

**On prime factors of integers of  
the form  $(ab + 1)(bc + 1)(ca + 1)$**

by

K. GYÖRY (Debrecen) and A. SÁRKÖZY (Budapest)

*To Professor J. W. S. Cassels on his 75th birthday*

**1. Introduction.** For any integer  $n > 1$  let  $P(n)$  denote the greatest prime factor of  $n$ . Győry, Sárközy and Stewart [5] conjectured that if  $a$ ,  $b$  and  $c$  are pairwise distinct positive integers then

$$(1) \quad P((ab + 1)(bc + 1)(ca + 1))$$

tends to infinity as  $\max(a, b, c) \rightarrow \infty$ . In this paper we confirm this conjecture in the special case when at least one of the numbers  $a$ ,  $b$ ,  $c$ ,  $a/b$ ,  $b/c$ ,  $c/a$  has bounded prime factors. We prove our result in a quantitative form by showing that if  $\mathcal{A}$  is a finite set of triples  $(a, b, c)$  of positive integers  $a$ ,  $b$ ,  $c$  with the property mentioned above then for some  $(a, b, c) \in \mathcal{A}$ , (1) is greater than a constant times  $\log |\mathcal{A}| \log \log |\mathcal{A}|$ , where  $|\mathcal{A}|$  denotes the cardinality of  $\mathcal{A}$  (cf. Corollary to Theorem 1). Further, we show that this bound cannot be replaced by  $|\mathcal{A}|^\varepsilon$  (cf. Theorem 2).

Recently, Stewart and Tijdeman [9] proved the conjecture in another special case. Namely, they showed that if  $a \geq b > c$  then (1) exceeds a constant times  $\log((\log a)/\log(c + 1))$ . In the present paper we give an estimate from the opposite side in terms of  $a$  (cf. Theorem 3).

**2. Lower bounds.** For any integer  $n > 1$  let  $\omega(n)$  denote the number of distinct prime factors of  $n$ . Let  $p_1, \dots, p_s$  be distinct primes, and let  $S$  denote the set of positive rational numbers whose prime decompositions do not contain any prime factor different from  $p_1, \dots, p_s$ .

---

The research of the first author was partially supported by the Hungarian Academy of Sciences and by the Hungarian National Foundation for Scientific Research, Grants No. 16975 and 16791.

The research of the second author was partially supported by the Hungarian National Foundation for Scientific Research, Grant No. 17433.

**THEOREM 1.** *Let  $\mathcal{A}$  be a finite set of triples  $(a, b, c)$  of pairwise distinct positive integers  $a, b, c$ . Suppose that for all  $(a, b, c) \in \mathcal{A}$ , at least one of the numbers  $a, b, c, a/b, b/c$  and  $c/a$  is contained in  $S$ . Then there exists an effectively computable positive absolute constant  $c_1$  such that*

$$(2) \quad \omega\left(\prod_{(a,b,c) \in \mathcal{A}} (ab+1)(bc+1)(ca+1)\right) > c_1 \log |\mathcal{A}| - s.$$

Obviously, the lower bound in (2) can be replaced by  $(c_1/2) \log |\mathcal{A}|$  provided that  $\log |\mathcal{A}| \geq 2s/c_1$ .

By the prime number theorem (or more precisely, by the fact that the  $n$ th prime exceeds  $n \log n$ ; see [7]) this implies the following.

**COROLLARY.** *Under the assumptions of Theorem 1, there exists a triple  $(a, b, c)$  in  $\mathcal{A}$  for which*

$$(3) \quad P((ab+1)(bc+1)(ca+1)) > c_2 \log |\mathcal{A}| \log \log |\mathcal{A}|$$

*provided that  $\log |\mathcal{A}| > s/c_2^2$ , where  $c_2$  is an effectively computable positive absolute constant.*

In the particular case when, for all  $(a, b, c) \in \mathcal{A}$ , at least one of the numbers  $a, b, c, a/b, b/c, c/a$  is contained in  $S$ , our Corollary confirms the above-mentioned conjecture.

We note that for positive integers  $a, b, c$  with  $a = b > c$ , (1) is at least  $P(a^2 + 1)$  which can be estimated from below by  $\log \log a$  (see e.g. [8]). Hence, for such integers  $a, b, c$  the conjecture also holds. On the other hand, the conjecture is not true for positive integers  $a, b, c$  with  $a > b = c$  as is shown by the example  $a = 2^m - 1, b = c = 1$ , where  $m \in \mathbb{N}$ .

Both the Corollary above and the result of Stewart and Tijdeman [9] support the following.

**CONJECTURE.** *Let  $\mathcal{A}$  be a finite set of triples  $(a, b, c)$  of pairwise distinct positive integers  $a, b, c$ . Then there exists  $(a, b, c)$  in  $\mathcal{A}$  for which (3) holds, provided that  $|\mathcal{A}| > 2$ , where  $c_2$  is an effectively computable positive absolute constant.*

In the proof of Theorem 1, we shall reduce the assertion to be proved to appropriate  $T$ -unit equations in at most 5 unknowns. Several cases will be distinguished and then a recent bound of Evertse [4] will be used on the number of solutions of  $T$ -unit equations. The constants  $c_1$  and  $c_2$  in Theorem 1 and in its Corollary can be made explicit from our proof.

**3. Upper bounds.** We shall show that the right hand side of (3) cannot be replaced by  $|\mathcal{A}|^\varepsilon$ .

**THEOREM 2.** *For all  $\varepsilon > 0$  there exist infinitely many finite sets  $\mathcal{A}$  of triples  $(a, b, c)$  of positive integers  $a, b, c$  with  $b = 2, c = 1$  such that for all*

$(a, b, c) \in \mathcal{A}$  we have

$$P((ab+1)(bc+1)(ca+1)) < |\mathcal{A}|^\varepsilon.$$

One might like to see how small one can make  $P((ab+1)(bc+1)(ca+1))$  in terms of  $\max(a, b, c)$ . The proof of Theorem 2 gives the existence of triples  $(a, b, c)$  with

$$P((ab+1)(bc+1)(ca+1)) < (\max(a, b, c))^\varepsilon$$

for any fixed  $\varepsilon > 0$ . The following theorem improves upon this estimate.

**THEOREM 3.** *There exist infinitely many positive integers  $m$  such that for  $c = 2^m$ ,  $b = c^2$ ,  $a = c^3$ , we have*

$$P((ab+1)(bc+1)(ca+1)) < \exp\left(c_3 \frac{\log a}{\log \log \log a}\right)$$

where  $c_3$  is an effectively computable positive absolute constant.

Note that the triples  $(a, b, c)$  in Theorem 3 have the property that each of the six numbers  $a, b, c, a/b, b/c, c/a$  are contained in the set  $S$  consisting of the powers of 2. This shows that the greatest prime factor of  $(ab+1)(bc+1)(ca+1)$  can be made small (in terms of  $\max(a, b, c)$ ) even for triples  $(a, b, c)$  of the type studied in Theorem 1 and the Corollary. Note, moreover, that in the construction given in Theorem 3 each of  $a, b$  and  $c$  is large and, indeed,

$$\log \min(a, b, c) \gg \log \max(a, b, c),$$

while in Theorem 2,  $b$  and  $c$  are bounded. Finally, we remark that the proofs of Theorems 2 and 3 can be extended to the case when we study  $k$ -tuples  $(a_1, \dots, a_k)$  instead of triples  $(a, b, c)$  and we want  $\max_{1 \leq i < j \leq k} P(a_i a_j + 1)$  to be small.

It is likely that our lower bounds obtained for (1) are much closer to the truth than our upper bounds. In [2] and [5], better upper bounds have been derived for the greatest prime factors of  $\prod_{b \in B, b' \in B'} (b + b')$  and  $\prod_{b \in B, b' \in B'} (bb' + 1)$  respectively, where  $B, B'$  are appropriate finite subsets of  $\mathbb{N}$ . However, the constructions given in [2] and [5] cannot be adapted to our situation because in the present paper we deal with the elements of a single set  $\mathcal{A}$  only, and not of two sets as in [2] and [5].

While in Theorems 2 and 3 we gave non-trivial upper bounds for (1), we have not been able to give a non-trivial upper bound for the left hand side of (2). Indeed, let  $n$  be a large but fixed integer, and let  $\mathcal{A}$  denote the set of triples  $(a, b, c)$  of positive integers with  $n \geq a > b > c$  so that  $|\mathcal{A}| = \binom{n}{3}$ . Then clearly the left hand side of (2) is

$$\leq \pi(n^2) = \left(\frac{1}{2} + o(1)\right) \frac{n^2}{\log n} = (c_4 + o(1)) \frac{|\mathcal{A}|^{2/3}}{\log |\mathcal{A}|},$$

and we have not been able to settle the following

PROBLEM. Are there infinitely many finite sets  $\mathcal{A}$  of triples  $(a, b, c)$  of distinct positive integers  $a, b, c$  such that, as  $|\mathcal{A}| \rightarrow \infty$ , we have

$$\omega\left(\prod_{(a,b,c) \in \mathcal{A}} (ab+1)(bc+1)(ca+1)\right) = o\left(\frac{|\mathcal{A}|^{2/3}}{\log |\mathcal{A}|}\right)?$$

**4. Proof of Theorem 1.** Let  $q_1, \dots, q_t$  be distinct primes, and denote by  $T$  the set of non-zero rational numbers whose prime decompositions do not contain any prime different from  $q_1, \dots, q_t$ . Then  $T$  is a multiplicative group. It is in fact the unit group of the ring  $\mathbb{Z}[(q_1 \dots q_t)^{-1}]$ .

The following lemma is a special case of Theorem 3 of [4] on unit equations.

LEMMA 1 (Evertse [4]). Let  $a_1, \dots, a_n$  be non-zero rational numbers. Then the equation

$$(4) \quad a_1 u_1 + \dots + a_n u_n = 1$$

in  $u_1, \dots, u_n \in T$  with  $\sum_{i \in I} a_i u_i \neq 0$  for each non-empty  $I \subseteq \{1, \dots, n\}$  has at most  $(2^{35} n^2)^{n^3(t+1)}$  solutions.

Proof of Theorem 1. In what follows,  $c_5, c_6, \dots, c_{15}$  denote effectively computable positive absolute constants.

Denote by  $\mathcal{A}_1$  the subset of  $\mathcal{A}$  consisting of those triples  $(a, b, c)$  in  $\mathcal{A}$  for which  $a/b$ ,  $b/c$  or  $c/a$  is contained in  $S$ . We may consider without loss of generality those  $(a, b, c) \in \mathcal{A}_1$  for which  $c/a \in S$ . Let  $r_1, \dots, r_q$  denote the distinct prime factors of

$$\prod_{\substack{(a,b,c) \in \mathcal{A}_1 \\ c/a \in S}} ((ab+1)(bc+1)(ca+1)).$$

Denote by  $T$  the set of non-zero rational numbers whose prime decompositions do not contain any prime different from  $p_1, \dots, p_s$  and  $r_1, \dots, r_q$ . Then  $T$  is a multiplicative group generated by at most  $s+q$  distinct primes. Let  $(a, b, c)$  be an arbitrary triple in  $\mathcal{A}_1$  with  $c/a \in S$ , and put

$$(5) \quad ab+1 = e_1, \quad bc+1 = e_2, \quad ca+1 = e_3.$$

Then  $e_1, e_2$  and  $e_3$  are clearly pairwise distinct and greater than 1. Further,  $a, b$  and  $c$  are uniquely determined by  $e_1, e_2$  and  $e_3$ .

Put  $\lambda = c/a$ . Then it follows from (5) that

$$\frac{e_2 - 1}{e_1 - 1} = \frac{bc}{ab} = \lambda,$$

whence

$$(6) \quad e_2 - \lambda e_1 + \lambda = 1, \quad \text{where } e_2, \lambda e_1, \lambda \in T.$$

This is a  $T$ -unit equation in  $(e_2, \lambda e_1, \lambda)$ . If  $e_2 - \lambda e_1 = 0$  then  $\lambda = 1$ , i.e.  $a = c$ , which is not possible. If  $-\lambda e_1 + \lambda = 0$  then  $e_1 = 1$ , which is also impossible. Hence there is no vanishing subsum on the left hand side of (6). Thus, by Lemma 1, the number of  $(e_2, \lambda e_1, \lambda)$  is at most  $c_5^{s+q+1}$ .

We can write  $a = a'd$ ,  $c = c'd$  where  $a'$ ,  $c'$ ,  $d$  are positive integers with  $(a', c') = 1$ . The numbers  $a'$  and  $c'$  are uniquely determined by  $e_2$ ,  $\lambda e_1$  and  $\lambda$ . Then, by (5),  $e_3 = ca + 1 = (c'a')d^2 + 1$ , i.e.  $d$  is a solution of the diophantine equation

$$(7) \quad (c'a')x^2 + 1 \in T \quad \text{in } x \in \mathbb{Z}.$$

By Theorem 2 of [3], the number of solutions  $d$  of (7) is at most  $c_6^{s+q+1}$ . It is easy to see that  $e_1$ ,  $e_2$ ,  $e_3$  and hence  $a$ ,  $b$ ,  $c$  are uniquely determined by  $e_2$ ,  $\lambda e_1$ ,  $\lambda$  and  $d$ . Thus the number of triples  $(a, b, c)$  in  $\mathcal{A}_1$  with  $c/a \in S$  is at most  $(c_5 c_6)^{s+q+1}$ , whence the cardinality  $|\mathcal{A}_1|$  of  $\mathcal{A}_1$  satisfies

$$(8) \quad |\mathcal{A}_1| \leq c_7^{s+q+1}.$$

Denote now by  $\mathcal{A}_2$  the subset of  $\mathcal{A}$  consisting of those triples  $(a, b, c)$  for which  $a$ ,  $b$  or  $c$  is contained in  $S$ . We may consider without loss of generality those  $(a, b, c) \in \mathcal{A}_2$  for which  $c \in S$ . Let now  $r_1, \dots, r_q$  denote the distinct prime factors of the product

$$\prod_{\substack{(a,b,c) \in \mathcal{A}_2 \\ c \in S}} ((ab + 1)(bc + 1)(ca + 1)),$$

and let  $T$  be as above. Let  $(a, b, c)$  be an arbitrary triple in  $\mathcal{A}_2$  with  $c \in S$ , and let  $e_1$ ,  $e_2$ ,  $e_3$  be defined as in (5). Then it follows from (5) that

$$(e_2 - 1)(e_3 - 1) = (bc)(ca) = c^2(ab) = c^2(e_1 - 1),$$

whence

$$(9) \quad c^2 e_1 - e_2 e_3 + e_2 + e_3 - c^2 = 1.$$

This is a  $T$ -unit equation in  $(c^2 e_1, e_2 e_3, e_2, e_3, c^2)$ . It is easily seen that distinct triples  $(a, b, c)$  in  $\mathcal{A}_2$  with  $c \in S$  yield distinct solutions of (9). To apply our Lemma 1 to equation (9), we have to distinguish several cases.

First assume that there is no vanishing subsum on the left hand side of (9). Then, by Lemma 1, the number of solutions of (9) is bounded above by  $c_8^{s+q+1}$ . Hence, in this case the number of  $(a, b, c)$  under consideration is at most  $c_8^{s+q+1}$ .

Next we assume that there is a vanishing subsum, denoted by  $\Sigma$ , on the left hand side of (9). After omitting this vanishing subsum  $\Sigma$ , consider the remaining equation in (9). Since  $\Sigma$  has at least two terms, there are at most three terms on the left hand side of the remaining equation. We distinguish some subcases according to the number of terms on the left hand side of the remaining equation.

If there is only one term in the remaining equation, then it must be positive, i.e. it can be only  $c^2e_1$ ,  $e_2$  or  $e_3$ . But this contradicts the fact that  $e_1, e_2, e_3$  are all greater than 1.

If there are two terms in the remaining equation, then we have  $\binom{5}{2} = 10$  possibilities. In each case, the remaining equation is a  $T$ -unit equation in 2 unknowns, and up to a  $T$ -unit factor,  $\Sigma$  is another unit equation in 2 unknowns. By our Lemma 1, the first equation has at most  $c_9^{s+q+1}$  solutions, and the same holds for the number of solutions of the second equation up to a  $T$ -unit factor.

First consider the cases when, in (9),  $\Sigma$  contains both  $c^2e_1$  and  $e_2e_3$ .

(a<sub>1</sub>)  $\Sigma$  cannot be  $c^2e_1 - e_2e_3 - c^2 = 0$  since  $e_2 + e_3 = 1$  cannot hold because of  $e_2, e_3 > 1$ .

(a<sub>2</sub>) If  $\Sigma : c^2e_1 - e_2e_3 + e_3 = 0$  and  $e_2 - c^2 = 1$  then for  $\varrho := e_1/e_3$  we get  $c^2\varrho - e_2 + 1 = 0$ . Then it follows that  $\varrho = 1$ , i.e.  $e_1 = e_3$ , which is impossible.

(a<sub>3</sub>) If  $\Sigma : c^2e_1 - e_2e_3 + e_2 = 0$  and  $e_3 - c^2 = 1$  then interchanging  $e_2$  and  $e_3$  we get the previous case, which is not possible.

Consider now the cases when  $\Sigma$  contains  $c^2e_1$  but does not contain  $e_2e_3$ . Then we have again three cases to be distinguished.

(a<sub>4</sub>) The case  $\Sigma : c^2e_1 + e_2 + e_3 = 0$ ,  $-e_2e_3 - c^2 = 1$  cannot hold since  $e_1, e_2, e_3$  and  $c$  are positive.

(a<sub>5</sub>) If  $\Sigma : c^2e_1 + e_2 - c^2 = 0$  and  $-e_2e_3 + e_3 = 1$  then, by Lemma 1, the number of  $(e_2e_3, e_3, e_1, e_2/c^2)$  is at most  $c_{10}^{2(s+q+1)}$ . Then the number of  $(a, b, c)$  in  $\mathcal{A}_2$  under consideration is at most  $c_{10}^{2(s+q+1)}$ .

(a<sub>6</sub>) If  $\Sigma : c^2e_1 + e_3 - c^2 = 0$  and  $-e_2e_3 + e_2 = 1$  then we get the previous case by interchanging  $e_2$  and  $e_3$ .

Next consider the cases when  $\Sigma$  contains  $-e_2e_3$ , but does not contain  $c^2e_1$ . Then there are again three possibilities.

(a<sub>7</sub>) The case  $\Sigma : -e_2e_3 + e_2 - c^2 = 0$ ,  $c^2e_1 + e_3 = 1$  cannot hold because  $c^2e_1, e_3 > 1$ .

(a<sub>8</sub>) Similarly,  $\Sigma : -e_2e_3 + e_3 - c^2 = 0$ ,  $c^2e_1 + e_2 = 1$  cannot hold.

(a<sub>9</sub>) If  $\Sigma : -e_2e_3 + e_2 + e_3 = 0$  and  $c^2e_1 - c^2 = 1$  then  $c^2(e_1 - 1) = 1$  whence  $c = 1$  and  $e_1 = 2$ . But this implies that  $ab = 1$ , which is impossible.

(a<sub>10</sub>) Finally, there remains the case when  $\Sigma$  does not contain  $c^2e_1$  and  $e_2e_3$ . In this case we have  $\Sigma : e_2 + e_3 - c^2 = 0$  and  $c^2e_1 - e_2e_3 = 1$ . Then the number of  $(c^2e_1, e_2e_3, e_3/e_2, c^2/e_2)$  is at most  $c_{10}^{2(s+q+1)}$ . For fixed values of the coordinates it follows that  $e_2e_3(e_3/e_2) = e_3^2$  and hence  $e_3, e_2, c$  and  $e_1$  are uniquely determined. Thus the number of  $(a, b, c)$  in  $\mathcal{A}_2$  under consideration is at most  $c_{10}^{2(s+q+1)}$ .

Consider now the cases when there are three terms in the remaining equation. This equation cannot have vanishing subsums because otherwise one of the positive terms on the left hand side of (9) would be equal to 1, which is impossible. Further, in  $\Sigma$  there must exist one positive and one negative term. Hence we have to distinguish  $3 \cdot 2 = 6$  subcases.

(b<sub>1</sub>) If  $\Sigma : c^2e_1 - e_2e_3 = 0$  and  $e_2 + e_3 - c^2 = 1$  then, by Lemma 1, the number of  $(e_2, e_3, c^2, c^2e_1/(e_2e_3))$  is at most  $c_{11}^{s+q+1}$ . But for fixed values of the coordinates,  $e_1$  and hence  $a, b, c$  are uniquely determined. Thus, in this case the number of  $(a, b, c)$  in  $\mathcal{A}_2$  under consideration is at most  $c_{11}^{s+q+1}$ .

(b<sub>2</sub>) If  $\Sigma : c^2e_1 - c^2 = 0, -e_2e_3 + e_2 + e_3 = 1$  then  $e_1 = 1$ , which is impossible.

(b<sub>3</sub>) If  $\Sigma : -e_2e_3 + e_2 = 0$  and  $c^2e_1 + e_3 - c^2 = 1$  then  $e_3 = 1$ , which is not possible.

(b<sub>4</sub>) If  $\Sigma : -e_2e_3 + e_3 = 0$  and  $c^2e_1 + e_2 - c^2 = 1$  then  $e_2 = 1$ , which is impossible.

(b<sub>5</sub>) If  $\Sigma : e_2 - c^2 = 0$  and  $c^2e_1 - e_2e_3 + e_3 = 1$  then the number of  $(c^2e_1, e_2e_3, e_3, c^2/e_2)$  is at most  $c_{12}^{s+q+1}$ . However, for fixed values of the coordinates,  $e_2$  and hence  $c$  and  $e_1$  are uniquely determined. Hence the number of  $(a, b, c) \in \mathcal{A}_2$  under consideration is at most  $c_{12}^{s+q+1}$ .

(b<sub>6</sub>) If  $\Sigma : e_3 - c^2 = 0$  and  $c^2e_1 - e_2e_3 + e_2 = 1$  then interchanging  $e_2$  and  $e_3$  we arrive at the previous case.

The left hand side of the remaining equation cannot have more than three terms, hence all possibilities have been taken into account. Finally, we infer that the total number of  $(a, b, c)$  in  $\mathcal{A}_2$  is at most  $c_{13}^{s+q+1}$ . In other words,

$$(10) \quad |\mathcal{A}_2| < c_{13}^{s+q+1}.$$

It follows from (8) and (10) that

$$|\mathcal{A}| < c_{14}^{s+q},$$

whence

$$q > c_{15} \log |\mathcal{A}| - s.$$

This completes the proof of Theorem 1. ■

**5. Proofs of Theorems 2 and 3.** Theorem 2 will follow easily from the following lemma.

LEMMA 2. *For all  $\varepsilon > 0$  there are numbers  $\delta = \delta(\varepsilon)$  and  $n_0 = n_0(\varepsilon)$  such that if  $n \geq n_0$ , then there are more than  $\delta n$  integers  $m$  with the properties that  $1 \leq m \leq n$  and*

$$(11) \quad P(m(2m-1)) \leq m^\varepsilon.$$

Proof. This is a special case of a result of Balog and Ruzsa ([1], Corollary 2) which generalizes a theorem of Hildebrand [6].

Proof of Theorem 2. We apply Lemma 2 with  $\varepsilon/2$  in place of  $\varepsilon$ , and for some  $n > n_0(\varepsilon/2)$ , we consider all the numbers  $m$  satisfying the conditions in Lemma 2, and let  $\mathcal{M}$  denote the set of those integers  $m$ . Let  $\mathcal{A}$  denote the set of triples  $(a, b, c)$  for which  $a = m - 1$ ,  $b = 2$ ,  $c = 1$  with  $m > 3$  and  $m \in \mathcal{M}$ . Then for sufficiently large  $n$  we have

$$(12) \quad |\mathcal{A}| = |\{m : m \in \mathcal{M}, m > 3\}| \geq |\mathcal{M}| - 3 > \delta n - 3 > \delta n/2,$$

and it follows from (11) (with  $\varepsilon/2$  in place of  $\varepsilon$ ) and (12) that for all  $(a, b, c) = (m - 1, 2, 1) \in \mathcal{A}$  we have

$$(13) \quad P((ab + 1)(bc + 1)(ca + 1)) = P((2m - 1) \cdot 3 \cdot m) \leq m^{\varepsilon/2} \leq n^{\varepsilon/2}$$

for  $n$  large enough. It follows from (12) and (13) that

$$P((ab + 1)(bc + 1)(ca + 1)) < |\mathcal{A}|^\varepsilon$$

for  $n > n_1(\varepsilon)$  and this completes the proof of Theorem 2. ■

Proof of Theorem 3. For  $k = 2, 3, \dots$ , write  $Q_k = \prod_{p \leq k} p$  so that by the prime number theorem we have

$$(14) \quad \log Q_k = (1 + o(1))k \quad \text{as } k \rightarrow \infty.$$

Assume that  $k \geq 10$ , and let  $c = 2^{Q_k}$ ,  $b = c^2$ ,  $a = c^3$ . Then each of the numbers  $ab + 1$ ,  $bc + 1$ ,  $ca + 1$  is of the form  $c^j + 1 = 2^{jQ_k} + 1$  with  $j = 3, 4$  or  $5$ , and this number divides  $(2^{jQ_k} + 1)(2^{jQ_k} - 1) = 2^{2jQ_k} - 1$ . As is known,

$$2^{2jQ_k} - 1 = \prod_{d|2jQ_k} \Phi_d(2)$$

where  $\Phi_d(x)$  denotes the  $d$ th cyclotomic polynomial. Hence

$$P(2^{2jQ_k} - 1) = \max_{d|2jQ_k} P(\Phi_d(2)) \leq \max_{d|2jQ_k} \Phi_d(2).$$

However, we have

$$\Phi_d(2) = \prod_{\substack{1 \leq j \leq d \\ (j, d) = 1}} |2 - e^{2\pi i j/d}| \leq 3^{\varphi(d)} \leq 3^{\varphi(2jQ_k)}$$

where  $\varphi(\cdot)$  is Euler's function. Thus it follows that

$$(15) \quad P((ab + 1)(bc + 1)(ca + 1)) \leq \max_{j=3,4,5} P(2^{2jQ_k} - 1) < \max_{j=3,4,5} 3^{\varphi(2jQ_k)}.$$



Since  $j \leq 5$  and  $k \geq 10$ , by Mertens' formula and (14) we have

$$\begin{aligned}\varphi(2jQ_k) &= 2jQ_k \prod_{p|2jQ_k} \left(1 - \frac{1}{p}\right) = 2jQ_k \prod_{p|Q_k} \left(1 - \frac{1}{p}\right) \\ &= 2jQ_k \prod_{p \leq k} \left(1 - \frac{1}{p}\right) < c_{16} \frac{Q_k}{\log k} < c_{17} \frac{Q_k}{\log \log Q_k}.\end{aligned}$$

Here  $c_{16}$ ,  $c_{17}$  and  $c_{18}$ ,  $c_{19}$  below, are effectively computable positive absolute constants. It follows that for  $3 \leq j \leq 5$  we have

$$\begin{aligned}(16) \quad 2^{\varphi(2jQ_k)} &= \exp((\log 2)\varphi(2jQ_k)) = \exp\left(c_{18} \frac{Q_k}{\log \log Q_k}\right) \\ &< \exp\left(c_{19} \frac{\log c^3}{\log \log \log c^3}\right) = \exp\left(c_{19} \frac{\log a}{\log \log \log a}\right).\end{aligned}$$

The result follows from (15) and (16) and this completes the proof of Theorem 3. ■

### References

- [1] A. Balog and I. Z. Ruzsa, *On an additive property of stable sets*, in: Proc. Cardiff Number Theory Conf., 1995, to appear.
- [2] P. Erdős, C. L. Stewart and R. Tijdeman, *Some diophantine equations with many solutions*, Compositio Math. 66 (1988), 37–56.
- [3] J. H. Evertse, *On equations in  $S$ -units and the Thue–Mahler equation*, Invent. Math. 75 (1984), 561–584.
- [4] —, *The number of solutions of decomposable form equations*, ibid. 122 (1995), 559–601.
- [5] K. Györy, 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.
- [6] A. Hildebrand, *On a conjecture of Balog*, Proc. Amer. Math. Soc. 95 (1985), 517–523.
- [7] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
- [8] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, 1986.
- [9] C. L. Stewart and R. Tijdeman, *On the greatest prime factor of  $(ab + 1)(ac + 1)(bc + 1)$* , this volume, 93–101.

Institute of Mathematics  
Kossuth Lajos University  
4010 Debrecen, Hungary  
E-mail: gyory@math.klte.hu

Mathematical Institute  
Hungarian Academy of Sciences  
1053 Budapest, Hungary  
E-mail: sarkozy@cs.elte.hu

Received on 6.9.1996

(3043)