; t) = S(\mathscr{A}, \sqrt{A}). \tag{43}$$

By Bertrand's postulate in arithmetic progressions (see for instance [10]),

$$\pi(2y; k, l) - \pi(y; k, l) > 0$$

for $(k, l) = 1$ with k sufficiently large and $y \geqslant c_5(k)$ for a suitable constant c_5. This implies that there is a positive constant c_6 such that there exists a prime $q \equiv l \bmod k$ satisfying $c_6 x < q < x$ for large x. Hence

$$A = \max_{a \in \mathscr{A}} a = c_7 x,$$

where $c_7 > 0$. Without loss of generality, we may assume $c_7 \leqslant 1$. We choose $Q = (c_7 x)^{\varepsilon}$, hence

$$A/Q \leqslant x^{1-\varepsilon}.$$

This yields

$$(\log A)^{-1/2}\left(1 + O\left(e^{6c_2}\left(\frac{c_1 + \log Q}{\log A}\right)^{\gamma}\right)\right) = (\log x)^{-1/2}(1 + O(\varepsilon^{\gamma})).$$

Applying Lemma 10 to the error term, and summing $\sum |R(\mathscr{A}, d)|$ over all modules, (43) and Proposition 3 give the desired result.

4. The error terms $W_2(H; x; k, l; t)$. Rosser's sieve. We will estimate the error terms occurring in Proposition 1 by Rosser's sieve [6]. We use the notation of the preceeding section, in particular (30), (34) and (35). The conditions (31) and (32) are replaced by

$$0 \leqslant \omega(p) < p, \quad \omega(p) = 0 \quad \text{for } p \notin \mathscr{P}; \tag{44}$$

$$\prod_{w \leqslant p < z}\left(1 - \frac{\omega(p)}{p}\right)^{-1} < \left(\frac{\log z}{\log w}\right)^{\varkappa}\left(1 + \frac{c_8}{\log w}\right) \tag{45}$$

for all $z > w \geqslant 2$, and some constant $c_8 \geqslant 2$. The smallest $\varkappa \geqslant 0$ satisfying (45) is called the dimension of the sieve. The sets $\mathscr{A}$ and $\mathscr{P}$ are chosen in the following way: For $H \subseteq G(4t)$, let

$$\mathscr{A} = \mathscr{A}_t(x) = \{4tq + 1 : q \leqslant x\}, \quad \mathscr{P} = \mathscr{P}_H = \{p \in \mathbf{P} : p \in G(4t) \backslash H\}.$$

In particular,

$$2 \notin \mathscr{P}, \quad t \notin \mathscr{P}. \tag{46}$$

We obviously have an integer l', $(l', d) = 1$, such that

$$\mathscr{A}_d = \pi(x; d, l') \tag{47}$$

for squarefree d satisfying $p \in \mathscr{P}$ for all $p|d$. Setting

$$X = \operatorname{Li} x,$$

$$\omega(p) = \begin{cases} p/\varphi(p) & \text{for } p \in \mathscr{P}, \\ 0 & \text{otherwise,} \end{cases}$$

we get from (47)

$$R(\mathscr{A}, d) = \begin{cases} \pi(x; d, l') - \operatorname{Li} x/\varphi(d) & \text{for } p \in \mathscr{P} \quad (p|d), \\ 0 & \text{otherwise.} \end{cases} \tag{48}$$

By the definition of $\omega(p)$, (44) is obviously satisfied. Now we consider (45). We have

$$\sum_{w \leqslant p < z} \sum_{m=2}^{\infty} \frac{1}{mp^m} < \sum_{w \leqslant n < z} \frac{1}{n^2} \sum_{m=0}^{\infty} \frac{1}{n^m} < \sum_{n \geqslant w} \frac{1}{n(n-1)} \ll \frac{1}{w}.$$

Hence for $z > w \geqslant 2$

$$-\sum_{\substack{w \leqslant p < z \\ p \equiv h \bmod 4t}} \log\left(1 - \frac{1}{p-1}\right) = \sum_{\substack{w \leqslant p < z \\ p \equiv h \bmod 4t}} \sum_{m=1}^{\infty} \frac{1}{m(p-1)^m} = \sum_{\substack{w \leqslant p < z \\ p \equiv h \bmod 4t}} \frac{1}{p-1} + O\left(\frac{1}{w}\right).$$

By the quantitative version of Dirichlet's prime number theorem (see for instance [7, p. 450]), i.e.

$$\sum_{\substack{p < z \\ p \equiv h \bmod 4t}} \frac{1}{p} = \frac{1}{\varphi(4t)} \log\log z + c_9 + O\left(\frac{1}{\log z}\right),$$

and partial summation, we get

$$-\sum_{\substack{w \leqslant p < z \\ p \equiv h \bmod 4t}} \log\left(1 - \frac{1}{p-1}\right) = \frac{1}{\varphi(4t)}(\log\log z - \log\log w) + O\left(\frac{1}{\log w}\right).$$

Thus

$$\prod_{\substack{w \leqslant p < z \\ p \equiv h \bmod 4t}}\left(1 - \frac{1}{p-1}\right)^{-1} = \left(\frac{\log z}{\log w}\right)^{1/\varphi(4t)}\left(1 + O\left(\frac{1}{\log w}\right)\right).$$

This implies

$$\prod_{w \leqslant p < z}\left(1 - \frac{\omega(p)}{p}\right)^{-1} = \prod_{\substack{w \leqslant p < z \\ p \in \mathscr{P}}}\left(1 - \frac{1}{p-1}\right)^{-1} \tag{49}$$

$$= \prod_{h \in G(4t) \backslash H} \prod_{\substack{w \leqslant p < z \\ p \equiv h \bmod 4t}}\left(1 - \frac{1}{p-1}\right)^{-1}$$

$$= \prod_{h \in G(4t)\setminus H} \left(\left(\frac{\log z}{\log w} \right)^{1/\varphi(4t)} \left(1 + O\left(\frac{1}{\log w} \right) \right) \right)$$

$$= \left(\frac{\log z}{\log w} \right)^{|G(4t)\setminus H|/|G(4t)|} \left(1 + O\left(\frac{1}{\log w} \right) \right).$$

Thus (45) holds for some constant c_8. The dimension

$$\varkappa = \frac{|G(4t)\setminus H|}{|G(4t)|} \tag{50}$$

of the sieve satisfies

$$1/2 < \varkappa \leqslant 1$$

for $|H| < \frac{1}{2}|G(4t)|$, which will be important to give terms of lower order than the main term.

PROPOSITION 5. *Let* $H \subseteq G(4t)$, *let* $0 < \varepsilon < 1$. *Then*

$$W_2(H; x; k, l; t) \ll \varepsilon^{-\varkappa} x (\log x)^{-1-\varkappa} + E(x, x^{\varepsilon}),$$

with $\varkappa$ *as defined in* (50).

Proof. Since (44) and (45) hold as shown above, we may apply Theorem 1 of [6]. We set

$$y = x^{\varepsilon}, \quad z = x^{\varepsilon/2},$$

hence $s = 2$. Then by (48) and (49),

$$S(\mathscr{A}, z) < \operatorname{Li} x \prod_{\substack{p < z \\ p \in \mathscr{P}}} \left(1 - \frac{1}{p-1} \right) \left(F(2) + e^{\sqrt{c_8}} Q(2) (\log y)^{-1/3} \right) + \sum_{d < y} |R(\mathscr{A}, d)| \tag{51}$$

$$\ll \varepsilon^{-\varkappa} x (\log x)^{-1-\varkappa} + E(x, x^{\varepsilon}).$$

By Bertrand's postulate, we have $A = \max_{a \in \mathscr{A}} a \geqslant 2tx$, thus

$$W_2(H; x; k, l; t) \leqslant S(\mathscr{A}, A) \leqslant S(\mathscr{A}, A^{\varepsilon/2}) \leqslant S(\mathscr{A}, z),$$

which by (51) proves the proposition.

COROLLARY 1. *Let* $H \subseteq G(4t)$, $|H| < \frac{1}{2}|G(4t)|$. *Then*

$$W_2(H; x; k, l; t) \ll x (\log x)^{-3/2 - 1/(2t-2)}.$$

Proof. By Bombieri's theorem (see [8]), we have

$$E(x, x^{\varepsilon}) \ll x/(\log x)^2$$

for some small $\varepsilon > 0$. Since

$$|G(4t)| = \varphi(4t) = 2(t-1), \quad |H| \leqslant \tfrac{1}{2}|G(4t)| - 1 = t - 2,$$

we get

$$1 \geqslant \frac{|G(4t)\setminus H|}{|G(4t)|} \geqslant \frac{t}{2(t-1)} = \frac{1}{2} + \frac{1}{2t-2}.$$

Now Proposition 5 implies the corollary.

5. The error terms connected with $\mathscr{H}_t$. Rosser's sieve again. For a fixed prime p_1, $(p_1, 2t) = 1$, and $H \subseteq G(4t)$, let

$$\mathscr{A} = \mathscr{A}_{t,p_1}(x) = \{(4tq+1)/p_1 \colon q \leqslant x,\ p_1 | (4tq+1)\},$$

$$\mathscr{P} = \mathscr{P}_H = \{p \in \boldsymbol{P} \colon p \in G(4t)\setminus H\}.$$

Since $2 \notin \mathscr{P}$, $t \notin \mathscr{P}$, and by the condition on p_1, we get for squarefree d satisfying $p \in \mathscr{P}$ for all $p | d$

$$|\mathscr{A}_d| = \operatorname{card}\{q \leqslant x \colon 4tq+1 \equiv 0 \bmod p_1,\ (4tq+1)/p_1 \equiv 0 \bmod d\} \tag{52}$$

$$= \operatorname{card}\{q \leqslant x \colon 4tq+1 \equiv 0 \bmod p_1 d\} = \pi(x; p_1 d, l')$$

for some l', $(l',\ p_1 d) = 1$.

Setting

$$X = \operatorname{Li} x/\varphi(p_1),$$

$$\omega(p) = \begin{cases} p/\varphi(p) & \text{for } p \in \mathscr{P},\ p \neq p_1, \\ 1 & \text{for } p \in \mathscr{P},\ p = p_1, \\ 0 & \text{otherwise,} \end{cases}$$

we have by (52)

$$R(\mathscr{A}, d) = \begin{cases} \pi(x; p_1 d, l') - \operatorname{Li} x/\varphi(p_1 d) & \text{for } p \in \mathscr{P} \quad (p|d), \\ 0 & \text{otherwise.} \end{cases} \tag{53}$$

PROPOSITION 6. *Let* $H \subseteq G(4t)$, $h \in H$, $H^* = H\setminus\{h\}$; $p_1 \equiv h \bmod 4t$. *Let* $0 < \varepsilon < 1$. *Then*

$$W_{p_1,t} = \operatorname{card}\left\{ q \leqslant x \colon p_1 | (4tq+1),\ p \left| \frac{4tq+1}{p_1} \Rightarrow p \in H^* \right. \right\}$$

satisfies

$$W_{p_1,t} \ll \frac{1}{\varphi(p_1)} \varepsilon^{-\varkappa^*} x (\log x)^{-1-\varkappa^*} + E(x, x^{\varepsilon}),$$

where

$$\varkappa^* = \frac{|G(4t)\setminus H^*|}{|G(4t)|}.$$

Proof. Since $\mathscr{P} = \mathscr{P}_H$ is the same as in the preceeding section, (44), (45) and (49) hold. Thus we may again apply Theorem 1 of [6]. Let

$$y = x^{\varepsilon}, \quad z = x^{\varepsilon/2}.$$

By (49) and (53), we have for $\mathscr{P} = \mathscr{P}_{H^*}$

$$S(\mathscr{A}, z) < 2\frac{\operatorname{Li} x}{\varphi(p_1)} \prod_{\substack{p<z \\ p\in\mathscr{P}}} \left(1-\frac{1}{p-1}\right)(F(2)+e^{\sqrt{c_8}}Q(2)(\log y)^{-1/3}) + \sum_{d<y} |R(\mathscr{A}, d)| \tag{54}$$

$$\ll \frac{1}{\varphi(p_1)} \varepsilon^{-\varkappa^*} x(\log x)^{-1-\varkappa^*} + E(x, x^{\varepsilon}).$$

If $A = \max_{a\in\mathscr{A}} a \leqslant \sqrt{x}$, then

$$W_{p_1,t} \leqslant |\mathscr{A}| \leqslant \sqrt{x},$$

and the proposition is proved. If $A \geqslant \sqrt{x}$, then

$$W_{p_1,t} \leqslant S(\mathscr{A}, A) \leqslant S(\mathscr{A}, \sqrt{x}) \leqslant S(\mathscr{A}, z),$$

which again proves the proposition by (54).

COROLLARY 2. *Let* $H \subseteq G(4t)$, $|H| \leqslant \frac{1}{2}|G(4t)|$, $h \in H$, $H^* = H\setminus\{h\}$; $p_1 \equiv h \bmod 4t$. *Then for* $W_{p_1,t}$ *as defined in Proposition* 6

$$W_{p_1,t} \ll \frac{1}{p_1} x(\log x)^{-3/2-1/(2t-2)}.$$

Proof. As in the proof of Corollary 1, Bombieri's theorem yields the result, using Proposition 6.

6. Proof of the theorem. Using Proposition 4 for $U = U_1$ and $U = U_2$, we get the main term and a suitable error term in the theorem by Proposition 1. Condition (42) in Proposition 4, namely

$$p \not\equiv (4tl+1) \quad \text{or} \quad p \in G(4t)\setminus U,$$

has to be satisfied for $U = U_1$ and $U = U_2$. This is equivalent to

$$p \not\equiv (4tl+1) \quad \text{or} \quad p \in U_1 \cap U_2. \tag{55}$$

By Lemma 5 (ii) and (iii), $a \in U_1 \cap U_2$ if and only if a is a square in $G(4t)$. Thus (55) is the same as (4) by Lemma 4 (ii) for $t > 2$. The case $t = 2$ is clear.

In order to prove the theorem, it remains to bound the two error terms in Proposition 1. Corollary 1 takes care of the first one, namely

$$\sum_{\substack{H\subseteq G(4t) \\ |H|<|G(4t)|/2}} W_2(H; x; k, l; t) \ll x(\log x)^{-3/2-1/(2t-2)}. \tag{56}$$

Now let $H \in \mathscr{H}_5$. By Lemma 8, there are $h_1, h_2 \in H$, $h_1 \neq h_2$, such that

$$h_1^2 h_2 \equiv -1 \bmod 20. \tag{57}$$

Let q be counted in $W_2(H; x; k, l; 5)$, and assume that there is a prime p_1 satisfying

$$p_1 \equiv h_1 \bmod 20, \quad p_1^2 | (20q+1).$$

By the definition of $W_2(H; x; k, l; 5)$, there is a prime $p_2 \equiv h_2 \bmod 20$ such that $p_2|(20q+1)$. Thus

$$p_1^2 p_2 | (20q+1).$$

Now (57) implies

$$p_1^2 p_2 \equiv -1 \bmod 20,$$

contradicting (P_3). Hence $p_1^2 \not| (20q+1)$. Therefore, we have

$$W_2(H; x; k, l; 5) \leqslant \sum_{p_1 \leqslant 20x+1} W_{p_1,5} \tag{58}$$

(as defined in Proposition 6). Similarly, we get

$$W_2(H; x; k, l; 7) \leqslant \sum_{p_1 \leqslant 28x+1} W_{p_1,7} \tag{59}$$

for $H \in \mathscr{H}_7$. By the definition of $\mathscr{H}_t$ and Corollary 2, (58) respectively (59) yields

$$\sum_{H\in\mathscr{H}_t} W_2(H; x; k, l; t) \ll x(\log x)^{-3/2-1/(2t-2)} \sum_{p_1 \leqslant 4tx+1} \frac{1}{p_1}$$

$$\ll x(\log x)^{-3/2-1/(2t-2)} \log\log x$$

$$\ll x(\log x)^{-3/2-1/(2t-2)+\varepsilon'}$$

for any $\varepsilon' > 0$. This completes the proof of the theorem.

Remark. Finally, we remark that, using a slightly more general version of Corollary 2 and a shorter argument, one could avoid the comparatively tedious Lemma 7. Then, however, we would miss the result that, except for $t = 5$ and $t = 7$, H in Lemma 7 satisfies one of the conditions (i), (ii) or (iii), which implies that the corresponding $W_2(H; x; k, l; t)$ is zero. In fact, except for $t = 5$, 7, Section 5 is superfluous.

References

[1] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York 1981.
[2] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London 1974.
[3] H. Hasse, *Vorlesungen über Zahlentheorie*, 2nd ed., Springer, Berlin 1964.
[4] L. K. Hua, *Introduction to Number Theory*, Springer, Berlin 1982.
[5] H. Iwaniec, *The half dimensional sieve*, Acta Arith. 29 (1976), 69–95.
[6] –, *Rosser's sieve*, ibid. 36 (1980), 171–202.
[7] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, B. G. Teubner, Leipzig 1909.
[8] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Springer, Berlin 1971.
[9] J. W. Sander, *On* $4/n = 1/x+1/y+1/z$ *and Iwaniec's half dimensional sieve*, to appear.
[10] T. Tatuzawa, *On Bertrand's problem in an arithmetic progression*, Proc. Japan Acad. 28 (1962), 293–294.
[11] R. C. Vaughan, *On a problem of Erdös, Straus and Schinzel*, Mathematika 17 (1970), 193–198.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER
Welfengarten 1
3000 Hannover 1
Fed. Rep. of Germany

Received on 7.8.1990 (2067)

ACTA ARITHMETICA
LIX.3 (1991)

On the Möbius sum function

by

ROBERT J. ANDERSON (DeKalb, Ill.)

1. Introduction. Let $M(x) = \sum_{n \leqslant x} \mu(n)$, $\mu(n)$ being the Möbius function. The inequality $M(x) = O(x^{1/2+\varepsilon})$ for every $\varepsilon > 0$ is equivalent to the Riemann hypothesis. A major question in the theory of $M(x)$ is whether or not the stronger bound

$$M(x) = O(x^{1/2}) \tag{1}$$

holds. Although (1) is probably false, the best known estimate of large values of $|M(x)|x^{-1/2}$ is

$$\overline{\lim_{x \to \infty}} |M(x)|x^{-1/2} > 1.06$$

due to Odlyzko and te Riele [5].

For any x let

$$M^*(x) = 1 + \sum_{n=1}^{\infty} \frac{(-1)^n (2\pi x)^{2n}}{2n(2n)!\zeta(2n+1)}.$$

If $x_0 > 0$ then

$$|M(x_0) + 2M^*(x_0^{-1})|x_0^{-1/2} \leqslant \overline{\lim_{x \to \infty}} |M(x)|x^{-1/2}.$$

This is a result of Jurkat [4, p. 148], also see Anderson and Stark [1, pp. 99–100]. In particular, (1) implies

$$M^*(x) = O(x^{-1/2}). \tag{2}$$

Let $r(t) = t \sum_{n \leqslant t} \mu(n) n^{-1}$. The function $M^*(x)$ is the cosine transform of $r(t^{-1})$; thus,

$$M^*(x) = \int_0^1 r(t^{-1}) \cos 2\pi x t \, dt$$

[4, p. 152]. By definition

$$\tilde{M}^*(x) = \int_0^1 r(t^{-1}) \sin 2\pi x t \, dt.$$