ACTA ARITHMETICA
LXXIV.4 (1996)

On the number of prime factors of integers of the form $ab + 1$

by

K. Győry (Debrecen), A. Sárközy (Budapest) and
C. L. Stewart (Waterloo, Ont.)

1. Introduction. For any set X let $|X|$ denote its cardinality and for any integer n, larger than one, let $\omega(n)$ denote the number of distinct prime factors of n and let $P(n)$ denote the greatest prime factor of n. Denote the set of positive integers by $\mathbb{N}$. In 1934 Erdős and Turán [5] proved that there exists a positive number c_1 such that for any non-empty finite subset A of $\mathbb{N}$,

$$\omega\Big(\prod_{a,a'\in A}(a+a')\Big) > c_1 \log |A|. \tag{1.1}$$

In 1986, Győry, Stewart and Tijdeman [12] proved that this result can be extended to the case when the summands are taken from different sets. They proved that there is a positive number c_2 such that for any finite subsets A and B of $\mathbb{N}$ with $|A| \ge |B| \ge 2$ we have

$$\omega\Big(\prod_{a\in A,\, b\in B}(a+b)\Big) > c_2 \log |A|. \tag{1.2}$$

Moreover, in 1988, Erdős, Stewart and Tijdeman [4] showed that (1.2) is not far from best possible. They proved that there is a positive number c_3 such that for each integer k, with $k \ge 3$, there exist sets of positive integers A and B with $k = |A| \ge |B| \ge 2$ satisfying

$$\omega\Big(\prod_{a\in A,\, b\in B}(a+b)\Big) < c_3(\log |A|)^2 \log\log |A|. \tag{1.3}$$

The research of the first two authors was partially supported by the Hungarian National Foundation for Scientific Research, Grants No. 1641 and 1901 respectively.

The research of the third author was supported in part by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

If A and B are dense subsets of $\mathbb{N}$ then estimates (1.1) and (1.2) may be strengthened. Let ε and δ be positive real numbers and let N be a positive integer. Let A and B be subsets of $\{1,\ldots,N\}$ of cardinality at least δN. In [3], Erdős, Pomerance, Sárközy and Stewart proved that there exists a positive number N_0, which is effectively computable in terms of ε and δ, such that if N exceeds N_0 then there exists an integer a from A and an integer b from B for which

$$\omega(a+b) > (1-\varepsilon)(\log N)/\log\log N. \tag{1.4}$$

Sárközy and Stewart [17] were able to show that a lower bound of the same order of magnitude holds even under a much weaker density condition. Let θ be a real number with $1/2 < \theta \le 1$ and let N be a positive integer. They proved that there exists a positive number c_4, which is effectively computable in terms of θ, such that if A and B are subsets of $\{1,\ldots,N\}, N$ exceeds c_4 and

$$(|A|\cdot|B|)^{1/2} \ge N^{\theta},$$

then there exists an integer a from A and an integer b from B for which

$$\omega(a+b) > \frac{1}{6}\left(\theta-\frac{1}{2}\right)^2(\log N)/\log\log N. \tag{1.5}$$

In the same article [17], they estimated the average value of $\omega(a+b)$. They showed that if A and B are subsets of $\{1,\ldots,N\}$ with $(|A|\cdot|B|)^{1/2} = N\exp(-(\log N)^{o(1)})$ then

$$\frac{1}{|A|\cdot|B|}\sum_{a\in A}\sum_{b\in B}\omega(a+b) > (1+o(1))\log\log N. \tag{1.6}$$

For further results of this type we refer to [15], [22] and [23].

In 1992, Sárközy [16] commenced the study of the multiplicative analogues of the above results, where in place of terms $a+b$ one considers terms $ab+1$. In particular, he proved the multiplicative analogue of (1.4). Let ε and δ be positive real numbers and let N be a positive integer. Let A be a subset of $\{1,\ldots,N\}$ of cardinality at least δN. He proved that there exists a positive number N_1, which is effectively computable in terms of ε and δ, such that if N exceeds N_1 then there exist integers a and a' from A such that

$$\omega(aa'+1) > (1-\varepsilon)(\log N)/\log\log N. \tag{1.7}$$

We remark that this is slightly weaker than (1.4) since only the special case $A=B$ is covered and since while one cannot replace the factor $1-\varepsilon$ in (1.4) by $1+\varepsilon$ one expects (1.7) to hold with $2-\varepsilon$ in place of $1-\varepsilon$.

Our goal in this paper is to study the multiplicative analogues of (1.1)–(1.3), (1.5) and (1.6).

2. Lower bounds. We will prove the following multiplicative analogue of (1.2).

THEOREM 1. *Let A and B be finite subsets of $\mathbb{N}$ with $|A| \geq |B| \geq 2$. Then*

$$\omega\Big(\prod_{a\in A,\, b\in B}(ab+1)\Big) > c_5 \log |A|,$$

where c_5 is an effectively computable positive constant.

Both (1.2) and Theorem 1 are special cases of Theorem 2 below.

THEOREM 2. *Let $n \geq 2$ be an integer, and let A and B be finite subsets of $\mathbb{N}^n$ with $|A| \geq |B| \geq 2(n-1)$ and with the following properties: the n-th coordinate of each vector in A is equal to 1 and any n vectors in $B \cup (0,\ldots,0,1)$ are linearly independent. Then*

$$\omega\Big(\prod_{\substack{(a_1,\ldots,a_n)\in A\\(b_1,\ldots,b_n)\in B}}(a_1b_1+\ldots+a_nb_n)\Big) > c_6 \log |A| \tag{2.1}$$

with an effectively computable positive number c_6.

Note that (1.2) follows from Theorem 2 by taking $n = 2$ and $b_1 = 1$ for all (b_1, b_2) in B. Further, for $n = 2$, Theorem 2 gives Theorem 1 if $b_2 = 1$ for each (b_1, b_2) in B.

The next theorem is a slightly modified version of Theorem 2. A vector $\mathbf{a} = (a_1,\ldots,a_n)$ in $\mathbb{N}^n$ is called *primitive* if $a_1,\ldots,a_n$ are relatively prime.

THEOREM 3. *Let $n \geq 2$ be an integer, and let A and B be finite subsets of $\mathbb{N}^n$ with $|A| \geq |B| \geq 2n-1$ and with the following properties: A consists of primitive vectors and any n vectors in B are linearly independent. Then the lower estimate* (2.1) *holds.*

In Theorems 2 and 3 all assumptions are necessary. For example, the vectors $\mathbf{a}$ in A must be primitive, since otherwise the left-hand side of (2.1) may assume the value

$$\omega\Big(\prod_{(b_1,\ldots,b_n)\in B}(a_1b_1+\ldots+a_nb_n)\Big)$$

for each $\mathbf{a} = (a_1,\ldots,a_n)$ in A. This is the case if A consists of vectors of the form $p^m\mathbf{a}$, $m = 1, 2, \ldots$, where p is a prime and $\mathbf{a}$ is in $\mathbb{N}^n$. Further, it is easy to see that the lower bounds $2(n-1)$ and $2n-1$, respectively, for $|B|$ cannot be lowered and that the linear independence of the vectors in B, respectively in $B \cup (0,\ldots,0,1)$, is necessary.

Since the nth prime can be estimated from below by a constant times $n \log n$, Theorem 1 implies the following result.

Corollary 1. *Let A and B be finite subsets of $\mathbb{N}$ with $|A| \geq |B| \geq 2$. Then there exist a in A and b in B such that*

$$P(ab+1) > c_7 \log|A| \log\log|A|,$$

where c_7 is an effectively computable positive constant.

Theorems 2 and 3 have similar consequences. An easy consequence of Theorem 1 is as follows.

Corollary 2. *Let A be a finite subset of $\mathbb{N}$ with $|A| \geq 2$. Then*

$$\omega\Big(\prod_{\substack{a,a' \in A \\ a \neq a'}} (aa'+1)\Big) > c_8 \log|A|,$$

where c_8 is an effectively computable positive constant.

We remark that a similar lower bound can be given for the total number of distinct prime factors of the special numbers of the form $aa'+1$ with $a' = a$ and a in A. For if $p_1, \ldots, p_s$ are the distinct prime factors of $\prod_{a\in A}(a^2+1)$, then all $x = a$ in A satisfy the equation $x^2 + 1 = p_1^{z_1} \ldots p_s^{z_s}$ in positive integers x and non-negative integers $z_1, \ldots, z_s$. Now Theorem 2 of Evertse [6] gives $|A| \leq 3 \cdot 7^{6+4s}$, whence

$$\omega\Big(\prod_{a\in A}(a^2+1)\Big) > c_9 \log|A|$$

follows with an effectively computable positive constant c_9. We note that this result has no additive analogue.

By Corollary 2 there exist distinct a, a' in A with $P(aa'+1) \to \infty$ as $|A| \to \infty$. This suggests the following conjecture.

Conjecture. *Let a, b and c denote distinct positive integers. If $\max(a,b,c) \to \infty$ then*

$$P((ab+1)(bc+1)(ca+1)) \to \infty.$$

To prove Theorems 2 and 3, we shall need two lemmas. Let

$$F(\mathbf{x}) = F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$$

be a decomposable form of degree r, that is a homogeneous polynomial which factorizes into linear forms $l_1(\mathbf{x}), \ldots, l_r(\mathbf{x})$ over a finite extension of $\mathbb{Q}$. Let R be a subring of $\mathbb{Q}$ which is finitely generated over $\mathbb{Z}$, so that $R = \mathbb{Z}\big[\frac{1}{p_1 \ldots p_s}\big]$ with s a non-negative integer and $p_1, \ldots, p_s$ distinct prime numbers. Consider the decomposable form equation

$$F(\mathbf{x}) \in R^* \quad \text{with } \mathbf{x} = (x_1, \ldots, x_n) \in R^n, \tag{2.2}$$

where R^* denotes the multiplicative group of units of R. If $\mathbf{x}$ is a solution of (2.2) then so is $\varepsilon\mathbf{x}$ for every ε in R^*. A set of solutions of the form $R^*\mathbf{x}$ is called an R^*-*coset of solutions*.

In [8], Evertse and Győry gave a finiteness criterion for equation (2.2). In the special case when the splitting field of F is $\mathbb{Q}$ this criterion can be formulated in the following form. Denote by L_0 a maximal subset of pairwise linearly independent linear forms in $\{l_1, \ldots, l_r\}$. For any system L of linear forms from $\mathbb{Q}[x_1, \ldots, x_n]$, we denote by $V(L)$ the $\mathbb{Q}$-vector space generated by the forms of L. Then we have the following lemma.

LEMMA 1. *Suppose that the linear factors $l_1, \ldots, l_r$ of F have rational coefficients. Then the following two statements are equivalent*:

(i) *The forms in L_0 have rank n over $\mathbb{Q}$ and for each proper non-empty subset L_1 of L_0 there is a linear form in L_0 which is contained both in $V(L_1)$ and in $V(L_0 \backslash L_1)$*;

(ii) *The number of R^*-cosets of solutions of* (2.2) *is finite for every finitely generated subring R of $\mathbb{Q}$.*

Proof. This is an immediate consequence of Theorem 2 and the Proposition in [8].

Using a result of Schlickewei [19] on S-unit equations, Győry [10] gave an upper bound for the number of families of solutions of (2.2). This implies an upper bound for the number of R^*-cosets of solutions of (2.2), provided that condition (i) in Lemma 1 is fulfilled. Recently Evertse [7] has improved this latter bound by proving the following result.

LEMMA 2. *If the finiteness condition* (i) *of Lemma* 1 *holds*, *then equation* (2.2) *has at most* $(2^{33}r^2)^{n^3(s+1)}$ *R^*-cosets of solutions.*

The proof depends on Evertse's improvement of the quantitative subspace theorems of Schmidt [21] and Schlickewei [20].

Proof of Theorem 2. It suffices to prove the theorem for the case when B has cardinality $2(n-1)$. Put $r = 2n-1$. Let $\mathbf{b}_i = (b_{i1}, \ldots, b_{in})$ be the elements of B for $i = 1, \ldots, r-1$, and put $\mathbf{b}_r = (b_{r1}, \ldots, b_{rn}) = (0, \ldots, 0, 1)$. Let $l_i(\mathbf{x}) = b_{i1}x_1 + \ldots + b_{in}x_n$ for $i = 1, \ldots, r$. Then $F(\mathbf{x}) = l_1(\mathbf{x}) \ldots l_r(\mathbf{x})$ is a decomposable form of degree r with coefficients in $\mathbb{Z}$ which factorizes into linear factors over $\mathbb{Q}$. Denote by $p_1, \ldots, p_s$ the distinct prime factors of the product

$$\prod_{\substack{(a_1, \ldots, a_n) \varepsilon A \\ i=1, \ldots, r}} (a_1 b_{i1} + \ldots + a_n b_{in}),$$

and by R the ring $\mathbb{Z}\left[\frac{1}{p_1 \ldots p_s}\right]$. Then we have $s > 0$. Since, by assumption, $a_n = 1$ for all $(a_1, \ldots, a_n) \in A$, all the vectors $\mathbf{a} = (a_1, \ldots, a_n)$ in A are solutions of the decomposable form equation (2.2) and these solutions belong to distinct R^*-cosets.

We use now an idea from the proof of Theorem 3 of [11]. Put $L_0 = \{l_1, \ldots, l_r\}$. By assumption, the forms in L_0 have rank n and are pairwise linearly independent over $\mathbb{Q}$. Consider an arbitrary proper non-empty subset L_1 of L_0. Since $r = 2n-1$, at least one of L_1 and $L_0 \backslash L_1$ has cardinality at least n. If $|L_1| \geq n$ then L_1 has rank n. In this case we have $L_0 \backslash L_1 \subseteq V(L_1)$ and so $L_0 \backslash L_1$ is contained both in $V(L_1)$ and in $V(L_0 \backslash L_1)$. If $|L_0 \backslash L_1| \geq n$, we get in the same way that L_1 is contained in $V(L_1)$ and $V(L_0 \backslash L_1)$. We can now apply Lemmas 1 and 2 to equation (2.2). We get

$$|A| \leq (2^{33}(2n-1)^2)^{n^3(s+1)}.$$

Our result now follows by taking logarithms.

Proof of Theorem 3. Theorem 3 can be proved in a similar way as Theorem 2 above.

3. An upper bound. In this section we will prove the multiplicative analogue of (1.3). Erdős, Stewart and Tijdeman [4] proved a result which includes (1.3) as a special case. Let $\varepsilon > 0$. For instance, it follows from Theorem 1 of [4] that there is a positive number c_{10} which is effectively computable in terms of ε, such that if k is an integer larger than c_{10} and l is an integer with $2 \leq l \leq (\log k)/\log\log k$ then there exists a set of positive integers A of cardinality k and a set of non-negative integers of cardinality l such that

$$P\Big(\prod_{a\in A}\prod_{b\in B}(a+b)\Big) < \left((1+\varepsilon)\frac{\log k}{l}\log\left(\frac{\log k}{l}\right)\right)^l. \tag{3.1}$$

In this section we shall prove the following result.

THEOREM 4. *Let ε be a positive real number and let k and l be positive integers with*

$$k \geq 16 \quad \textit{and} \quad 2 \leq l \leq \left(\frac{\log\log k}{\log\log\log k}\right)^{1/2}.$$

There exists a positive number $c_{11}(\varepsilon)$, which is effectively computable in terms of ε, such that if k exceeds $c_{11}(\varepsilon)$ then there are sets of positive integers A and B with $|A| = k$ and $|B| = l$ for which

$$P\Big(\prod_{a\in A}\prod_{b\in B}(ab+1)\Big) < (\log k)^{l+1+\varepsilon}. \tag{3.2}$$

Of course estimate (3.2) also applies with ω in place of P. While the estimate (3.2) is weaker than (3.1) it is worth noting that we have allowed B to include 0 in the additive case and not in the multiplicative case. In the latter case we may certainly add 0 to B and so increase the cardinality of B by 1 without affecting the upper bound. On the other hand, (3.1) applies over a wider range for l. Indeed, Erdős, Stewart and Tijdeman were able to obtain significant improvements on the trivial estimate $k+l$ for l in the range $2 \le l \le \theta \log k$ for any real number θ less than 1 (see Theorem 2 of [4]). We are able to extend the range for l in the statement of Theorem 4 and bound the largest elements of A and B at the cost of some precision in our upper bound in (3.2).

THEOREM 5. *Let k and l be positive integers with $k \ge 3$. There exist effectively computable positive numbers c_{12} and c_{13} such that if k exceeds c_{12} and*

$$2 \le l \le c_{13}(\log k)/\log\log k,$$

then there are subsets A and B of $\{1,\ldots,k^3\}$ with $|A| = k$ and $|B| = l$ for which

$$P\Big(\prod_{a\in A}\prod_{b\in B}(ab+1)\Big) < (\log k)^{5l}. \tag{3.3}$$

One reason that the upper bounds (3.2) and (3.3) are not as sharp as (3.1) is that we must replace Lemma 1 of [4] by Lemma 4 below.

LEMMA 3. *Let N, L, t and l be positive integers with*

$$4lL \le t. \tag{3.4}$$

Let S be a set of N elements and let $A_1,\ldots,A_t$ be subsets of S with at least N/L elements. Then there exist distinct integers $i_1,\ldots,i_l$ such that

$$|A_{i_1}\cap\ldots\cap A_{i_l}| \ge N/(4L)^l.$$

P r o o f. Let $a_1,\ldots,a_N$ be the elements of A and put

$$M = \max_{1\le i_1<\ldots<i_l\le t} |A_{i_1}\cap\ldots\cap A_{i_l}|$$

and

$$Z = \sum_{1\le i_1<\ldots<i_l\le t} |A_{i_1}\cap\ldots\cap A_{i_l}|.$$

We have

$$Z \le M\binom{t}{l} \le Mt^l/l!. \tag{3.5}$$

Further, on putting $N_j = |\{i : 1\le i\le t,\ a_j \in A_i\}|$ for $j = 1,\ldots,N$, we see that

$$Z = \sum_{1\le i_1<\ldots<i_l\le t}\ \sum_{\substack{1\le j\le N\\ a_j\in A_{i_1}\cap\ldots\cap A_{i_l}}} 1 \tag{3.6}$$

$$= \sum_{j=1}^{N} \sum_{\substack{1\le i_1<\ldots<i_l\le t\\ a_j\in A_{i_1}\cap\ldots\cap A_{i_l}}} 1 = \sum_{j=1}^{N} \binom{N_j}{l}.$$

We shall now estimate $\sum_{j=1}^{N}\binom{N_j}{l}$ from below. To this end we note that

$$\sum_{j=1}^{N} N_j = \sum_{j=1}^{N} \sum_{\substack{1\le i\le t\\ a_j\in A_i}} 1 = \sum_{i=1}^{t} \sum_{\substack{1\le j\le N\\ a_j\in A_i}} 1 = \sum_{j=1}^{t} |A_i|,$$

hence that

$$\sum_{j=1}^{N} N_j \ge Nt/L. \tag{3.7}$$

Put

$$J = \{j : 1 \le j \le N,\ N_j > t/(2L)\}.$$

We have, by (3.7),

$$\sum_{j\in J} N_j = \sum_{j=1}^{N} N_j - \sum_{\substack{1\le j\le N\\ j\notin J}} N_j \ge \sum_{j=1}^{N} N_j - \frac{Nt}{2L} \ge \frac{Nt}{2L}. \tag{3.8}$$

Further, by (3.4), for all j in J,

$$\binom{N_j}{l} = \frac{N_j(N_j-1)\ldots(N_j-l+1)}{l!} \ge \frac{(N_j/2)^l}{l!}. \tag{3.9}$$

Since, for any positive real numbers $x_1,\ldots,x_u$,

$$\sum_{i=1}^{u} x_i^l \ge \Big(\sum_{i=1}^{u} x_i\Big)^l / u^{l-1},$$

we have, from (3.8) and (3.9),

$$\sum_{j\in J}\binom{N_j}{l} \ge \frac{1}{2^l l!}\left(\frac{Nt}{2L}\right)^l N^{-l+1} = \frac{N}{(4L)^l}\cdot\frac{t^l}{l!}. \tag{3.10}$$

Our result now follows from (3.5), (3.6) and (3.10).

Lemma 4. *Let N, L and l be positive integers with $l \le L \le N$ and let X and Y be non-empty sets of positive integers such that*

$$4lL \le |X|, \tag{3.11}$$

and for each x in X there are at least N/L integers j with $1 \le j \le N$ for which jx is in Y. Then there is a subset A of $\{1,\ldots,N\}$ and a subset B of X with

$$|B| = l \quad \text{and} \quad |A| \ge N/(4L)^l, \tag{3.12}$$

for which $A \cdot B \subset Y$.

Proof. We apply Lemma 3 with $S=\{1,\dots,N\}$, $t=|X|$, $X=\{x_1,\dots\ \dots,x_t\}$ and $A_i=\{j : 1\le j\le N \text{ and } jx_i\in Y\}$ for $i=1,\dots,t$. Note that $|A_i|\ge N/L$ for $i=1,\dots,t$. Then there exist distinct integers $i_1,\dots,i_l$ such that $|A_{i_1}\cap\dots\cap A_{i_l}|\ge N/(4L)^l$. Put $A=A_{i_1}\cap\dots\cap A_{i_l}$ and $B=\{x_{i_1},\dots,x_{i_l}\}$. Our result now follows.

Lemma 5. *Let M be an integer, N a positive integer and $a_{M+1},\dots,a_{M+N}$ complex numbers. For each character χ put*

$$T(\chi)=\sum_{n=M+1}^{M+N} a_n\chi(n).$$

Then for any $Q\ge 1$, we have

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi\,(\mathrm{mod}\,q)}|T(\chi)|^2\le (Q^2+\pi N)\sum_{n=M+1}^{M+N}|a_n|^2,$$

where $\sum^*_{\chi\,(\mathrm{mod}\,q)}$ denotes a sum over all primitive characters modulo q.

Proof. This character version of the large sieve is due to Gallagher [9].

Lemma 6. *Let R be a positive integer, J a subset of $\{1,\dots,R\}$ and Q a real number with $Q\ge 1$. For each prime p, denote the number of solutions of the congruence*

$$rr'\equiv 1 \pmod p,$$

with r and r' in J, by $F(J,p)$ and denote the number of the integers in J divisible by p by $G(J,p)$. Then

$$\sum_{p\le Q}p\left|F(J,p)-\frac{1}{p-1}(|J|-G(J,p))^2\right|\le (Q^2+\pi R)|J|.$$

Proof. Let χ_0 denote the principal character modulo p. We have

$$\begin{aligned}
F(J,p)&=\sum_{r\in J}\sum_{r'\in J}\frac{1}{\varphi(p)}\sum_{\chi\,(\mathrm{mod}\,p)}\chi(rr')\\
&=\frac{1}{p-1}\sum_{\chi\,(\mathrm{mod}\,p)}\Big(\sum_{r\in J}\chi(r)\Big)^2\\
&=\frac{1}{p-1}\bigg(\Big(\sum_{\substack{r\in J\\ p\nmid r}}1\Big)^2+\sum_{\chi\ne\chi_0\,(\mathrm{mod}\,p)}\Big(\sum_{r\in J}\chi(r)\Big)^2\bigg)\\
&=\frac{1}{p-1}\bigg((|J|-G(J,p))^2+\sideset{}{^*}\sum_{\chi\,(\mathrm{mod}\,p)}\Big(\sum_{r\in J}\chi(r)\Big)^2\bigg)
\end{aligned}$$

whence

$$\left|F(J,p)-\frac{1}{p-1}(|J|-G(J,p))^2\right|\le\frac{1}{p-1}\sideset{}{^*}\sum_{\chi\,(\mathrm{mod}\,p)}\Big|\sum_{r\in J}\chi(r)\Big|^2.$$

By Lemma 5, it follows that

$$\sum_{p\le Q}p\left|F(J,p)-\frac{1}{p-1}(|J|-G(J,p))^2\right|\le(Q^2+\pi R)|J|.$$

Let $\psi(x,y)$ be the number of positive integers not exceeding x which are free of prime divisors larger than y.

LEMMA 7. *Let x be a positive integer and u a real number with $u\ge 3$. There exists an effectively computable constant c_{14} such that*

$$\psi(x,x^{1/u})\ge x\exp\bigg(-u\bigg(\log u+\log\log u-1+c_{14}\bigg(\frac{\log\log u}{\log u}\bigg)\bigg)\bigg).$$

Proof. See Theorem 3.1 of Canfield, Erdős and Pomerance [1].

For any positive integer n let $\tau(n)$ denote the number of positive divisors of n.

LEMMA 8. *There is an effectively computable number c_{15} such that if N is a positive integer larger than c_{15} and A is a subset of $\{1,\ldots,N\}$ then the set $A'=\{a:a\in A$ and $\tau(a)<(4N\log N)/|A|\}$ satisfies*

$$|A'|>|A|/2. \tag{3.13}$$

Proof. There is an effectively computable number N_0 such that for $N>N_0$,

$$\sum_{a\in A}\tau(a)\le\sum_{n=1}^{N}\tau(n)<2N\log N \tag{3.14}$$

(see, for instance, Theorem 320 of [13]). On the other hand, we have

$$\sum_{a\in A}\tau(a)\ge\sum_{a\in(A\setminus A')}\tau(a)\ge\sum_{a\in(A\setminus A')}(4N\log N)/|A|$$

so

$$\sum_{a\in A}\tau(a)\ge 2N\log N(2-2|A'|/|A|). \tag{3.15}$$

It follows from (3.14) and (3.15) that $2-2|A'|/|A|<1$ and this implies (3.13).

Proof of Theorem 4. We may assume, without loss of generality, that $0<\varepsilon<1$. Let $C_1,C_2,\ldots$ denote positive numbers which are effectively computable in terms of ε. Let N be a positive integer larger than 30 and let l be a positive integer with

$$2 \le l \le ((\log\log N)/\log\log\log N)^{1/2}. \tag{3.16}$$

For any real number x let $[x]$ denote the greatest integer less than or equal to x. Put $R = [N^{(l+1)/(2l)}]$, $Q = 2N^{1/l}$ and $y = (\log R)^{l+1+\varepsilon}$. Let J denote the set of positive integers n with $n \le R$ and $P(n) \le y$. Put

$$u = \frac{\log R}{(l+1+\varepsilon)\log\log R},$$

and notice that for $N > C_1$ we have $u \ge 3$, hence, by Lemma 7,

$$|J| \ge \psi(R,y) \ge R\exp\left(-u\left(\log u+\log\log u-1+c_{14}\left(\frac{\log\log u}{\log u}\right)\right)\right). \tag{3.17}$$

Thus, for $N > C_2$,

$$|J| \ge R^{1-1/(l+1+\varepsilon)} = R^{l/(l+1)+\varepsilon/((l+1)(l+1+\varepsilon))},$$

whence

$$|J| \ge N^{1/2}N^{\varepsilon/(3l(l+1))} \tag{3.18}$$

for $N > C_3$.

Let F be the set of integers of the form $rr'-1$ with r, r' in J. Define $F(J,p)$ to be the number of pairs (r,r') with $rr'-1$ divisible by p and let $G(J,p)$ be the number of integers in J divisible by p.

Let E be the set of primes p with $Q/2 < p \le Q$ for which

$$F(J,p) > |J|^2/(2Q), \tag{3.19}$$

and let $\overline{E}$ be the other primes in this range. Observe that for $N > C_4$, $y < Q/2$, so $G(J,p) = 0$ whenever p exceeds $Q/2$. Thus for $p \in \overline{E}$ we have

$$\frac{1}{p-1}(|J| - G(J,p))^2 = \frac{|J|^2}{p-1} \ge \frac{|J|^2}{Q}. \tag{3.20}$$

From Lemma 6, we deduce that

$$\sum_{p\in\overline{E}} p\left|F(J,p) - \frac{1}{p-1}(|J|-G(J,p))^2\right| \le (Q^2+\pi R)|J|.$$

Since for p in $\overline{E}$ we have, by (3.18) and (3.19),

$$\left|F(J,p) - \frac{1}{p-1}(|J|-G(J,p))^2\right| > |J|^2/(2Q),$$

it follows that

$$|\overline{E}|\cdot|J|^2/4 \le (Q^2+\pi R)|J|, \tag{3.21}$$

hence that $|\overline{E}| \le 32\max(N^{2/l}/|J|, R/|J|)$. Thus, by (3.18),

$$|\overline{E}| \le \begin{cases} N^{1/2}N^{-\varepsilon/20} & \text{for } l = 2,\\ N^{1/(2l)} & \text{for } l \ne 2,\end{cases}$$

for $N > C_5$. However, for $N > C_6$, there are at least $Q/(3\log Q)$ primes p with $Q/2 < p \le Q$. Further, for $N > C_7$, $|\overline{E}| < Q/(6\log Q)$, whence

$$|E| > Q/(6\log Q). \tag{3.22}$$

For each prime p in E there are more than $|J|^2/(2Q)$ pairs (r, r') with r and r' in R for which p divides $rr' - 1$. Put $D = \max_{n\le R}\tau(n)$. By, for instance, Theorem 317 of [13],

$$D < \exp(\log N/\log\log N)$$

for $N > C_8$. Moreover, if an integer n can be represented in the form rr' with r and r' in R then it can be represented in at most D^2 ways in this form. Thus, for each prime p in E there are at least $|J|^2/(2D^2Q)$ distinct integers f with $f = rr' - 1$ and for which p divides f. Let $j = f/p$ and notice that

$$1 \le j \le R^2/(Q/2) < N.$$

For $N > C_9$, we have

$$|J|^2/(2D^2Q) \ge N/L,$$

where

$$L = \tfrac{1}{4}N^{1/l-\varepsilon/(4l(l+1))}. \tag{3.23}$$

We may now apply Lemma 4 with $X = E$ and $Y = F$. We remark that condition (3.11) applies for $N > C_{10}$ by virtue of (3.22) and (3.23). We find that there is a subset A_1 of $\{1, \ldots, N\}$ and a subset B of E with $|B| = l$ and

$$|A_1| \ge N/(4l)^l = N^{\varepsilon/(4(l+1))},$$

for which $A_1 \cdot B$ is contained in F.

Let k be an integer larger than 15 and let l be an integer with

$$2 \le l \le \left(\frac{\log\log k}{\log\log\log k}\right)^{1/2}.$$

Choose N so that

$$k = [N^{\varepsilon/(4(l+1))}].$$

Since $k \le N$, (3.16) holds and provided that k exceeds C_{11}, we may find A_1 and B as above. Let A be a subset of A_1 with $|A| = k$. Notice that

$$(\varepsilon/(5(l+1)))\log N < \log k$$

for $N > C_{12}$ and that

$$\log R \le ((l+1)/(2l))\log N.$$

Thus, for $k > C_{13}$, we have

$$y \le ((5(l+1)^2/(2\varepsilon l))\log k)^{l+1+\varepsilon} \le (\log k)^{l+1+2\varepsilon}.$$

Since $P(ab+1)$ is at most y whenever a is in A and b is in B, our result follows.

Proof of Theorem 5. Our proof of Theorem 5 is a modification of the proof of Theorem 4. Let $C_1, C_2, \ldots$ denote effectively computable positive numbers. Let k be a positive integer, θ be a positive real number and l be an integer with

$$2 \le l \le (\theta \log k)/\log\log k. \tag{3.24}$$

Put $N = k^3$, $Q = 2N^{1/2}$ and $R = [N^{3/4}]$. Let

$$y = (\log R)^{14l/3} \tag{3.25}$$

and put

$$u = (14\log R)/(3l\log\log R).$$

Let J' denote the set of positive integers n with $n \le R$ and $P(n) \le y$. If $\theta < C_1$ we have $u \ge 3$ and so (3.17) holds with J' in place of J. Further if $\theta < C_2$ we have

$$-1 + c_{14}((\log\log u)/\log u) < 0,$$

and so, for $k > C_3$,

$$|J'| \ge 2N^{(3/4)(1-3/(14l))}.$$

We may now apply Lemma 7 to find a subset J of J' with $|J| \ge |J'|/2$, hence for which

$$|J| \ge N^{(3/4)(1-3/(14l))}, \tag{3.26}$$

and for which D, the maximum of $\tau(n)$ for n in J, satisfies

$$D < 4R\log R/|J'|.$$

Thus, for $k > C_4$,

$$D < 2N^{9/(56l)}\log N. \tag{3.27}$$

We now define F, E and $\overline{E}$, as in the proof of Theorem 4. We again apply Lemma 6 to deduce that (3.21) holds. Consequently, for $k > C_5$, we find that $|\overline{E}| \le 20N/|J|$, and, from (3.26), we see that $|\overline{E}| < Q/(6\log Q)$, whence (3.22) holds.

Therefore, as in the proof of Theorem 4, we find that there are at least $|J|^2/(2D^2Q)$ distinct integers f with $f = rr' - 1$, r and r' in J, and for which p divides f. Let $j = f/p$ and notice that $1 \le j \le N$. Further, we have

$$|J|^2/(2D^2Q) \ge N/(16N^{36/(56l)}(\log N)^2).$$

Thus, for $\theta < C_6$ and $k > C_7$, we have

$$|J|^2/(2D^2Q) \geq N/L,$$

where

$$L = \tfrac{1}{4}N^{2/(3l)}. \tag{3.28}$$

We may now apply Lemma 4 with $X = E$ and $Y = F$. For $\theta < C_8$, (3.11) holds by virtue of (3.24) and (3.28). We find that there is a subset A_1 of $\{1, \ldots, N\}$ and a subset B of E with $|B| = l$ and

$$|A_1| \geq N/(4l)^l = N^{1/3},$$

for which $A_1 \cdot B$ is contained in F. We now let A be a subset of A_1 with $|A| = k$. Take $\theta = \frac{1}{2}\min(C_1, C_2, C_6, C_8)$. Then for $k > C_9$, (3.24) holds and

$$P\Big(\prod_{a\in A}\prod_{b\in B}(ab+1)\Big) < \left(\frac{9}{4}\log k\right)^{14l/3} < (\log k)^{5l},$$

as required.

4. Terms with many prime factors. In this section we shall establish the multiplicative analogue of (1.5). For the proof we shall require the following result which was derived with the aid of the large sieve inequality.

LEMMA 9. *Let N be a positive integer and let A and B be non-empty subsets of $\{1, \ldots, N\}$. Let α and β be real numbers with $\alpha > 1$. Let T be the set of primes p which satisfy $\beta < p \leq (\log N)^\alpha$ and let S be a subset of T consisting of all but at most $2\log N$ elements of T. There is a real number c_{16}, which is effectively computable in terms of α and β, such that if N exceeds c_{16} and*

$$(|A| \cdot |B|)^{1/2} \geq N^{(1+1/\alpha)/2}/10$$

then there is a prime p from S and elements a from A and b from B such that p divides $ab + 1$.

Proof. This is Lemma 3 of [18].

We shall use Lemma 9 to prove the next result.

THEOREM 6. *Let θ be a real number with $1/2 < \theta \leq 1$ and let N be a positive integer. There exists a positive number c_{17}, which is effectively computable in terms of θ, such that if A and B are subsets of $\{1, \ldots, N\}$ with N greater than c_{17} and*

$$(|A| \cdot |B|)^{1/2} \geq N^\theta, \tag{4.1}$$

then there exists an integer a from A and an integer b from B for which

$$\omega(ab+1) > \tfrac{1}{6}(\theta - 1/2)^2 \log N/\log\log N. \tag{4.2}$$

P r o o f. Our proof is very similar to the proof of Theorem 1 of [17]. We have repeated parts of that argument here for the convenience of the reader.

Let $\theta_1 = (\theta + 1/2)/2$ and define G and v by

$$G = (\log N)^{1/(2\theta_1 - 1)},$$

and

$$v = \left[\frac{1}{6}(\theta - 1/2)^2 \frac{\log N}{\log\log N}\right] + 1, \tag{4.3}$$

respectively.

Put $A_0 = A, B_0 = B$ and $W_0 = \emptyset$. We shall construct inductively sets $A_1, \ldots, A_v, B_1, \ldots, B_v$ and $W_1, \ldots, W_v$ with the following properties. First, W_i is a set of i primes q satisfying $10 < q \le G, A_i \subseteq A_{i-1}$ and $B_i \subseteq B_{i-1}$ for $i = 1, \ldots, v$. Secondly, every element of the set $A_iB_i + 1$ is divisible by each prime in W_i for $i = 1, \ldots, v$. Finally,

$$|A_i| \ge |A|/G^{3i} \quad \text{and} \quad |B_i| \ge |B|/G^{3i} \tag{4.4}$$

for $i = 1, \ldots, v$. Note that this suffices to prove our result since A_v and B_v are both non-empty and on taking a from A_v and b from B_v we find that $ab + 1$ is divisible by the v primes from W_v and so (4.2) follows from (4.3).

Suppose that i is an integer with $0 \le i < v$ and that A_i, B_i and W_i have been constructed with the above properties. We shall now show how to construct A_{i+1}, B_{i+1} and W_{i+1}. First, for each prime p with $10 < p \le G$ let $a_1, \ldots, a_{j(p)}$ be representatives for those residue classes modulo p which are occupied by fewer than $|A_i|/p^3$ terms of A_i. For each prime p with $10 < p \le G$ we remove from A_i those terms of A_i which are congruent to one of $a_1, \ldots, a_{j(p)}$ modulo p. We are left with a subset A_i' of A_i with

$$|A_i'| \ge |A_i|\Big(1 - \sum_{10<p\le G} \frac{j(p)}{p^3}\Big) \ge |A_i|\Big(1 - \sum_{10<p} \frac{1}{p^3}\Big) \ge \frac{|A_i|}{10} \tag{4.5}$$

and such that for each prime p with $10 < p \le G$ and each a' in A_i', the number of terms of A_i which are congruent to a' modulo p is at least $|A_i|/p^3$. Similarly, we produce a subset B_i' of B_i with

$$|B_i'| \ge |B_i|/10 \tag{4.6}$$

and such that for each prime p with $10 < p \le G$ and each residue class modulo p which contains an element of B_i' the number of terms of B_i in the residue class is at least $|B_i|/p^3$.

The number of terms in W_i is i which is less than v and, by (4.3), is at most $\log N$. Further by (4.4), we find that

$$(|A_i| \cdot |B_i|)^{1/2} = (|A| \cdot |B|)^{1/2} G^{-3i} \ge N^{\theta_1}. \tag{4.7}$$

Therefore, by (4.5)–(4.7),

$$(|A'_i|\cdot|B'_i|)^{1/2}\ge N^{\theta_1}/10.$$

We now apply Lemma 9 with $A=A'_i$, $B=B'_i$, $\beta=10$, $\alpha=1/(\theta-1/2)$ and S the set of primes p with $10<p\le G$ for which p is not in W_i. We find that provided that N exceeds a number which is effectively computable in terms of θ, there is a prime q_{i+1} in S, an element a' in A'_i and an element b' in B'_i such that q_{i+1} divides $a'b'+1$. We put

$$A_{i+1}=\{a\in A_i : a\equiv a' \pmod{q_{i+1}}\},$$
$$B_{i+1}=\{b\in B_i : b\equiv b' \pmod{q_{i+1}}\},$$

and

$$W_{i+1}=W_i\cup\{q_{i+1}\}.$$

By our construction every element of $A_{i+1}B_{i+1}+1$ is divisible by each prime in W_{i+1}. Further, we have, by (4.4),

$$|A_{i+1}|\ge\frac{|A_i|}{q_{i+1}^3}\ge\frac{|A_i|}{G^3}\ge\frac{|A|}{G^{3(i+1)}},$$

and

$$|B_{i+1}|\ge\frac{|B|}{G^{3(i+1)}},$$

as required. Our result now follows.

5. Terms with few prime factors. Let N and l be positive integers with $l<\log N$. Pomerance, Sárközy and Stewart [14] proved that there exists an effectively computable positive number C_{18} such that if N exceeds C_{18} then there exist subsets A and B of $\{1,\dots,N\}$ with $|B|=l$ and

$$|A|>\frac{N}{l(\log N)^l},$$

such that every element of $A+B$ is prime. We shall prove the following result.

THEOREM 7. *Let N and l be positive integers with*

$$l\le\frac{\log N}{2\log\log N}. \tag{5.1}$$

For N sufficiently large, there exists a set B of l prime numbers from $\{1,\dots,[(\log N)^3]\}$ and a subset A of $\{1,\dots,N\}$ with

$$|A|\ge\frac{N}{(8\log N)^l},$$

such that $ab+1$ is a prime whenever a is from A and b is from B.

The proof depends on the Siegel–Walfisz theorem for primes in arithmetical progressions and as a consequence is ineffective in nature. In particular, we are not able to replace the requirement that N be sufficiently large with the requirement that N be larger than an effectively computable positive number.

Let ε be a positive real number. It follows from Theorem 6 that if A and B are subsets of $\{1,\ldots,N\}$ with $|A|\cdot|B|>N^{1+\varepsilon}$ then

$$\max_{a\in A,\, b\in B}\omega(ab+1)\to\infty \tag{5.2}$$

as $N\to\infty$. Taking $l=2$ in the statement of Theorem 7 we see that there are subsets A and B of $\{1,\ldots,N\}$ with $|B|=2$ and

$$|A|\ge\frac{N}{64(\log N)^2}$$

for which

$$\max_{a\in A,\, b\in B}\omega(ab+1)=1. \tag{5.3}$$

Thus if we measure the size of A and B in terms of the geometric mean of the cardinalities of A and B, we have determined, up to a factor of ε, when (5.2) holds. On the other hand, if we measure the size of A and B in terms of the minimum of $|A|$ and $|B|$, a different situation applies. Certainly, (5.2) holds if

$$\min(|A|,|B|)>N^{1/2+\varepsilon} \tag{5.4}$$

by Theorem 6. Further, by Theorem 7 we see that there are subsets A and B of $\{1,\ldots,N\}$ with

$$\min(|A|,|B|)\ge\left[\frac{\log N}{2\log\log N}\right] \tag{5.5}$$

for which (5.3) holds. There is a large gap between (5.4) and (5.5). We suspect that (5.5) is closer to the truth.

Proof of Theorem 7. Let X denote the set of prime numbers less than $(\log N)^3$. By the prime number theorem we have

$$|X|>\frac{(\log N)^3}{4\log\log N}$$

for N sufficiently large. Let Y denote the set of integers of the form $p-1$, where p is a prime. By the Siegel–Walfisz theorem (see for example [2], p. 133) if q is in X then the number of integers j with $1\le j\le N$ for which qj is in Y, or equivalently for which $qj+1$ is prime, is $(1+o(1))\frac{qN}{(q-1)\log N}$ and so for N sufficiently large exceeds N/L, where $L=2[\log N]$. We may now apply Lemma 4 with l satisfying (5.1). Then (3.11) holds for N sufficiently large and our result follows directly.

6. The average value of $\omega(ab+1)$. Finally, we shall prove the multiplicative analogue of (1.6).

THEOREM 8. *There exists an effectively computable positive number c_{19} such that if T and N are positive integers with $T \le N^{1/2}$ and A and B are non-empty subsets of $\{1,\ldots,N\}$ then*

$$\left|\frac{1}{|A|\cdot|B|}\sum_{T<p}\ \sum_{a\in A,\,b\in B,\,p\mid ab+1} 1-(\log\log N-\log\log 3T)\right| < c_{19}\left(1+\frac{N}{T\min(|A|,|B|)}\right).$$

Taking $T=[N/\min(|A|,|B|)]$ in Theorem 8 we obtain the following result.

COROLLARY 3. *There exists an effectively computable positive number c_{20} such that if N is a positive integer and A and B are non-empty subsets of $\{1,\ldots,N\}$ then*

$$\left|\frac{1}{|A|\cdot|B|}\sum_{p>N/\min(|A|,|B|)}\ \sum_{a\in A,\,b\in B,\,p\mid ab+1} 1 - (\log\log N-\log\log(3N/\min(|A|,|B|)))\right| < c_{20}.$$

Therefore

$$\frac{1}{|A|\cdot|B|}\sum_{a\in A}\sum_{b\in B}\omega(ab+1) > (1+o(1))\log\log N,$$

provided that A and B are subsets of $\{1,\ldots,N\}$ with

$$\min(|A|,|B|)=N\exp(-(\log N)^{o(1)}).$$

Proof of Theorem 8. The proof will be similar to the proof of Theorem 3 of [17]. However, while in [17] the crucial tool in the proof is the standard analytical form of the large sieve, here, due to the multiplicative structure of the numbers studied, we employ Lemma 5. Let $C_1, C_2, \ldots$ denote effectively computable positive numbers.

Put $R=[(N^2+1)^{1/4}]$. We have

$$(6.1)\quad \left|\sum_{a\in A}\sum_{b\in B}\sum_{T<p,\,p\mid ab+1} 1-\sum_{a\in A}\sum_{b\in B}\sum_{T<p\le R,\,p\mid ab+1} 1\right| = \left|\sum_{a\in A}\sum_{b\in B}\sum_{R<p\le N^2+1,\,p\mid ab+1} 1\right| \le \left|\sum_{a\in A}\sum_{b\in B} 3\right| = 3|A|\cdot|B|.$$

We define, for each character χ,

$$F(\chi)=\sum_{a\in A}\chi(a),\qquad G(\chi)=\sum_{b\in B}\chi(b).$$

Then

$$\begin{aligned}\sum_{a\in A}\sum_{b\in B}\sum_{T<p\le R,\, p\mid ab+1}1&=\sum_{T<p\le R}\frac{1}{p-1}\sum_{\chi\,(\mathrm{mod}\,p)}\overline{\chi}(-1)\sum_{a\in A}\sum_{b\in B}\chi(ab)\\&=\sum_{T<p\le R}\frac{1}{p-1}\Big(\sum_{p\nmid a,\,a\in A}\ \sum_{p\nmid b,\,b\in B}1+\sum_{\chi\ne\chi_0\,(\mathrm{mod}\,p)}\overline{\chi}(-1)F(\chi)G(\chi)\Big)\end{aligned}$$

whence

$$\begin{aligned}&\Big|\sum_{a\in A}\sum_{b\in B}\sum_{T<p\le R,\,p\mid ab+1}1-|A|\cdot|B|\sum_{T<p\le R}\frac{1}{p-1}\Big|\\&\le\sum_{T<p\le R}\frac{1}{p-1}\Big(\sum_{p\mid a,\,a\in A}\ \sum_{b\in B}1+\sum_{a\in A}\ \sum_{p\mid b,\,b\in B}1+\sum_{\chi\ne\chi_0\,(\mathrm{mod}\,p)}|F(\chi)|\cdot|G(\chi)|\Big)\\&\le\sum_{T<p\le R}\frac{1}{p-1}\Big(\Big(\sum_{p\mid n,\,n\le N}1\Big)(|A|+|B|)+\tfrac12\sum_{\chi\ne\chi_0\,(\mathrm{mod}\,p)}(|F(\chi)|^2+|G(\chi)|^2)\Big)\\&\le 2(|A|+|B|)\sum_{T<p\le R}\frac{N}{p^2}+\sum_{T<p\le R}\frac{1}{\varphi(p)}\sum_{\chi\ne\chi_0\,(\mathrm{mod}\,p)}(|F(\chi)|^2+|G(\chi)|^2).\end{aligned}$$

Further, we have

$$\Big|\sum_{T<p\le R}\frac{1}{p-1}-(\log\log R-\log\log 3T)\Big|<C_1.$$

Thus it follows that

$$\begin{aligned}\Big|\sum_{a\in A}\sum_{b\in B}\sum_{T<p\le R,\,p\mid ab+1}1-|A|\cdot|B|(\log\log R-\log\log 3T)\Big|\\<C_1|A|\cdot|B|+C_2\frac{N}{T\log T}(|A|+|B|)\\+\sum_{T<p\le R}\frac{1}{\varphi(p)}\sum_{\chi\ne\chi_0\,(\mathrm{mod}\,p)}(|F(\chi)|^2+|G(\chi)|^2).\end{aligned}\tag{6.2}$$

Put

$$S(n)=\sum_{p\le n}\frac{p}{\varphi(p)}\sum_{\chi\ne\chi_0\,(\mathrm{mod}\,p)}|F(\chi)|^2.$$

Then, by Lemma 5, for $n\le R$ we have

$$S(n)\le(n^2+\pi N)|A|\le 6N|A|.$$

Thus we obtain by partial summation that

$$\sum_{T<p\le R}\frac{1}{\varphi(p)}\sum_{\chi\ne\chi_0\ (\mathrm{mod}\, p)}|F(\chi)|^2 \tag{6.3}$$
$$= \sum_{n=T+1}^{R}\frac{S(n)-S(n-1)}{n}$$
$$= \sum_{n=T+1}^{R} S(n)\left(\frac{1}{n}-\frac{1}{n+1}\right)-\frac{S(T)}{T+1}+\frac{S(R)}{R+1}$$
$$\le \sum_{n=T+1}^{R} 6N(A)\left(\frac{1}{n}-\frac{1}{n+1}\right)+\frac{6N|A|}{R+1}=\frac{6N|A|}{T+1},$$

and similarly,

$$\sum_{T<p\le R}\frac{1}{\varphi(p)}\sum_{\chi\ne\chi_0\ (\mathrm{mod}\, p)}|G(\chi)|^2\le\frac{6N|B|}{T+1}. \tag{6.4}$$

It follows from (6.1)–(6.4) that

$$\left|\frac{1}{|A|\cdot|B|}\sum_{T<p}\sum_{a\in A,\, b\in B,\, p\mid ab+1}1-(\log\log R-\log\log 3T)\right|$$
$$< c_3\left(1+\frac{N}{T}\left(\frac{1}{|A|}+\frac{1}{|B|}\right)\right),$$

whence the result follows.

References

[1] E. R. Canfield, P. Erdős and C. Pomerance, *On a problem of Oppenheim concerning "Factorisatio Numerorum"*, J. Number Theory 17 (1983), 1–28.
[2] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Graduate Texts in Math. 74, Springer, 1980.
[3] P. Erdős, C. Pomerance, A. Sárközy and C. L. Stewart, *On elements of sumsets with many prime factors*, J. Number Theory 44 (1993), 93–104.
[4] P. Erdős, C. L. Stewart and R. Tijdeman, *Some diophantine equations with many solutions*, Compositio Math. 66 (1988), 37–56.
[5] P. Erdős and P. Turán, *On a problem in the elementary theory of numbers*, Amer. Math. Monthly 41 (1934), 608–611.
[6] J.-H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), 561–584.
[7] —, *The number of solutions of decomposable form equations*, to appear.
[8] J.-H. Evertse and K. Győry, *Finiteness criteria for decomposable form equations*, Acta Arith. 50 (1988), 357–379.
[9] P. X. Gallagher, *The large sieve*, Mathematika 14 (1967), 14–20.

[10] K. Győry, *On the numbers of families of solutions of systems of decomposable form equations*, Publ. Math. Debrecen 42 (1993), 65–101.

[11] —, *Some applications of decomposable form equations to resultant equations*, Colloq. Math. 65 (1993), 267–275.

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

[13] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, 1979.

[14] C. Pomerance, A. Sárközy and C. L. Stewart, *On divisors of sums of integers III*, Pacific J. Math. 133 (1988), 363–379.

[15] A. Sárközy, *Hybrid problems in number theory*, in: Number Theory, New York 1985–88, Lecture Notes in Math. 1383, Springer, 1989, 146–169.

[16] —, *On sums* $a+b$ *and numbers of the form* $ab+1$ *with many prime factors*, Grazer Math. Ber. 318 (1992), 141–154.

[17] A. Sárközy and C. L. Stewart, *On divisors of sums of integers V*, Pacific J. Math. 166 (1994), 373–384.

[18] —, —, *On prime factors of integers of the form* $ab+1$, to appear.

[19] H. P. Schlickewei, *S-unit equations over number fields*, Invent. Math. 102 (1990), 95–107.

[20] —, *The quantitative Subspace Theorem for number fields*, Compositio Math. 82 (1992), 245–273.

[21] W. M. Schmidt, *The subspace theorem in diophantine approximations*, ibid. 69 (1989), 121–173.

[22] C. L. Stewart, *Some remarks on prime divisors of sums of integers*, in: Séminaire de Théorie des Nombres, Paris, 1984–85, Progr. Math. 63, Birkhäuser, 1986, 217–223.

[23] C. L. Stewart and R. Tijdeman, *On prime factors of sums of integers II*, in: Diophantine Analysis, J. H. Loxton and A. J. van der Poorten (eds.), Cambridge University Press, 1986, 83–98.

Mathematical Institute
Kossuth Lajos University
4010 Debrecen, Hungary

Mathematical Institute
Hungarian Academy of Sciences
H-1053 Budapest, Hungary

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1

Received on 10.7.1995
and in revised form on 7.9.1995 (2820)