ACTA ARITHMETICA
114.3 (2004)

A quantitative lower bound for the greatest prime factor of $(ab+1)(bc+1)(ca+1)$

by

Yann Bugeaud (Strasbourg) and Florian Luca (Morelia)

À Wolfgang Schmidt, pour son soixante-dixième anniversaire

1. Introduction. For any integer $n \geq 2$, we denote by $P(n)$ the greatest prime factor of n. Győry, Sárközy & Stewart [8] conjectured that if $a > b > c$ are positive integers, then

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

as a tends to infinity. Partial results have been obtained by Győry & Sárközy [7], Stewart & Tijdeman [11] and Bugeaud [3]. Very recently, Corvaja & Zannier [4] and, independently and simultaneously, Hernández & Luca [9] applied the Schmidt Subspace Theorem to give a positive answer to the above-mentioned conjecture. Actually, a stronger result is proved in [4], namely that the greatest prime factor of $(ab+1)(ac+1)$ tends to infinity as the maximum of the pairwise distinct positive integers a, b and c goes to infinity.

There are two natural extensions of such a result. First, one can search for an effective lower bound for $P((ab+1)(bc+1)(ca+1))$ in terms of $\max\{a,b,c\}$. This has been achieved, under additional assumptions on a, b and c, in [11] and in [3]. Second, given a finite set $\mathcal{A}$ of triples (a,b,c), one can aim at establishing a lower bound for $P(\prod(ab+1)(bc+1)(ca+1))$, where the product is taken over all the triples in $\mathcal{A}$, in terms of the cardinality of $\mathcal{A}$. This question has been considered in [7], where some partial results were obtained, which have motivated the following conjecture. Throughout the present paper, we denote by $|\mathcal{S}|$ the cardinality of a finite set $\mathcal{S}$.

Conjecture (Győry and Sárközy). *Let $\mathcal{A}$ be a finite set of cardinality at least two of triples (a,b,c) of pairwise distinct integers. Then there exists*

2000 *Mathematics Subject Classification*: 11N32, 11D57.

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

$$P((ab+1)(bc+1)(ca+1)) > \kappa \log|\mathcal{A}| \log\log|\mathcal{A}|,$$

where κ is an effectively computable positive absolute constant.

In the present work, we show that the conjecture of Győry & Sárközy holds true with $\kappa = 10^{-7}$, without any additional assumption on the set $\mathcal{A}$. Our main results are stated in Section 2. Section 4 is devoted to their proofs, which depend on a quantitative version of the Schmidt Subspace Theorem, due to Evertse, and recalled in Section 3. Some related questions are discussed in Section 5.

2. Statements of the main results. For any integer $n \geq 2$ we write $\omega(n)$ for the number of distinct prime factors of n. As in [7], we first establish a lower bound for the number of distinct prime factors of $\prod(ab+1)(ac+1)(bc+1)$, where the product is taken over a finite set of triples of distinct integers.

THEOREM 1. *For any finite set $\mathcal{A}$ of cardinality at least two of triples of positive integers (a,b,c) with $a>b>c$, we have*

$$\omega\Big(\prod_{(a,b,c)\in\mathcal{A}} (ab+1)(ac+1)(bc+1)\Big) > 10^{-6}\log|\mathcal{A}|. \tag{1}$$

By the Prime Number Theorem, Theorem 1 enables us to confirm the conjecture of Győry & Sárközy, even with an explicit value for the constant κ.

COROLLARY 1. *Let $\mathcal{A}$ be a finite set of cardinality at least two of triples of positive integers (a,b,c) with $a>b>c$. There exists a triple (a,b,c) in $\mathcal{A}$ such that*

$$P((ab+1)(ac+1)(bc+1)) > 10^{-7}\log|\mathcal{A}|\log\log|\mathcal{A}|. \tag{2}$$

The proof of Theorem 1 requires five steps and is not a mere combination of the arguments of [4] with an effective version of the Subspace Theorem. We can summarize the argument as follows. Let (a,b,c) be a triple of positive integers with $a>b>c$ and set $u := ab+1$ and $v := ac+1$. First, we exactly follow [4] to prove that u and v satisfy linear equations of the type

$$\gamma_1 \frac{u-1}{v-1} + \gamma_2 \frac{u^2-1}{v-1} + \sum_{\substack{0\leq j\leq 2\\ 1\leq n\leq 5}} \delta_{jn} u^j v^{5-n} = 0,$$

where γ_1, γ_2 and the δ_{jn}'s are rational numbers, not all zero. We apply Evertse's quantitative result to bound the number of these equations in terms of the number of distinct prime factors of uv. We would then like to prove that each of these equations can be satisfied only by finitely many pairs (u, v), but this is by no means obvious since we cannot exclude the presence of equations like $t_1 + t_2uv + t_3(uv)^2$, for which we have no control on the size of t_1, t_2 and t_3. Using Evertse's bound, we have an upper estimate for the number of projective solutions. To see that to each projective solution corresponds a controlled number of pairs (u, v), we apply the Subspace Theorem once again (Step 4 of the proof). We then get an explicit upper bound for the number of pairs (u, v). However, this is not sufficient to deduce an upper estimate for the number of triples (a, b, c), since $u - 1$ and $v - 1$ can have a very large greatest common divisor which is divisible by many small primes (see Section 5 of the paper). To conclude, we use the fact that $bc+1$ is also composed of primes from S. Our argument here rests on the existence of primitive divisors for Lucas sequences.

REMARK 1. Győry & Sárközy [7] have proved that, for any positive real number ε, the right hand side of (2) cannot be replaced by $|\mathcal{A}|^{\varepsilon}$. They however think that (2) should be close to the truth.

REMARK 2. By adapting arguments of Győry, Sárközy & Stewart [8], it is likely that one can prove the existence of finite sets $\mathcal{A}$ of triples (a, b, c) with $a > b > c$ such that $P((ab + 1)(ac + 1)) \leq \kappa(\log |\mathcal{A}|)^{10}$ for any triple (a, b, c) in $\mathcal{A}$ and an absolute constant κ.

REMARK 3. Other related quantitative questions are considered in Section 5. In particular, we show that the right hand side of (1) cannot be replaced by $|\mathcal{A}|^{1/2+\varepsilon}$ for some $\varepsilon > 0$.

Throughout this paper, we use $c_1, c_2, \ldots$ for effectively computable positive constants which are absolute. We also use the Vinogradov symbols $\ll$ and $\gg$ as well as the Landau symbols O and o with their regular meaning.

3. Auxiliary results. We start by recalling a particular instance of a quantitative version of the Schmidt Subspace Theorem due to Evertse [6].

Let $M_{\mathbb{Q}}$ be all the places of $\mathbb{Q}$. For $x \in \mathbb{Q}$ and $w \in M_{\mathbb{Q}}$ we put $|x|_w := |x|$ if $w = \infty$ and $|x|_w := p^{-\mathrm{ord}_p(x)}$ if w corresponds to the prime number p. When $x = 0$, we set $\mathrm{ord}_p(x) := \infty$ and $|x|_w := 0$. Then

$$\prod_{w \in M_{\mathbb{Q}}} |x|_w = 1 \quad \text{for all } x \in \mathbb{Q}^*. \tag{3}$$

Let $N \geq 1$ be a positive integer and define the *height* of $\mathbf{x} := (x_1, \ldots, x_N) \in \mathbb{Q}^N$ as follows. For $w \in M_{\mathbb{Q}}$ write

$$|\mathbf{x}|_w := \begin{cases} \Big(\sum_{i=1}^{N} x_i^2\Big)^{1/2} & \text{if } w = \infty, \\ \max\{|x_1|_w, \ldots, |x_N|_w\} & \text{otherwise.} \end{cases} \tag{4}$$

Set

$$\mathcal{H}(\mathbf{x}) := \prod_{w \in M_{\mathbb{Q}}} |\mathbf{x}|_w.$$

For a linear form $L(\mathbf{x}) := \sum_{i=1}^{N} a_i x_i$ with $\mathbf{a} := (a_1, \ldots, a_N) \in \mathbb{Q}^N$, we write $\mathcal{H}(L) := \mathcal{H}(\mathbf{a})$. We now let $N \geq 1$ be a positive integer, S be a finite subset of $M_{\mathbb{Q}}$ of cardinality s containing the infinite place, and for every $w \in S$ we let $L_{1w}, \ldots, L_{Nw}$ be N linearly independent linear forms in N indeterminates with coefficients in $\mathbb{Q}$ satisfying

$$\mathcal{H}(L_{iw}) \leq H \quad \text{for } i = 1, \ldots, N \text{ and } w \in S. \tag{5}$$

Theorem E1. *Let* $0 < \delta < 1$ *and consider the inequality*

$$\prod_{w \in S} \prod_{i=1}^{N} \frac{|L_{iw}(\mathbf{x})|_w}{|\mathbf{x}|_w} < \Big(\prod_{w \in S} |\det(L_{1w}, \ldots, L_{Nw})|_w\Big) \mathcal{H}(\mathbf{x})^{-n-\delta}. \tag{6}$$

(i) *There exist proper linear subspaces* $T_1, \ldots, T_{t_1}$ *of* $\mathbb{Q}^N$ *with*

$$t_1 \leq (2^{60N^2} \delta^{-7N})^s \tag{7}$$

such that every solution $\mathbf{x} \in \mathbb{Q}^N \setminus \{\mathbf{0}\}$ *of* (6) *satisfying* $\mathcal{H}(\mathbf{x}) \geq H$ *belongs to* $T_1 \cup \cdots \cup T_{t_1}$.

(ii) *There exist proper linear subspaces* $T'_1, \ldots, T'_{t_2}$ *of* $\mathbb{Q}^N$ *with*

$$t_2 \leq (150 N^4 \delta^{-1})^{Ns+1} (2 + \log\log 2H) \tag{8}$$

such that every solution $\mathbf{x} \in \mathbb{Q}^N \setminus \{\mathbf{0}\}$ *of* (6) *satisfying* $\mathcal{H}(\mathbf{x}) < H$ *belongs to* $T'_1 \cup \cdots \cup T'_{t_2}$.

We shall apply Theorem E1 to a certain finite subset S of $M_{\mathbb{Q}}$, and certain systems of linear forms L_{iw} with $i = 1, \ldots, N$ and $w \in S$. Moreover, in our case, the points $\mathbf{x}$ for which (6) will hold will be in $(\mathbb{Z}^*)^N$. In particular, $|\mathbf{x}|_w \leq 1$ will hold for all $w \in M_{\mathbb{Q}} \setminus \{\infty\}$, as well as the inequalities

$$1 \leq \mathcal{H}(\mathbf{x}) \leq \prod_{w \in S} |\mathbf{x}|_w \leq N \max\{|x_i| \mid i = 1, \ldots, N\}. \tag{9}$$

Finally, our linear forms will have integer coefficients and will satisfy

$$\det(L_{1w}, \ldots, L_{Nw}) = \pm 1 \quad \text{for all } w \in S. \tag{10}$$

With these conditions, the following statement is a straightforward consequence of Theorem E1 above.

Corollary E1. *Assume that* (10) *is satisfied, that* $0 < \delta < 1$, *and consider the inequality*

$$\prod_{w \in S} \prod_{i=1}^{N} |L_{iw}(\mathbf{x})|_w < N^{-\delta} (\max\{|x_i| \mid i = 1, \ldots, N\})^{-\delta}. \tag{11}$$

Then there exist proper linear subspaces $T_1, \ldots, T_{t_1}$ *of* $\mathbb{Q}^N$ *with*

$$t_1 \le (2^{60N^2}\delta^{-7N})^s \tag{12}$$

such that every solution $\mathbf{x} \in \mathbb{Z}^N \setminus \{\mathbf{0}\}$ *of* (11) *satisfying* $\mathcal{H}(\mathbf{x}) \ge H$ *belongs to* $T_1 \cup \cdots \cup T_{t_1}$.

Recall that an S-*unit* x is a non-zero rational number such that $|x|_w = 1$ for all $w \notin S$. We shall also need the following version of a theorem of Evertse [5] on S-unit equations.

THEOREM E2. *Let* $a_1, \ldots, a_N$ *be non-zero rational numbers. Then the equation*

$$\sum_{i=1}^{N} a_i u_i = 1 \tag{13}$$

in S-*unit unknowns* u_i *for* $i = 1, \ldots, N$ *and such that* $\sum_{i\in I} a_i u_i \ne 0$ *for each non-empty subset* $I \subseteq \{1, \ldots, N\}$ *has at most* $(2^{35}N^2)^{N^3 s}$ *solutions.*

We are now ready to proceed with the proofs of our results.

4. The proofs

Proof of Theorem 1. We may certainly assume that $|\mathcal{A}| > e^{10^6}$, for otherwise (1) is satisfied. Let

$$s := \omega\Big(\prod_{(a,b,c)\in\mathcal{A}} (ab+1)(ac+1)(bc+1)\Big). \tag{14}$$

We need to find an upper bound of $|\mathcal{A}|$ in terms of s. We shall split our argument into several steps.

STEP 1. *The first system of forms.* In this part of the argument, we follow the method from [4].

We write S for the set of places consisting of the infinite place and the valuations corresponding to the primes p dividing $(ab+1)(ac+1)(bc+1)$ for some triple $(a,b,c) \in \mathcal{A}$. We assume that $a > b > c$. Clearly, S contains $s+1$ elements. We write $u := ab+1,\ v := ac+1$, and put

$$y_1 := \frac{u-1}{v-1} = \frac{b}{c}, \qquad y_2 := \frac{u^2-1}{v-1} = \frac{(u+1)b}{c}.$$

Thus, $u > v \ge 4$ are positive integers which are S-units, and y_1 and y_2 are rational numbers with denominator at most c. Write

$$\frac{1}{v-1} = \frac{1}{v(1-v^{-1})} = \sum_{n\ge 1} v^{-n} = \sum_{n=1}^{5} v^{-n} + \sum_{n\ge 6} v^{-n}.$$

Thus,

$$\left|\frac{1}{v-1}-\sum_{n=1}^{5} v^{-n}\right| = \sum_{n\ge 6} v^{-n} = \frac{1}{v^5(v-1)} < 2v^{-6}.$$

On multiplying the above estimate by u^j-1 for $j=1,2$, we obtain

$$\left|y_j+\sum_{n=1}^{5} v^{-n}-\sum_{n=1}^{5} u^j v^{-n}\right| < 2u^j v^{-6}, \qquad j=1,2,$$

which is equivalent to

$$\left|v^5 y_j+\sum_{n=1}^{5} v^{5-n}-\sum_{n=1}^{5} u^j v^{5-n}\right| < 2u^j v^{-1}, \qquad j=1,2. \tag{15}$$

We let $\sigma_1,\ldots,\sigma_{15}$ denote the integers $u^j v^{5-n}$ for $j=0,1,2$ and $n=1,\ldots,5$ in some order. We may then rewrite (15) as

$$\left|v^5 y_j+\sum_{i=1}^{15} \alpha_{ji}\sigma_i\right| < 2u^j v^{-1}, \qquad j=1,2, \tag{16}$$

where $\alpha_{ji}\in\{0,\pm 1\}$. We now let L_{jw} be the linear forms in the 17 variables $Y_1,Y_2,X_1,\ldots,X_{15}$, where $j=1,\ldots,17$ and $w\in S$, defined as follows:

$$L_{j\infty}=Y_j+\sum_{i=1}^{15}\alpha_{ji}X_i, \qquad L_{jw}=Y_j \quad \text{ for } w\neq\infty, \qquad j=1,2,$$

and $L_{jw}=X_{j-2}$ for all $j=3,\ldots,17$ and $w\in S$. It is easy to see that (5) is satisfied with $H=1$, and that (10) holds for our $N=17$, S, L_{iw} with $i=1,\ldots,17$ and $w\in S$. We also define

$$\mathbf{x}=(x_1,\ldots,x_{17})=(cv^5y_1,cv^5y_2,c\sigma_1,\ldots,c\sigma_{15})\in(\mathbb{Z}^*)^{17}.$$

It is clear that the components of $\mathbf{x}$ are non-zero integers. Inequalities (16) yield

$$|L_{jw}(\mathbf{x})|_\infty < 2cu^j v^{-1}, \qquad j=1,2. \tag{17}$$

The argument from [4] now shows that

$$\prod_{w\in S\setminus\{\infty\}} |L_{jw}(\mathbf{x})|_w \le v^{-5} \quad \text{ for } j=1,2, \tag{18}$$

$$\prod_{w\in S} |L_{jw}(\mathbf{x})|_w \le c \qquad \text{ for } j=3,\ldots,17. \tag{19}$$

Multiplying all the above inequalities (17)–(19), we get

$$\prod_{i=1}^{17}\prod_{w\in S} |L_{iw}(\mathbf{x})|_w \le 4c^{17}u^3v^{-12}. \tag{20}$$

Since $u = ab+1 < a^2$ and $v = ac+1 > ac$, we have $c^{17}u^3v^{-12} < c^5a^{-6} < a^{-1}$, while $\max\{|x_i| \mid i = 1,\ldots,17\} < cu^2v^5 < a^{15}$, and so (20) implies that

$$\prod_{i=1}^{17}\prod_{w\in S}|L_{iw}(\mathbf{x})|_w < 4(\max\{|x_i| \mid i=1,\ldots,17\})^{-1/15}. \tag{21}$$

Note that only the fact that $a > \max\{b,c\}$ was used in the above argument, but not the fact that $u > v$.

Step 2. *Quantitative estimates and non-degenerate Newton polygons.* Let $\mathcal{A}_1$ be the set of (a,b,c) in $\mathcal{A}$ such that

$$\max\{|x_i| \mid i=1,\ldots,17\} \le 4^{15\cdot 16}\cdot 17^{15} < e^{400}.$$

For such triples, since $a < u < \max\{|x_i| \mid i=1,\ldots,17\}$, we get $a < e^{400}$, and therefore

$$|\mathcal{A}_1| < e^{1200}.$$

We write $\mathcal{B}_1$ for the set of pairs (u,v) obtained from triples $(a,b,c)\in\mathcal{A}_1$, and therefore $|\mathcal{B}_1| < e^{1200}$.

From now on, we work only with $(a,b,c)\in\mathcal{A}\setminus\mathcal{A}_1$. In this case,

$$\max\{|x_i| \mid i=1,\ldots,17\} > 4^{15\cdot 16}\cdot 17^{15},$$

which implies

$$4(\max\{|x_i| \mid i=1,\ldots,17\})^{-1/15} < 17^{-1/16}(\max\{|x_i| \mid i=1,\ldots,17\})^{-1/16}.$$

From (21), we get

$$\prod_{i=1}^{17}\prod_{w\in S}|L_{iw}(\mathbf{x})|_w < 17^{-1/16}(\max\{|x_i| \mid i=1,\ldots,17\})^{-1/16}, \tag{22}$$

and since $H = 1$ and $\mathcal{H}(\mathbf{x}) \ge 1$, we can apply Corollary E1 with $N = 17$ and $\delta = (16)^{-1}$ to conclude that there exist proper linear subspaces $T_1,\ldots,T_{t_1}$ of $\mathbb{Q}^{17}$ with

$$t_1 < (2^{60\cdot 17^2}\cdot 16^{7\cdot 17})^{s+1} < \exp(12400(s+1)) \tag{23}$$

such that all the solutions of (22) lie in $T_1\cup\cdots\cup T_{t_1}$.

Let T be one of the subspaces T_l for $l = 1,\ldots,t_1$, and assume that $\mathbf{x}\in T$. We then have an equation of the type

$$\gamma_1 y_1 + \gamma_2 y_2 + \sum_{\substack{0\le j\le 2\\ 1\le n\le 5}} \delta_{jn} u^j v^{5-n} = 0,$$

where γ_1,γ_2 and δ_{jn} are rational numbers for $j = 0,1,2$ and $n = 1,\ldots,5$, not all zero. This leads to

$$P_T(u,v) = 0, \tag{24}$$

where

$$(25)\quad P_T(X,Y) := \sum_{(i,j)} \eta_{(i,j)} X^i Y^j = \gamma_1(X-1) + \gamma_2(X^2-1) + (Y-1)\Big(\sum_{\substack{0\le j\le 2\\ 1\le n\le 5}} \delta_{jn} X^j\, Y^{5-n}\Big) \in \mathbb{Q}[X,Y].$$

The fact that $P_T(X,Y)$ is a non-zero polynomial has been justified in [4]. Note that the vertices of the *Newton polygon* of $P_T(X,Y)$ (i.e., the pairs of non-negative integers (i,j) such that the monomial X^iY^j appears in $P_T(X,Y)$) are contained in $\{0 \le i \le 2,\ 0 \le j \le 5\}$, which consists of precisely 18 lattice points.

Each of equations (24) is an S-unit equation whose indeterminates are $M_{(i,j)} := u^i v^j$, where (i,j) is a vertex of the Newton polygon of P_T. For each of these solutions, equation (24) may be non-degenerate or not. If it is degenerate, then there exists a non-empty proper subset $\mathcal{D}$ of the vertices of the Newton polygon of P_T such that $P_{T,\mathcal{D}}(u,v) = 0$ is a non-degenerate S-unit equation, where

$$P_{T,\mathcal{D}} := \sum_{(i,j)\in D} \eta_{(i,j)} X^i Y^j.$$

Note that $\mathcal{D}$ can be chosen in at most 2^{18} ways once T is known. Omitting the dependence on the variable subset $\mathcal{D}$, it follows that up to multiplying the upper bound on t_1 shown at (23) by $2^{18} < \exp(13)$, we may assume that each of equations (24) is non-degenerate. Assume now that the Newton polygon of P_T has exactly $m \le 18$ monomials (note that $m \ge 2$), and let them be $M_\mu := X^{i_\mu} Y^{j_\mu}$ for $\mu = 1,\dots,m$. By Theorem E2, there exist solutions $(u^{(\lambda)}, v^{(\lambda)})$ with λ in a finite set Λ_T of cardinality at most

$$(26)\qquad |\Lambda_T| \le (2^{35}(m-1)^2)^{(m-1)^3(s+1)} \le (2^{35}\cdot 17^2)^{17^3(s+1)} < \exp(150000(s+1)),$$

and such that for any other solution (u,v) of (24) whose components are S-units there exists an S-unit ζ and $\lambda \in \Lambda_T$ such that $M_\mu(u,v) = M_\mu(u^{(\lambda)}, v^{(\lambda)})\zeta$ for all $\mu = 1,\dots,m$. Eliminating ζ and taking logarithms, these last equations are seen to imply that

$$(27)\quad (i_\mu - i_1)\log u - (j_\mu - j_1)\log v = (i_\mu - i_1)\log u^{(\lambda)} - (j_\mu - j_1)\log v^{(\lambda)} \quad \text{for } \mu = 2,\dots,m.$$

Since all the data in (27) are fixed except for (u,v), it follows that the only solution of (27) is $(u,v) = (u^{(\lambda)}, v^{(\lambda)})$, *except* for the case when the Newton polygon of P_T is degenerate, i.e., when all the points (i_μ, j_μ) for $\mu = 1, \ldots, m$ are collinear.

Let $\mathcal{A}_2$ be the set of $(a,b,c) \in \mathcal{A} \setminus \mathcal{A}_1$ with $a > b > c$ such that the corresponding pair (u,v) is a non-degenerate solution of an equation of the type $P_T(u,v) = 0$, where the Newton polygon of P_T is non-degenerate, and let $\mathcal{B}_2$ be the set of pairs (u,v) which arise from $(a,b,c) \in \mathcal{A}_2$. The above argument together with estimates (23) and (26) shows that

$$(28)\quad \begin{aligned} |\mathcal{B}_2| &\le 2^{18} t_1 \max\{|\Lambda_T| \mid T = T_1, \ldots, T_{t_1}\} \\ &< \exp(13 + 12400(s+1) + 150000(s+1)) < \exp(170000(s+1)). \end{aligned}$$

From now on, we shall assume that $(a,b,c) \in \mathcal{A} \setminus (\mathcal{A}_1 \cup \mathcal{A}_2)$, and therefore that the Newton polygon of P_T is degenerate. Let (i_1, j_1) and (i_2, j_2) be two distinct vertices of that polygon, and write $i_0 := i_2 - i_1$ and $j_0 := j_2 - j_1$. Note that $(i_0, j_0) \ne (0,0)$. Then any solution (u,v) of $P_T(u,v) = 0$ satisfies $u^{i_0} v^{j_0} = K_\lambda$, where K_λ is a rational number belonging to a finite set of cardinality $|\Lambda_T|$. Note that $|i_0| \le 2$ and $|j_0| \le 5$.

STEP 3. *Exploiting the symmetry.* As pointed out in Step 1, $u > v$ is not used in the argument leading to (20). Thus, interchanging u and v everywhere in the first two steps, we conclude that there exists a subset $\mathcal{A}_3 \in \mathcal{A} \setminus \mathcal{A}_1$ such that if we write $\mathcal{B}_3$ for the set of all pairs (u,v) arising from triples $(a,b,c) \in \mathcal{A}_3$, then

$$(29)\quad \begin{aligned} |\mathcal{B}_3| &\le 2^{18} t_1' \max\{|\Lambda'_{T'}| \mid T' = T_1', \ldots, T'_{t_1'}\} \\ &< \exp(13 + 12400(s+1) + 150000(s+1)) < \exp(170000(s+1)), \end{aligned}$$

and if $(a,b,c) \in \mathcal{A} \setminus (\mathcal{A}_1 \cup \mathcal{A}_3)$, then there exist a proper subspace T' of $\mathbb{Q}^m$, a subset $\mathcal{D}'$ of the vertices of the Newton polygon of $P_{T'}$, integers $(i_0', j_0') \ne (0,0)$ with $|i_0'| \le 5$ and $|j_0'| \le 2$, and rational numbers $K_{\lambda'}$ in a set $|\Lambda'_T|$ of cardinality bounded by the right hand side of (26) such that $u^{i_0'} v^{j_0'} = K'_\lambda$. In the above inequality, t_1', T', $\mathcal{D}'$ and $\Lambda'_{T'}$ have the same meaning as t_1, T, $\mathcal{D}$ and Λ_T, respectively, when u and v are interchanged.

If the vector (i_0, j_0) is not parallel to (i_0', j_0'), then the system of equations $u^{i_0} v^{j_0} = K_\lambda$ and $u^{i_0'} v^{j_0'} = K'_\lambda$ has a unique solution (u,v) once K_λ and $K_{\lambda'}$ are fixed. Let $\mathcal{A}_4$ be the subset of $\mathcal{A} \setminus (\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3)$ formed by (a,b,c) such that the corresponding vectors (i_0, j_0) and (i_0', j_0') are not parallel, and let $\mathcal{B}_4$ be the set of pairs (u,v) arising from triples $(a,b,c) \in \mathcal{A}_4$. The above argument and estimates (23) and (26) show that

$$(30)\quad \begin{aligned} |\mathcal{B}_4| &\le 2^{2\cdot 18} t_1 t_1' \\ &\quad \times (\max\{|\Lambda_T|, |\Lambda'_{T'}| \mid T = T_1, \ldots, T_{t_1},\, T' = T_1', \ldots, T'_{t_1'}\})^2 \\ &< \exp(340000(s+1)). \end{aligned}$$

From now on, we assume that $(a,b,c) \in \mathcal{A}\backslash\bigcup_{k=1}^{4}\mathcal{A}_k$. In this case, (i_0,j_0) and (i_0',j_0') are parallel, and since $|i_0| \le 2$, $|j_0'| \le 2$, $|j_0| \le 5$ and $|i_0'| \le 5$, it follows that we may assume that $\max\{|i_0|,|j_0|\} \le 2$. Moreover, since $(i_0,j_0) \ne (0,0)$, by symmetry, and up to changing the signs of both i_0 and j_0, and cancelling their greatest common divisor if needed, we may assume that $i_0 = 1$, and that $j_0 \in \{0,\pm1,\pm2\}$.

STEP 4. *The second system of forms.* We now assume that $(a,b,c) \in \mathcal{A}\setminus\bigcup_{k=1}^{4}\mathcal{A}_k$, that the subspace $T \in \{T_1,\dots,T_{t_1}\}$, the subset $\mathcal{D}$, the index j_0 in $\{0,\pm1,\pm2\}$ (note that j_0 depends only on T and $\mathcal{D}$), and the number $K := K_\lambda$ for $\lambda \in \Lambda_T$ are fixed, and that $uv^{j_0} = K$.

CASE 1: $j_0 \ge 0$. We multiply both sides of (15) for $j = 1$ by c and rewrite it as

$$\Big|cv^5y_1 - \sum_{4-j_0<n\le4} cv^n + \sum_{0\le n<j_0} cuv^n + \sum_{0\le n\le 4-j_0} (uv^{j_0}-1)cv^n\Big| < 2cuv^{-1}. \tag{31}$$

We write $N_1 := 6 + j_0$, note that $N_1 \le 8$, and consider the linear forms in $(X_1,\dots,X_{N_1})$ given by

$$L_{1\infty} := X_1 - \sum_{1<n\le 1+j_0} X_n + \sum_{1+j_0<n\le 1+2j_0} X_n + \sum_{1+2j_0<n\le 6+j_0} (K-1)X_n,$$
$$L_{1w} = X_1, \quad w \in S\setminus\{\infty\}, \tag{32}$$

and $L_{nw} = X_n$ for all $n = 2,\dots,N_1$ and $w \in S$. Let $\mathbf{x} := (x_1,\dots,x_{N_1}) \in (\mathbb{Z}^*)^{N_1}$ be given by $x_1 := cv^5y_1$, $x_n = cv^{n+3-j_0}$ for all $n \in \{2,\dots,1+j_0\}$, $x_n := cuv^{n-2-j_0}$ for $n \in \{2+j_0,\dots,1+2j_0\}$, and $x_n := cv^{n-2-2j_0}$ for $n \in \{2+2j_0,\dots,N_1\}$. A similar calculation to Step 1 shows that

$$|L_{1\infty}(\mathbf{x})|_\infty < 2cuv^{-1}, \tag{33}$$

$$\prod_{w\in S\setminus\{\infty\}} |L_{1w}(\mathbf{x})|_w \le v^{-5}, \tag{34}$$

$$\prod_{w\in S} |L_{jw}(\mathbf{x})|_w \le c \quad \text{for } j = 2,\dots,N_1. \tag{35}$$

Multiplying all the above inequalities, we get

$$\prod_{j=1}^{N_1}\prod_{w\in S} |L_{jw}(\mathbf{x})|_w < 2c^{6+j_0}uv^{-6}, \tag{36}$$

and since $v > ac$, $a > c$ and $u < a^2$ we get

$$2c^{6+j_0}uv^{-6} < 2c^{j_0}ua^{-6} < 2c^{j_0}a^{-4} < 2a^{-2}. \tag{37}$$

It is clear that $\max\{|x_i| \mid i = 1,\dots,N_1\} < cv^5u < a^{13}$, and therefore

$$\prod_{w\in S} |L_{jw}(\mathbf{x})|_w < 2(\max\{|x_i| \mid i = 1,\dots,N_1\})^{-2/13}. \tag{38}$$

We now note that

$$2(\max\{|x_i| \mid i=1,\ldots,N_1\})^{-2/13} < 8^{-1/7}(\max\{|x_i| \mid i=1,\ldots,N_1\})^{-1/7}$$

whenever

$$\max\{|x_i| \mid i=1,\ldots,N_1\} > 2^{7\cdot 13}\cdot 8^{13},$$

and that if the above inequality is not satisfied, then since $a < v < cv^5 y_1 \le \max\{|x_i| \mid i=1,\ldots,N_1\}$, we get $a < 2^{7\cdot 13}\cdot 8^{13} < e^{400}$, and such triples (a,b,c) have already been accounted for in $\mathcal{A}_1$. Thus, we may assume that

$$\prod_{w\in S} |L_{jw}(\mathbf{x})|_w < 8^{-1/7}(\max\{|x_i| \mid i=1,\ldots,N_1\})^{-1/7}. \tag{39}$$

In particular, (11) is satisfied with $\delta = 1/7$ because $N_1 = 6+j_0 \le 8$. It is clear that (10) also holds. Moreover, since $x_1 = cv^5y_1 \ge cv^4(u-1) > 9cv^2(u-1)$ (because $v = ac+1 > 3$), and since one of x_n for $n=2,\ldots,N_1$ equals c, we get

$$\mathcal{H}(\mathbf{x}) > 9cv^2(u-1)c^{-1} > 9v^2(u-1).$$

On the other hand, since the coefficients of our linear forms are integers of absolute value at most $K-1$, we get

$$H(L_{iw}) \le (N_1(K-1)^2)^{1/2} \le 8^{1/2}(K-1) =: H$$

and

$$H = 8^{1/2}(K-1) < 3uv^2 < 9v^2(u-1) < \mathcal{H}(\mathbf{x}).$$

We can therefore apply Corollary E1 to deduce that there exist proper subspaces $W_1,\ldots,W_{t_2}$ of $\mathbb{Q}^{N_1}$ with

$$t_2 \le (2^{60N_1^2}\cdot 7^{7N_1})^{s+1} \le (2^{60\cdot 8^2}\cdot 7^{7\cdot 8})^{s+1} < \exp(2800(s+1)) \tag{40}$$

such that $\mathbf{x} \in W_1 \cup \cdots \cup W_{t_2}$. Let W be one of these subspaces. Imposing that $\mathbf{x}\in W$, and simplifying c, it follows that there exists a rational number γ_W and a polynomial $P_W(X,Y) \in \mathbb{Q}[X,Y]$ consisting only of the monomials Y^n for $n=0,\ldots,4$ and XY^j for $j=0,\ldots,j_0-1$, not both zero, such that

$$\gamma_W \frac{v^5(u-1)}{v-1} + P_W(u,v) = 0. \tag{41}$$

The fact that the left hand side of (41) is not identically zero can be justified by the argument from [4].

We now look at the solutions (u,v) of (41) with $uv^{j_0} = K$. Assume first that $j_0 = 0$. In this case $u = K > 1$ is fixed, $P_W(u,v) = P_W(v)$ does not depend on u, and since not both γ_W and P_W are zero, (41) leads to a non-trivial polynomial equation in v of degree at most 5, so that v can take at most 5 values. Assume now that $j_0 > 0$. If $\gamma_W = 0$, then either $\partial P_W/\partial X = 0$, i.e., $P_W(u,v)$ does not depend on u, and then (41) leads to a non-trivial polynomial equation in v of degree at most 4, and hence

v can assume at most 4 values, or $\partial P_W/\partial X \neq 0$, in which case (41) gives $u = R(v)$, where $R(v)$ is a non-zero rational function in v whose denominator has degree $\leq j_0 - 1$ and whose numerator has degree ≤ 4. Since $u = K/v^{j_0}$, the equation $R(v) = K/v^{j_0}$ leads to a non-trivial polynomial equation in v of degree $\leq 4 + j_0 \leq 6$, and so v can take at most 6 values in this instance.

Finally, assume that $\gamma_W \neq 0$. In this case, we may assume that $\gamma_W = 1$. Then (41) can be rewritten as

$$v^5 u - v^5 + (v-1)P_1(v) + u(v-1)P_2(v) = 0,$$

where $P_2(v)$ is of degree $\leq j_0 - 1$ and $P_1(v)$ is of degree at most 4. Thus,

$$u(v^5 + (v-1)P_2(v)) = v^5 - (v-1)P_1(v),$$

and the polynomial $v^5 + (v-1)P_2(v)$ is non-zero because the degree of $(v-1)P_2(v)$ is at most $j_0 \leq 2$. Thus, we get the equation

$$\frac{v^5 - (v-1)P_1(v)}{v^5 + (v-1)P_2(v)} = \frac{K}{v^{j_0}}. \tag{42}$$

If P_2 is non-zero, we may write $v^5 + (v-1)P_2(v) = v^k Q(v)$, where $k \leq j_0 - 1 < j_0$ and $Q(0) \neq 0$. It is then easy to see (by comparing the orders at which v divides the denominators of the two sides of (42)) that (42) leads to a non-trivial polynomial equation in v of degree at most $5 + j_0 \leq 7$, and therefore v can take at most 7 values. Finally, when $P_2 = 0$, (41) becomes

$$\frac{v^5 - (v-1)P_1(v)}{v^5} = \frac{K}{v^{j_0}},$$

which can be rewritten as

$$v^{5-j_0}(v^{j_0} - K) = (v-1)P_2(v), \tag{43}$$

which together with the fact that $K > 1$ and $j_0 > 0$ implies that $v - 1$ is coprime to both v^{5-j_0} and to $v^{j_0} - K$ (as polynomials in $\mathbb{Q}[v]$), and therefore (43) is a non-trivial polynomial equation in v of degree at most 5, and so v can take at most 5 values.

Let $\mathcal{A}_5$ be the set of triples (a,b,c) in $\mathcal{A} \setminus \bigcup_{k=1}^{4} \mathcal{A}_k$ for which $j_0 \geq 0$. The preceding argument together with estimates (23), (26) and (41) shows that if we write $\mathcal{B}_5$ for the set of pairs (u,v) arising from triples $(a,b,c) \in \mathcal{A}_5$, then

$$\begin{aligned} |\mathcal{B}_5| &< 2^{18} \cdot 7 \exp(12400(s+1)) \exp(150000(s+1)) \exp(2800(s+1)) \\ &< \exp(170000(s+1)). \end{aligned} \tag{44}$$

Case 2: $j_0 \in \{-1, -2\}$. In this case, we replace j_0 by $-j_0$ and assume again that T, $\mathcal{D}$ and $K := K_\lambda$ for $\lambda \in \Lambda_T$ are fixed, and that $u/v^{j_0} = K$. It then follows easily that there exist fixed positive integers α and β, which are S-units, and another positive integer ϱ, also an S-unit, such that $u = \alpha\varrho^{j_0}$

and $v=\beta\varrho$. We multiply again both sides of (15) by c, and rewrite it as

$$\Big|cv^5y_1-\sum_{n=0}^{j_0-1}c\beta^n\varrho^n+\sum_{n=0}^{4-j_0}(\alpha-\beta^{j_0})c\beta^n\varrho^{n+j_0}+\sum_{n=5-j_0}^{4}c\alpha\beta^n\varrho^{n+j_0}\Big|<2cuv^{-1}.$$

We let $N_1:=6+j_0$, $K_1:=\alpha-\beta^{j_0}$ and consider the linear forms in $X_1,\dots,X_{N_1}$ given by

$$L_{1\infty}:=X_1-\sum_{n=2}^{j_0+1}X_n+\sum_{n=j_0+2}^{6}K_1X_n+\sum_{n=7}^{6+j_0}X_n,\qquad L_{1w}:=X_1,\qquad w\in S\backslash\{\infty\},$$

and $L_{jw}=X_j$ for $j=2,\dots,N_1$ and $w\in S$. Note that $K_1\neq 0$, for otherwise $u-1=(\beta\varrho)^{j_0}-1=v^{j_0}-1$, leading either to $u=v$ if $j_0=1$, which is impossible, or to $u=v^2$ and $a\le\gcd(v^2-1,v-1)=v-1=u^{1/2}-1<u^{1/2}$, which is again impossible. We let $\mathbf{x}:=(x_1,\dots,x_{N_1})$ be the obvious vector with non-zero integer components given by $x_1=cv^5y_1$, $x_n=c(\beta\varrho)^{n-2}$ when $n\in\{2,\dots,j_0+1\}$, $x_n=c\beta^{n-2-j_0}\varrho^{n-2}$ when $n\in\{2+j_0,6\}$, and $x_n=c\alpha\beta^{n-2-j_0}\varrho^{n-2}$ when $n\in\{7,\dots,6+j_0\}$. Computations similar to the ones in the previous case show that inequality (38) holds for our forms, and since we are assuming that $(a,b,c)\notin\mathcal{A}_1$, inequality (39) is also satisfied. Moreover, it is clear that we can take

$$H:=8^{1/2}|\alpha-\beta^{j_0}|<3uv^{j_0}\le 3uv^2$$

and one checks, as in the previous case, that $\mathcal{H}(\mathbf{x})>H$. Finally, since (10) is also satisfied, we conclude, as in the previous case, that there exist proper subspaces $W_1',\dots,W_{t_2'}'$ of $\mathbb{Q}^{N_1}$ with

$$t_2'\le(2^{60N_1^2}\cdot 7^{7N_1})^{s+1}\le(2^{60\cdot 8^2}\cdot 7^{7\cdot 8})^{s+1}<\exp(2800(s+1))\tag{45}$$

such that $\mathbf{x}\in W_1'\cup\dots\cup W_{t_2'}'$. Let W' be one of these subspaces. Imposing that $\mathbf{x}\in W'$, and simplifying c, it follows that there exists a rational number $\gamma_{W'}$ and a polynomial $P_{W'}\in\mathbb{Q}[\varrho]$ consisting only of the monomials ϱ^n for $n=0,\dots,4+j_0$, not both zero, such that

$$\gamma_{W'}\frac{\beta^5\varrho^5(\alpha\varrho^{j_0}-1)}{\beta\varrho-1}+P_{W'}(\varrho)=0.\tag{46}$$

The fact that the left hand side of (46) is not identically zero is almost clear. Indeed, if say $\gamma_{W'}=0$, then this is obviously so because $P_{W'}$ is not the zero polynomial, while when $\gamma_{W'}\neq 0$, this follows from the fact that $\beta\varrho-1$ does not divide $\varrho^5(\alpha\varrho^{j_0}-1)$ in $\mathbb{Q}[\varrho]$, because $\alpha\neq\beta^{j_0}$. Clearly, each of equations (46) is a non-trivial polynomial equation in ϱ of degree at most $5+j_0\le 7$, and therefore ϱ can take at most 7 values.

Thus, if we let $\mathcal{A}_6$ be the set of triples (a,b,c) in $\mathcal{A}\setminus\bigcup_{k=1}^5\mathcal{A}_k$ for which our initial value of j_0 was negative, then the preceding argument together with estimates (23), (26) and (45) shows that if we write $\mathcal{B}_6$ for the set of pairs (u,v) arising from triples $(a,b,c)\in\mathcal{A}_6$, then

$$
\begin{aligned}
(47)\qquad |\mathcal{B}_6| &< 2^{18}\cdot 7\exp(12400(s+1))\exp(150000(s+1))\exp(2800(s+1))\\
&< \exp(170000(s+1)).
\end{aligned}
$$

The conclusion is that all pairs (u,v) obtained from all $(a,b,c)\in\mathcal{A}$ form a finite set $\mathcal{B} := \bigcup_{k=1}^{6}\mathcal{B}_k$, whose cardinality is, by (28), (29), (30), (44) and (47), at most

$$
\begin{aligned}
(48)\qquad |\mathcal{B}| &\le \sum_{k=1}^{6}|\mathcal{B}_k|\\
&< \exp(1200) + 4\exp(170000(s+1)) + \exp(340000(s+1))\\
&< 6\exp(340000(s+1)) < \exp(341000(s+1)).
\end{aligned}
$$

STEP 5. *Some Pell equations.* Let B denote the upper bound on $|\mathcal{B}|$ appearing in (48) and let $(u,v)\in\mathcal{B}$. Write $D := \gcd(u-1,v-1)$, $b_1 := (u-1)/D$, $c_1 := (v-1)/D$ and $\varrho := D/a$. Write $d_1 := b_1c_1$, and note that d_1 is fixed. It is then clear that ϱ is an integer, $b = b_1\varrho$, $c = c_1\varrho$, and $bc+1 = d_1\varrho^2+1$. We now finally exploit the fact that $w := bc+1$ is an S-unit. Write $w := d_2z^2$, where d_2 is square-free. It is clear that d_2 can be chosen in at most 2^s ways. Fixing d_2, it follows that ϱ and z are related via the Pell equation

$$(49)\qquad d_2z^2 - d_1\varrho^2 = 1,$$

and that moreover z is an S-unit. It is clear that not both d_1 and d_2 can be perfect squares. It is then well known that all the positive integer solutions (z,ϱ) of the above equation have the property that z is a member of a Lucas or a Lehmer sequence. That is, if (z_0,ϱ_0) denotes the smallest solution of (49) in positive integers, and if we write

$$\lambda := \sqrt{d_2}\,z_0 + \sqrt{d_1}\,\varrho_0,\qquad \mu := \sqrt{d_2}\,z_0 - \sqrt{d_1}\,\varrho_0,$$

then any solution of (49) in positive integers must have

$$(50)\qquad z = \frac{\lambda^t+\mu^t}{\lambda+\mu}\,z_0$$

for some odd positive integer t, except when $d_2 = 1$, in which case the same formula holds but with an arbitrary positive integer t not necessarily odd. The set of possible values of z given by (50) forms a *Lehmer* sequence $(z_t)_{t\ge 0}$, where t is allowed to take only odd values if $d_2 > 1$. A result of Morgan Ward [12] says that if $t > 18$, then z_t has *primitive divisors*, i.e., for such t there exists a prime number $p \mid z_t$ such that p does not divide z_l for any positive integer $l < t$. It now follows that if we want $z = z_t$ to be an S-unit, then t can take at most $s+18$ values. This shows that the triple (u,v,w) can take at most

$$2^s(s+18)B < \exp(s+18s)B < \exp(342000(s+1)) \tag{51}$$

values. Finally, note that if (u,v,w) is given, then (a,b,c) is uniquely determined, because $a^2=(u-1)(v-1)/(w-1)$, and a is positive. Thus,

$$|\mathcal{A}|+1 < 1+\exp(342000(s+1)) < \exp(350000(s+1)). \tag{52}$$

We further remark that $s \ge 2$. Indeed, if $s=1$ and $\mathcal{A}$ is non-empty, then there exists a prime number p and positive integers $i>j$ and $a>b>c$ such that $ab+1=u=p^i,\ ac+1=v=p^j$. Thus,

$$\begin{aligned} a &\le \gcd(u-1,v-1)=\gcd(p^i-1,p^j-1)=p^{\gcd(i,j)}-1\\ &\le p^{i/2} < p^{i/2} = u^{1/2} < a, \end{aligned}$$

which is a contradiction. Thus, $s\ge 2$, therefore $s+1 \le 3s/2$. Hence,

$$|\mathcal{A}|+1 < \exp(350000(s+1)) < \exp(350000\cdot 3s/2) < \exp(6\cdot 10^5 s),$$

and so

$$s > c_1 \log(|\mathcal{A}|+1),$$

with $c_1 := 6^{-1}\cdot 10^{-5}$, which is stronger than what is claimed in our theorem.

Proof of Corollary 1. Since $s\ge 2$ whenever $\mathcal{A}$ is non-empty, we may assume that $P:=\max\{P((ab+1)(ac+1)(bc+1)) \mid (a,b,c)\in\mathcal{A}\} \ge 3$, and that $\log(|\mathcal{A}|+1) > 2\cdot 10^6$, for otherwise the lower bound in (2) is smaller than 3. Let m be the smallest integer $\ge \frac{1}{6\cdot 10^5}\log(|\mathcal{A}|+1)$. Note that $m\ge 4$ since $\log(|\mathcal{A}|+1) > 2\cdot 10^6$. Let p_m be the mth prime number. From the above proof of Theorem 1, we know that $s\ge m$, therefore $P \ge p_m > m\log m$, where the last inequality is well known (see [10], for example). We now show that

$$m \ge \log^{1/15}(|\mathcal{A}|+1).$$

Indeed, this follows from

$$\frac{1}{6\cdot 10^5}\ \log(|\mathcal{A}|+1) > \log^{1/15}(|\mathcal{A}|+1),$$

which is equivalent to

$$\log(|\mathcal{A}|+1) > (6\cdot 10^5)^{15/14},$$

and this last inequality is satisfied when $\log(|\mathcal{A}|+1) > 2\cdot 10^6$. Thus,

$$\begin{aligned} P > m\log m &> \frac{1}{6\cdot 10^5}\ \log(|\mathcal{A}|+1)\log\left(\frac{\log(|\mathcal{A}|+1)}{6\cdot 10^5}\right)\\ &> \frac{1}{6\cdot 15}\cdot\frac{1}{10^5}\ \log(|\mathcal{A}|+1)\log\log(|\mathcal{A}|+1)\\ &> c_2\log(|\mathcal{A}|+1)\log\log(|\mathcal{A}|+1), \end{aligned}$$

with $c_2 := 9^{-1} \cdot 10^{-6}$, which is a stronger inequality than the one asserted by Corollary 1.

5. Other quantitative aspects. As mentioned in the introduction, it is shown in [4] that $P((ab+1)(ac+1))$ tends to infinity over all the triples of distinct positive integers (a,b,c) with $a > b > c$. One could ask whether there exists a quantitative lower bound for the number of distinct prime factors of $(ab+1)(ac+1)$, where (a,b,c) varies in a finite set of triples of distinct positive integers with $a > b > c$. More precisely, one can address the following question:

QUESTION 1. *Does there exist a function $f : \mathbb{N} \to \mathbb{N}$ with $\lim_{n\to\infty} f(n) = \infty$ such that if $\mathcal{A}$ is any non-empty set of triples of distinct positive integers (a,b,c) with $a > b > c$, then*

$$\omega\Big(\prod_{(a,b,c)\in\mathcal{A}} (ab+1)(ac+1)\Big) > f(|\mathcal{A}|)? \tag{53}$$

The answer to the above question is no. In order to show this, we recall a result on the distribution of primes in arithmetic progressions. For positive integers $1 \le a < d$ with $\gcd(a,d) = 1$ and for a large positive real number x we write $\pi(x; d, a)$ for the number of prime numbers $p \le x$ with $p \equiv a \pmod{d}$. We also write $\pi(x)$ for the number of prime numbers $p \le x$. The following theorem on the distribution of primes in arithmetic progressions with large moduli follows from Theorem 9 of [2] by partial integration.

THEOREM BFI. *For any positive constant B and any $\varepsilon > 0$, there exists a positive constant $C := C(B)$ depending on B such that if x is a large real number, and Q and R are positive integers with $R < x^{1/10-\varepsilon}$ and $QR < x/\log^C x$, then*

$$\sum_{r=1}^{R} \Big| \sum_{q=1}^{Q} \Big(\pi(x; qr, 1) - \frac{\pi(x)}{\phi(qr)} \Big) \Big| \ll \frac{x}{\log^B x}. \tag{54}$$

Let $c_3 > 1$ be any fixed constant, x be a large positive real number, and put $z := c_3 \log\log x$ and $R := \prod_{p\le z} p$. We note that by the Prime Number Theorem,

$$R = \exp(c_3(1+o(1))\log\log x) < \log^{2c_3} x \tag{55}$$

for large values of x. In particular, $R < x^{1/10-\varepsilon}$ say with $\varepsilon := 1/20$ when $x > x(c_3)$.

Let $B := 2c_3$ and $C := C(B)$. Since $x^{3/4}R < x^{3/4}\log^{2c_3} x < x/\log^C x$ for sufficiently large values of x, we apply Theorem BFI twice, with $Q = Q_1 := \lfloor x^{2/3} \rfloor$ and with $Q = Q_2 := \lfloor x^{3/4} \rfloor$, and use the absolute value inequality, to conclude that

$$\left|\sum_{Q_1<q\le Q_2}\left(\pi(x;qR,1)-\frac{\pi(x)}{\phi(qR)}\right)\right| \ll \frac{x}{\log^B x}. \tag{56}$$

We now show that there exists $q \in [Q_1, Q_2]$ such that $\pi(x;qR,1) \ge 2$. Assume that this is not so. Then $\pi(x;qR,1) \le 1$ for all $q \in [Q_1, Q_2]$, and therefore

$$\begin{aligned}\left|\sum_{Q_1<q\le Q_2}\left(\frac{\pi(x)}{\phi(qR)}-\pi(x;qR,1)\right)\right| &\ge \sum_{Q_1<q\le Q_2}\frac{\pi(x)}{qR} - Q_2 \\ &> \frac{\pi(x)}{R}\sum_{Q_1<q\le Q_2}\frac{1}{q} - x^{3/4}.\end{aligned} \tag{57}$$

Clearly,

$$\sum_{Q_1<q\le Q_2}\frac{1}{q} = \log\left(\frac{Q_2}{Q_1}\right) + o(1) = \frac{1}{12}\log x + o(1) > c_4 \log x$$

for large values of x, where one can take $c_4 := 1/13$, and since $\pi(x) > x/\log x$ for all $x > 17$ (see [10]), the above inequality together with (55) implies that

$$\frac{\pi(x)}{R}\sum_{Q_1<q\le Q_2}\frac{1}{q} \ge c_4\,\frac{x}{\log^{2c_3-1} x}.$$

By (57),

$$\begin{aligned}\left|\sum_{Q_1<q\le Q_2}\left(\frac{\pi(x)}{\phi(qR)}-\pi(x;qR,1)\right)\right| &\ge c_4\,\frac{x}{\log^{2c_3-1} x} - x^{3/4} \\ &\ge c_5\,\frac{x}{\log^{2c_3-1} x}\end{aligned} \tag{58}$$

for large values of x, where one can take $c_5 := 1/14$; but (58) contradicts (56) for large values of x.

Thus, we have shown that there exists $q \in [Q_1, Q_2]$ such that $\pi(x;qR,1) \ge 2$. Let $v < u \le x$ be two prime numbers which are congruent to 1 modulo qR. For every divisor d of R we let $a := qR/d$, $b := (u-1)/a$ and $c := (v-1)/a$. Note that $a \ge q \ge \lfloor x^{2/3} \rfloor > x^{1/2} \ge u^{1/2}$, and therefore $a > b > c$. Let $\mathcal{A}$ be the set of all the above triples. It is clear that

$$|\mathcal{A}| = \tau(R) = 2^{\pi(z)} > \exp\left(c_6\,\frac{\log\log x}{\log\log\log x}\right) \tag{59}$$

for sufficiently large x, where c_6 can be taken to be any positive constant smaller than $c_3 \log 2$. However, $(ab+1)(ac+1) = uv$ for all triples (a,b,c)

of $\mathcal{A}$. Thus,

$$\omega\Big(\prod_{(a,b,c)\in\mathcal{A}}(ab+1)(ac+1)\Big)=2, \tag{60}$$

and now (59) and (60) show that the answer to Question 1 is indeed negative.

Győry & Sárközy [7] also raised the question of finding examples of finite sets $\mathcal{A}$ of triples of distinct positive integers (a,b,c) such that the quantity

$$\omega\Big(\prod_{(a,b,c)\in\mathcal{A}}(ab+1)(ac+1)(bc+1)\Big)$$

is small with respect to $|\mathcal{A}|$. The trivial construction obtained by letting $\mathcal{A}$ be the set of all triples with $\max\{a,b,c\}<x$ shows that

$$\omega\Big(\prod_{(a,b,c)\in\mathcal{A}}(ab+1)(ac+1)(bc+1)\Big)\ll\frac{|\mathcal{A}|^{2/3}}{\log|\mathcal{A}|} \tag{61}$$

for infinitely many finite sets $\mathcal{A}$ whose cardinalities tend to infinity. Our next result improves upon the above estimate.

PROPOSITION 1. *Fix $\varepsilon>0$. There are infinitely many finite sets $\mathcal{A}$ of triples (a,b,c) of distinct positive integers whose cardinalities tend to infinity such that*

$$\omega\Big(\prod_{(a,b,c)\in\mathcal{A}}(ab+1)(ac+1)(bc+1)\Big)\ll|\mathcal{A}|^{1/2+\varepsilon}. \tag{62}$$

The constant understood in the $\ll$ above depends at most on ε.

For the proof of Proposition 1, we need a result concerning the distribution of smooth numbers in arithmetic progressions. Let x be a large positive real number. For any positive integer $y\le x$, we write $\Psi(x,y)$ for the number of positive integers $n\le x$ with $P(n)\le y$. For positive integers $1\le r<q$ with $\gcd(r,q)=1$ we write $\Psi(x,y;q,r)$ for the number of numbers $n\le x$ with $P(n)\le y$ such that $n\equiv r\pmod q$. The following result is due to Balog & Pomerance [1].

THEOREM BP. *Let $\varepsilon>0$ be an arbitrarily small positive real number. The estimate*

$$\Psi(x,y;q,r)=\frac{x}{q}\,(w\log(w+1))^{-w}e^{O(w)} \tag{63}$$

holds uniformly under the conditions

$$\begin{gathered}x\ge 2,\qquad \exp((\log\log x)^2)\le y\le x^{2/3-\varepsilon},\\ 1\le q\le(\min\{y,x/y\})^{4/3-\varepsilon},\qquad \gcd(r,q)=1,\end{gathered} \tag{64}$$

where $w:=\log x/\log y$.

Let $\varepsilon > 0$ be sufficiently small, x be a large positive real number, and put $I := [x^{2/3-\varepsilon/2}/2, x^{2/3-\varepsilon/2}]$. Let $r := 1$, q be an arbitrary integer in I, and $y := x^{1/2}$. It is clear that

$$\exp((\log\log x)^2) \le y \le x^{2/3-\varepsilon/2}$$

if x is sufficiently large and $\varepsilon < 1/12$. Note also that

$$(\min\{y, x/y\})^{4/3-\varepsilon/2} = x^{2/3-\varepsilon/4} > q$$

for all $q \in I$. Thus, all conditions (64) are satisfied, and by (11) with $w = \log x/\log y = 2$, we get

$$\Psi(x, y; q, 1) \gg \frac{x}{q} \gg x^{1/3+\varepsilon/2}. \tag{65}$$

We now take $\mathcal{A}$ to be the set of all triples (a, b, c), where $a := q \in I$, $b := (u-1)/a$, $c := (v-1)/a$, and $v < u \le x$ are positive integers with $P(uv) \le y$ both in the arithmetic progression $1 \pmod q$. We observe that since $q > x^{2/3-\varepsilon/2}/2 > x^{1/2}$ whenever $\varepsilon < 1/12$ and x is sufficiently large, it follows that all such triples are distinct. Thus,

$$|\mathcal{A}| \ge |I \cap \mathbb{N}| \binom{\Psi(x, y; q, 1)}{2} \gg |I \cap \mathbb{N}| \Psi(x, y; q, 1)^2 \gg x^{4/3+\varepsilon/2}. \tag{66}$$

We now note that

$$bc + 1 \le (2x^{1/3+\varepsilon/2})^2 + 1 \le 5x^{2/3+\varepsilon},$$

and since $P(uv) \le x^{1/2}$, it follows that for large x we have

$$\omega\Big(\prod_{(a,b,c)\in\mathcal{A}} (ab+1)(ac+1)(bc+1)\Big) \le \pi(5x^{2/3+\varepsilon}) \ll \frac{x^{2/3+\varepsilon}}{\log x}. \tag{67}$$

Finally, note that inequality (66) implies that

$$|\mathcal{A}|^{1/2+\varepsilon} \gg x^{(4/3+\varepsilon/2)(1/2+\varepsilon)} > x^{2/3+\varepsilon},$$

which together with (67) shows that

$$\omega\Big(\prod_{(a,b,c)\in\mathcal{A}} (ab+1)(ac+1)(bc+1)\Big) < |\mathcal{A}|^{1/2+\varepsilon}$$

for large values of x, which completes the proof of Proposition 1.

Acknowledgements. This work was completed while the second author visited the University Louis Pasteur in Strasbourg in July 2003. He thanks the people of the Mathematical Institute for their warm hospitality. Both authors were supported by the joint project ECOS Nord – CONACyT, France-Mexico M02-M01.

References

[1] A. Balog and C. Pomerance, *The distribution of smooth numbers in arithmetic progressions*, Proc. Amer. Math. Soc. 115 (1992), 33–43.

[2] E. Bombieri, J. B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. 156 (1986), 203–251.

[3] Y. Bugeaud, *On the greatest prime factor of* $(ab+1)(bc+1)(ca+1)$, Acta Arith. 86 (1998), 45–49.

[4] P. Corvaja and U. Zannier, *On the greatest prime factor of* $(ab+1)(ac+1)$, Proc. Amer. Math. Soc. 131 (2003), 1705–1709.

[5] J.-H. Evertse, *The number of solutions of decomposable form equations*, Invent. Math. 122 (1995), 559–601.

[6] —, *An improvement of the Quantitative Subspace Theorem*, Compositio Math. 101 (1996), 225–311.

[7] K. Győry and A. Sárközy, *On prime factors of integers of the form* $(ab+1)(bc+1)\times(ca+1)$, Acta Arith. 79 (1997), 163–171.

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

[9] S. Hernández and F. Luca, *On the largest prime factor of* $(ab+1)(ac+1)(bc+1)$, Bol. Soc. Mat. Mexicana (3) 9 (2003), 235–244.

[10] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[11] C. L. Stewart and R. Tijdeman, *On the greatest prime factor of* $(ab+1)(ac+1)\times(bc+1)$, Acta Arith. 79 (1997), 93–101.

[12] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), 230–236.

U.F.R. de mathématiques
Université Louis Pasteur
7, rue René Descartes
67084 Strasbourg, France
E-mail: bugeaud@math.u-strasbg.fr

Mathematical Institute
UNAM
Ap. Postal 61-3 (Xangari), CP 58 089
Morelia, Michoacán, Mexico
E-mail: fluca@matmor.unam.mx

Received on 29.7.2003
and in revised form on 28.11.2003 (4584)