VOLUME
22/2014
No. 1

ISSN 1804-1388 (Print)
ISSN 2336-1298 (Online)

COMMUNICATIONS IN MATHEMATICS

Available online at
http://cm.osu.cz

UNIVERSITAS OSTRAVIENSIS

Communications in Mathematics 22 (2014) 49–55

A note on the number of S-Diophantine quadruples

Florian Luca, Volker Ziegler

Abstract. Let $(a_1, \dots, a_m)$ be an m-tuple of positive, pairwise distinct integers. If for all $1 \le i < j \le m$ the prime divisors of $a_i a_j + 1$ come from the same fixed set S, then we call the m-tuple S-Diophantine. In this note we estimate the number of S-Diophantine quadruples in terms of $|S| = r$.

1 Introduction

There is a vast amount of papers concerning the problem of determining the number of prime divisors of products of the form

$$\prod_{a\in A,\, b\in B} (a+b) \qquad \text{and} \qquad \prod_{a\in A,\, b\in B} (ab+1),$$

where A and B are finite sets of positive integers. In particular, the first product has been studied, first by Erdős and Turán [4] and their investigations were continued in a series of papers by Sárközy and Stewart (see e.g. [12], [13]). The second product was studied e.g. by Győry, Sárközy and Stewart [8], Sárközy and Stewart [14], and others.

In their paper [8], Győry, Sárközy and Stewart conjectured that the largest prime factor of

$$(ab+1)(ac+1)(bc+1)\,, \quad 0 < a < b < c\,,$$

goes to infinity as c does. This conjecture has been proved by Corvaja and Zannier [3] and Hernandez and Luca [9], independently. Due to the application of the Subspace theorem their results stay ineffective. The best approach to estimate the growth rate of the largest prime factor of $(ab+1)(ac+1)(bc+1)$ is due to Luca [10], who proved that for every fixed finite set of primes S, there exist ineffective constants C_S and C'_S such that

$$((bc+1)(ac+1))_{\bar{S}} > \exp\left(C_S \frac{\log c}{\log\log c}\right)$$

2010 MSC: 11D45, 11N32
Key words: Diophantine equations, S-unit equations, S-Diophantine tuples

whenever $a < b < c$ with $c > C'_S$, where $(\cdot)_{\bar{S}}$ denotes the S-free part.

In case of quadruples effective results are known. For example, Stewart and Tijdeman [15], proved that the largest prime factor of

$$\prod_{a,b\in A,\, a\neq b} (ab+1)$$

with $|A| \geq 4$, is at least $C \log\log \max A$, where C is an effective computable constant.

Let S be a fixed, finite set of primes. In view of classical Diophantine m-tuples we call an m-tuple $(a_1, \dots, a_m)$ of positive, pairwise distinct, integers S-Diophantine if for all $1 \leq i < j \leq m$ the set of prime divisors of $a_i a_j + 1$ is contained in S. The results of Corvaja, Zannier [3] and Hernandez, Luca [9] yield the finiteness of S-Diophantine triples for fixed S. Although we are able to estimate the number of S-Diophantine triples due to a result of Bugeaud and Luca [2], it is in principle not possible to determine all triples with the methods currently available.

In contrast to the case of triples we can, in principle, effectively determine all S-Diophantine quadruples for a given set S due to the result of Stewart and Tijdeman [15]. Recently, Szalay and Ziegler [16], established an efficient algorithm to determine all S-Diophantine quadruples for a given set S of primes, provided $|S| = 2$. In particular, the results of Szalay and Ziegler [16], [17], [18], suggest that for $|S| = 2$ no quadruple exists at all.

The aim of this note is to give upper bounds for the number of S-Diophantine quadruples for fixed sets S of r primes. We need the following notations. Let Γ be a multiplicative subgroup of $\mathbb{Q}^*$ of rank r and denote by $A(n,r)$ an upper bound for the number of non-degenerate solutions $(x_1, \dots, x_n) \in \Gamma^n$ to the linear S-unit equation

$$a_1 x_1 + \cdots + a_n x_n = 1\,, \quad a_i \in \mathbb{Q}^*. \tag{1}$$

We call a solution to (1) non-degenerate if no subsum on the left hand side of equation (1) vanishes. With this notation at hand our main result is:

Theorem 1. *Let S be a set of r primes. Then there exist at most*

$$\big(A(5,r) + A(2,r)^2\big)A(3,r)$$

S-Diophantine quadruples. If $r = 2$ or $2 \notin S$, then there exist at most

$$A(5,r)A(3,r)$$

S-Diophantine quadruples.

Using the best estimates for $A(n,r)$ currently available we obtain

Corollary 1. *Let S be a set of r primes. Then there exist at most*

$$\exp(27398 + 5136r)$$

S-Diophantine quadruples.

In the next section we prove Theorem 1 and in the third section we discuss the number of solutions to the S-unit equation (1) and establish Corollary 1.

2 A system of S-unit equations

Assume that (a, b, c, d) is an S-Diophantine quadruple, with $a < b < c < d$. We write,

$$\begin{aligned} ab + 1 &= s_1\,, & ac + 1 &= s_2\,, & ad + 1 &= s_3\,,\\ bc + 1 &= s_4\,, & bd + 1 &= s_5\,, & cd + 1 &= s_6\,. \end{aligned}$$

With these notations we have

$$\begin{aligned} abcd &= s_1 s_6 - s_1 - s_6 + 1\\ &= s_2 s_5 - s_2 - s_5 + 1\\ &= s_3 s_4 - s_3 - s_4 + 1 \end{aligned}$$

and obtain the following system of S-unit equations

$$\begin{aligned} s_1 s_6 - s_1 - s_6 - s_2 s_5 + s_2 + s_5 &= 0\,,\\ s_1 s_6 - s_1 - s_6 - s_3 s_4 + s_3 + s_4 &= 0\,. \end{aligned} \tag{2}$$

Let us consider the first equation more closely and write $y_1 = s_1 s_6$, $y_2 = s_1$, $y_3 = s_6$, $y_4 = s_2 s_5$, $y_5 = s_2$ and $y_6 = s_5$. Then the first equation of system (2) takes the form

$$y_1 - y_2 - y_3 - y_4 + y_5 + y_6 = 0$$

and has at most $A(5, r)$ projective solutions in $\mathbb{P}^5(\Gamma)$ such that no subsum vanishes, where $\Gamma \subset \mathbb{Q}^*$ is the multiplicative group generated by S. Note that each projective solution yields at most one solution (s_1, s_2, s_5, s_6). Indeed, assume (s_1, s_2, s_5, s_6) and (s_1', s_2', s_5', s_6') correspond to the same projective solution. Then there is a rational number $\rho \neq 0$ such that $s_1 = \rho s_1'$, $s_6 = \rho s_6'$, $s_2 = \rho s_2'$, $s_5 = \rho s_5'$ and $s_1 s_6 = \rho s_1' s_6'$. But this implies that $s_1 s_6 = \rho^2 s_1' s_6' = \rho s_1' s_6'$, thus $\rho = 1$ and $s_i = s_i'$ for $i = 1, 2, 5, 6$.

So we are left to count how many solutions exist with vanishing subsums. Of course there exist no vanishing one-term subsums. Two-term vanishing subsums imply either

- $s_i = s_j$ for $i \neq j$ which is impossible, unless $i, j \in \{3, 4\}$ which is excluded, or
- $s_i = s_1 s_6 > abcd > cd + 1 \geq s_6 \geq s_i$ for some $i \in \{1, 2, 5, 6\}$ which is also a contradiction, or
- $s_i = s_2 s_5 > abcd > cd + 1 \geq s_6 \geq s_i$ for some $i \in \{1, 2, 5, 6\}$ which is also a contradiction, or
- $s_1 s_6 = s_2 s_5$, which implies $ab + cd + 2 = s_1 + s_6 = s_2 + s_5 = ac + bd + 2$; hence, $(c - b)(d - a) = 0$; i.e., $d = a$ or $b = c$, again a contradiction.

Therefore no two-term subsums vanish. Since four- and five-term vanishing subsums imply the existence of two- and one-term vanishing subsums, respectively, we are left with the case of three-term vanishing subsums.

Without loss of generality we may assume that the vanishing three-term subsum contains s_1s_6. Thus we distinguish whether s_2s_5 is contained in the vanishing subsum or not. Let us consider the case that s_2s_5 is not contained. Then we have an equation of the from $s_1s_6 = \pm s_i \pm s_j$. Since $s_1 = ab + 1 > 2 \cdot 1 + 1 > 2$ we have $s_1s_6 > 2s_6 > s_i + s_j$ and this case yields no solution.

Therefore both s_1s_6 and s_2s_5 are contained in the same vanishing three-term subsum and we are left with four systems of S-unit equations namely

$$\begin{aligned} s_1s_6 - s_5s_2 &= s_1 \quad \text{and} \quad s_6 = s_5 + s_2\,, \\ s_1s_6 - s_5s_2 &= s_6 \quad \text{and} \quad s_1 = s_5 + s_2\,, \\ s_1s_6 - s_5s_2 &= -s_2 \quad \text{and} \quad s_1 + s_6 = s_5\,, \\ s_1s_6 - s_5s_2 &= -s_5 \quad \text{and} \quad s_1 + s_6 = -s_2\,. \end{aligned} \tag{3}$$

Note that only the first equation of (3) is possible since by assumption $s_1 < s_2 < s_5 < s_6$. Let $y_1 = s_1s_6$, $y_2 = s_5s_2$ and $y_3 = s_1$. Then the S-unit equation

$$y_1 - y_2 = y_3$$

has at most $A(2, r)$ projective solutions $(y_1, y_2, y_3) \in \mathbb{P}^2(\Gamma)$. Note that all solutions that yield S-Diophantine quadruples are non-degenerate, since a vanishing subsum would imply either $s_1s_6 = 0$ or $s_2s_5 = 0$ or $s_1 = 0$. Each projective solution yields only one possibility for s_6. Indeed, assume that (s_1, s_2, s_5, s_6) and (s_1', s_2', s_5', s_6') yield the same projective solution. Then there exists $\rho \in \mathbb{Q}^*$ such that $s_1s_6 = \rho s_1' s_6' = s_1 s_6'$, since $s_1 = \rho s_1'$, i.e. $s_6 = s_6'$. We have now at most $A(2, r)$ possible values for s_6; i.e., we are reduced to at most $A(2, r)$ equations of the form

$$a = s_5 + s_2$$

with $a = s_6 \neq 0$ fixed. Thus, system (3) yields at most $A(2, r)^2$ solutions.

In view of the second statement of Theorem 1 we note that any equation of system (3) cannot have a solution if $2 \notin S$. Otherwise s_6 is odd but $s_5 + s_2$ would be even. In case of $r = 2$, this implies $S = \{2, p\}$ and the equation $s_6 = s_5 + s_2$ turns into

$$2^{\alpha_6} p^{\beta_6} = 2^{\alpha_5} p^{\beta_5} + 2^{\alpha_2} p^{\beta_2}. \tag{4}$$

Considering 2-adic and p-adic valuations, equation (4) reduces to the Diophantine equation

$$2^x - p^y = \pm 1\,.$$

By Mihăilescu's solution of Catalan's equation [11], only $p = 3$ is possible. On the other hand, Szalay and Ziegler [16] showed that no $\{2, 3\}$-Diophantine quadruple exists.

Altogether, we have proved the following result.

Lemma 1. *The first S-unit equation in (2) has at most $A(5, r) + A(2, r)^2$ solutions. If $r = 2$ or $2 \notin S$, then there exist at most $A(5, r)$ solutions.*

Now, we turn to the second equation of system (2). By Lemma 1, the first equation in (2) yields at most $A(5,r)+A(2,r)^2$ or $A(5,r)$ many possibilities for the pair (s_1,s_6) respectively. Thus, we assume that the second equation of system (2) is of the form

$$s_3s_4 - s_3 - s_4 = a \quad \text{with } a \in \mathbb{Q} \text{ fixed.} \tag{5}$$

But S-unit equation (5) has at most $A(3,r)$ solutions provided $a \neq 0$. Indeed no degenerate solution exists since a vanishing subsum on the left side of equation (5) would imply either

- $s_3s_4 = s_3$ and therefore $s_4 = 1$, or
- $s_3s_4 = s_4$ and therefore $s_3 = 1$, or
- $s_3 + s_4 = 0$ and therefore $s_3s_4 < 0$.

Let us note that $a = s_6s_1 - s_6 - s_1 > 2s_6 - s_6 - s_1 > 0$, and therefore we have proved the following lemma.

Lemma 2. *The Diophantine system* (2) *has at most* $(A(5,r) + A(2,r)^2)A(3,r)$ *solutions. If* $r = 2$ *or* $2 \notin S$, *then there exist at most* $A(5,r)A(3,r)$ *solutions.*

In order to prove Theorem 1 it remains to prove that for fixed integers $s_1,\dots,s_6$ there exists at most one quadruple (a,b,c,d). Since

$$a = \sqrt{\frac{(s_1-1)(s_2-1)}{s_4-1}}, \qquad b = \sqrt{\frac{(s_1-1)(s_4-1)}{s_2-1}},$$
$$c = \sqrt{\frac{(s_2-1)(s_4-1)}{s_1-1}}, \qquad d = \sqrt{\frac{(s_5-1)(s_6-1)}{s_4-1}},$$

the proof of Theorem 1 is complete.

3 Proof of Corollary 1

A look through the vast literature on S-unit equations shows that for S-unit equations over the rationals the best result is due to Evertse [5] provided $|S| = 2$ and due to Amoroso and Viada [1] in the general case. Therefore we may assume $A(2,r) = 3\cdot 7^{3+2r}$ and $A(n,r) = (8n)^{4n^4(n+r+1)}$. A look at the proof of the bound for $A(n,r)$ in [1] shows that this bound is derived by the recursive relation

$$A(n,r) \leq 2^n A(n-1,r)B(n,r+1)\,,$$

where $B(n,r) = (8n)^{6n^3(n+r)}$. Note that this recursive estimate already appears in [7]. However, recursively computing $A(n,r)$ we obtain

$$A(3,r) \leq 8\cdot 3\cdot 7^{3+2r}\cdot 24^{162(4+r)} < \exp(2069 + 518.8r)\,.$$

Continuing these computations we arrive at

$$A(5,r) < \exp(25329 + 4616.3r)\,.$$

With these numbers plugged into Theorem 1, we obtain Corollary 1.

Remark 1. Let us note that directly applying the bounds due to Evertse [5] and Amoroso and Viada [1] would yield the slightly worse bound $\exp(73801+15378r)$ for the number of S-Diophantine quadruples. A closer inspection of the computation of the quantity $B(n,r)$ due to Amoroso and Viada [1] and Evertse et al. [7] would further improve the bounds also in view of the new improvements of the Subspace Theorem due to Evertse and Feretti [6]. But we are afraid that the gain is too small for such an effort.

Acknowledgement

We thank the anonymous referee for his valuable suggestions on treating the three--term vanishing subsums in the proof of Theorem 1.

The first author worked on this paper in Fall of 2013 as a long term guest of the Special Semester on Applications of Algebra and Number Theory at the RICAM, Linz, Austria. He thanks Arne Winterhof for the invitation to participate in this program and RICAM for hospitality. The first author was also supported in part by Projects PAPIIT IN104512, CONACyT Mexico-France 193539, CONACyT Mexico-India 163787, and a Marcos Moshinsky Fellowship. The second author was supported by the Austrian Science Fund (FWF) under the project P 24801-N26.

References

[1] F. Amoroso, E. Viada: Small points on subvarieties of a torus. *Duke Math. J.* 150 (3) (2009) 407–442.

[2] Y. Bugeaud, F. Luca: A quantitative lower bound for the greatest prime factor of $(ab+1)(bc+1)(ca+1)$. *Acta Arith.* 114 (3) (2004) 275–294.

[3] P. Corvaja, U. Zannier: On the greatest prime factor of $(ab+1)(ac+1)$. *Proc. Amer. Math. Soc.* 131 (6) (2003) 1705–1709. (electronic)

[4] P. Erdős, P. Turan: On a Problem in the Elementary Theory of Numbers. *Amer. Math. Monthly* 41 (10) (1934) 608–611.

[5] J.-H. Evertse: On equations in S-units, the Thue-Mahler equation. *Invent. Math.* 75 (3) (1984) 561–584.

[6] J.-H. Evertse, R. G. Ferretti: A further improvement of the quantitative subspace theorem. *Ann. of Math. (2)* 177 (2) (2013) 513–590.

[7] J.-H. Evertse, H. P. Schlickewei, W. M. Schmidt: Linear equations in variables which lie in a multiplicative group. *Ann. of Math. (2)* 155 (3) (2002) 807–836.

[8] K. Győry, A. Sárközy, C. L. Stewart: On the number of prime factors of integers of the form $ab+1$. *Acta Arith.* 74 (4) (1996) 365–385.

[9] S. Hernández, F. Luca: On the largest prime factor of $(ab+1)(ac+1)(bc+1)$. *Bol. Soc. Mat. Mexicana (3)* 9 (2) (2003) 235–244.

[10] F. Luca: On the greatest common divisor of $u-1$ and $v-1$ with u and v near S-units. *Monatsh. Math.* 146 (3) (2005) 239–256.

[11] P. Mihăilescu: Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.* 572 (2004) 167–195.

[12] A. Sárközy, C. L. Stewart: On divisors of sums of integers. II. *J. Reine Angew. Math.* 365 (1986) 171–191.

[13] A. Sárközy, C. L. Stewart: On divisors of sums of integers. V. *Pacific J. Math.* 166 (2) (1994) 373–384.

[14] A. Sárközy, C. L. Stewart: On prime factors of integers of the form $ab + 1$. *Publ. Math. Debrecen* 56 (3–4) (2000) 559–573. Dedicated to Professor Kálmán Győry on the occasion of his 60th birthday.

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

[16] L. Szalay, V. Ziegler: S-diophantine quadruples with $S = \{2, q\}$. (in preperation)

[17] L. Szalay, V. Ziegler: On an S-unit variant of Diophantine m-tuples. *Publ. Math. Debrecen* 83 (1–2) (2013) 97–121.

[18] L. Szalay, V. Ziegler: S-diophantine quadruples with two primes congruent 3 modulo 4. *Integers* 13 (2013). Paper No. A80, 9pp.

Authors' addresses:
F. Luca: Mathematical Institute, UNAM Juriquilla, Juriquilla, 76230 Santiago de Querétaro, Querétaro de Arteaga, México, and
School of Mathematics, University of the Witwatersrand, P. O. Box Wits 2050, South Africa

E-mail: `fluca@matmor.unam.mx`

V. Ziegler: Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Altenbergerstr. 69, A-4040 Linz, Austria

E-mail: `volker.ziegler@ricam.oeaw.ac.at`

Received: 3 February, 2014
Accepted for publication: 24 March, 2014
Communicated by: Attila Bérczes