Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Journal of Number Theory 124 (2007) 193–199
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Two S-unit equations with many solutions

S. Konyagin [a], K. Soundararajan [b,*,1,2]

[a] Department of Mathematics and Mechanics, Moscow State University, Moscow 119992, Russia
[b] Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA

Received 20 April 2006

Available online 9 November 2006

Communicated by Michael A. Bennett

Abstract

We show that there exist arbitrarily large sets S of s prime numbers such that the equation $a+b=c$ has more than $\exp(s^{2-\sqrt{2}-\epsilon})$ solutions in coprime integers a, b, c all of whose prime factors lie in the set S. We also show that there exist sets S for which the equation $a+1=c$ has more than $\exp(s^{\frac{1}{16}})$ solutions with all prime factors of a and c lying in S.

1. Introduction

In this note we consider two S-unit equations for which we will exhibit many solutions. Our first problem concerns solutions to the equation $a+b=c$ where a, b, and c are coprime integers such that all prime factors of abc lie in a given set S of s primes. In [8] J.-H. Evertse showed that this S-unit equation has at most $\exp(4s+6)$ solutions. On the other hand, in [7] P. Erdős, C. Stewart, and R. Tijdeman showed that there exist arbitrarily large sets S such that the S-unit equation $a+b=c$ has more than $\exp((4-\epsilon)\sqrt{s/\log s})$ solutions (see also [9] for a refinement of their result). The set S that they exhibited is rather special, and they conjectured that if S

* Corresponding author.
E-mail addresses: konyagin@ok.ru (S. Konyagin), ksound@umich.edu, ksound@math.stanford.edu (K. Soundararajan).
1 The author is partially supported by the National Science Foundation, and by the American Institute of Mathematics (AIM).
2 Current address: Department of Mathematics, Stanford University, 450 Serra Mall Bldg. 380, Stanford, CA 94305-2125, USA.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.07.017

were the set of the first s prime numbers then there should be $\gg \exp(s^{\frac{2}{3}-\epsilon})$ solutions to the S-unit equation. Moreover, for any set S they conjectured that there are $\ll \exp(s^{\frac{2}{3}+\epsilon})$ solutions. We remark that recently J. Lagarias and K. Soundararajan [12] have shown that if S is the set of the first s prime numbers and the Generalized Riemann Hypothesis is true then the S-unit equation has $\gg \exp(s^{\frac{1}{8}-\epsilon})$ solutions. Our first result improves the construction of Erdős, Stewart, and Tijdeman and shows the existence of arbitrarily large sets S with more than $\exp(s^{2-\sqrt{2}-\epsilon})$ solutions.

Theorem 1. *Let β be any positive number with $\beta < 2 - \sqrt{2}$. There exist arbitrarily large sets S of s prime numbers such that the S-unit equation $a + b = c$ has at least $\exp(s^{\beta})$ solutions in coprime integers a, b and c having all their prime factors from S.*

The second S-unit equation that we will consider is a special case of the first: namely, the equation $a + 1 = c$ with all prime factors of ac lying in the set S. Although this is a much more restrictive equation than our first, we are able to find arbitrarily large sets S with many solutions to this equation.

Theorem 2. *There exist arbitrarily large sets S of s prime numbers such that the equation $a + 1 = c$ has at least $\exp(s^{\frac{1}{16}})$ solutions where all prime factors of ac lie in S. In fact, there exist arbitrarily large integers N such that*

$$\#\{d\colon\ d(d+1) \mid N\} \geqslant \exp\bigl((\log N)^{\frac{1}{16}}\bigr).$$

The second, stronger, conclusion of Theorem 2 advances a line of inquiry initiated by Erdős and R.R. Hall [5]. They showed the existence of arbitrarily large numbers N with $\#\{d\colon\ d(d+1) \mid N\} \gg (\log N)^{\sqrt{e}-\epsilon}$. From the work of A. Hildebrand [10] on consecutive smooth numbers it follows that there are large N with $\#\{d\colon\ d(d+1) \mid N\} \gg (\log N)^{A}$ for any given positive number A. In [1] A. Balog, Erdős, and G. Tenenbaum quantified this and obtained large N with $\#\{d\colon\ d(d+1) \mid N\} \gg (\log N)^{\log_3 N/9\log_4 N}$ where $\log_3$ and $\log_4$ denote the third and fourth iterated logarithms. For upper bounds on the quantity $\#\{d\colon\ d(d+1) \mid N\}$ we refer the reader to [3,4], and [6].

There are at least $x^{\frac{1+\delta}{2+\delta}+o(1)} = x^{\frac{1}{2}+\frac{1}{4+2\delta}+o(1)}$ square-free numbers below x all of whose prime factors lie below $(\log x)^{2+\delta}$. If these numbers were randomly distributed then we would expect to find about $x^{\frac{1}{2+\delta}+o(1)}$ pairs of such consecutive numbers. This suggests that there should be arbitrarily large N with $\#\{d\colon\ d(d+1) \mid N\} \geqslant \exp((\log N)^{\frac{1}{2}-\epsilon})$. We venture the guess that for any set S, the S-unit equation $a + 1 = c$ has no more than $\exp(s^{\frac{1}{2}+\epsilon})$ solutions, but nothing substantially better than Evertse's bound appears to be known.

2. Proof of Theorem 1

Let y be a large real number and let β and γ be real numbers in $(0, 1)$. Consider the set $\mathcal{L}$ which consists of square-free numbers ℓ having exactly $[y^{\beta}]$ prime factors each from the interval $[y/2, y]$. Consider also the set $\mathcal{M}$ which contains square-free numbers m having exactly $[\gamma y^{\beta}]$

prime factors each from the interval $[y/4, y/2)$. Note that the elements of $\mathcal{L}$ are coprime to elements of $\mathcal{M}$. Further note that

$$|\mathcal{L}| = \binom{\pi(y) - \pi(y/2)}{[y^\beta]} = L^{1-\beta+o(1)},$$

where $L = y^{[y^\beta]}$, and similarly

$$|\mathcal{M}| = L^{\gamma(1-\beta)+o(1)}.$$

Pick a number $m \in \mathcal{M}$ and let $r(\mathcal{L}; a, m)$ denote the number of elements of $\mathcal{L}$ lying in the residue class $a \pmod m$. By Cauchy–Schwarz we know that

$$\sum_{a=1}^{m} r(\mathcal{L}; a, m)^2 \geqslant \frac{1}{m}\left(\sum_{a=1}^{m} r(\mathcal{L}; a, m)\right)^2 = \frac{|\mathcal{L}|^2}{m}.$$

The left-hand side counts the pairs (ℓ_1, ℓ_2) with $\ell_1 \equiv \ell_2 \pmod m$. This congruence has $|\mathcal{L}|$ trivial solutions, and if $m < |\mathcal{L}|/2$ then we are guaranteed $\gg |\mathcal{L}|^2/m$ non-trivial solutions. Since each element of $\mathcal{M}$ is below $y^{[\gamma y^\beta]} \leqslant yL^\gamma$ we conclude that if $\gamma < 1 - \beta$ then there exist $\gg L^{2(1-\beta)-\gamma+o(1)}$ non-trivial pairs (ℓ_1, ℓ_2) with $\ell_1 \equiv \ell_2 \pmod m$. Therefore, if $\gamma < 1 - \beta$ there exist $\gg L^{2(1-\beta)-\beta\gamma+o(1)}$ triples (m, ℓ_1, ℓ_2) with $m \in \mathcal{M}$, $\ell_1 \neq \ell_2 \in \mathcal{L}$ and $\ell_1 \equiv \ell_2 \pmod m$.

Suppose below that $\gamma < 1 - \beta$ and consider the ratios $(\ell_1 - \ell_2)/m$ arising from the triples produced above. Restricting to positive ratios, we have produced $\gg L^{2(1-\beta)-\beta\gamma+o(1)}$ such ratios, all below $L^{1-\gamma+o(1)}$. Therefore if $2(1-\beta) - \beta\gamma > 1 - \gamma$ then we can find a popular number $u \leqslant L^{1-\gamma+o(1)}$ which occurs as a ratio more than $L^{2(1-\beta)-\beta\gamma+\gamma-1+o(1)}$ times.

Summarizing, we see that if $\gamma < 1 - \beta$ and $(2+\gamma)(1-\beta) > 1$ then there is a number $u \leqslant L^{1-\gamma+o(1)}$ such that the equation $\ell_1 = \ell_2 + mu$ has more than $L^{(2+\gamma)(1-\beta)-1+o(1)}$ solutions in integers $\ell_1 \neq \ell_2 \in \mathcal{L}$ and $m \in \mathcal{M}$. We already know that ℓ_1 and ℓ_2 are coprime to m, so if ℓ_1 and ℓ_2 have a common factor then it must be a divisor of u. Since there are at most $L^{o(1)}$ divisors of u, after removing common factors, we find that for some divisor v of u, the equation $\ell_1 = \ell_2 + vm$ has $\gg L^{(2+\gamma)(1-\beta)-1+o(1)}$ solutions in coprime integers $\ell_1, \ell_2 \in \mathcal{L}$, and $m \in \mathcal{M}$. Take S to be the set of all primes in $[y/4, y]$ union the prime factors of v. Then $|S| \leqslant \pi(y) - \pi(y/4) + \log v \leqslant y$, and we have exhibited more than $\exp(y^\beta)$ solutions to this S-unit equation. If $\beta < 2 - \sqrt{2}$ then we can find a γ satisfying the conditions $\gamma < 1 - \beta$ and $(2+\gamma)(1-\beta) > 1$, and so Theorem 1 follows.

3. Proof of Theorem 2

Throughout we let y be a large real number. We need first the following zero-density result which may be found in [11] (see the Grand Density Theorem 10.4 on p. 260).

Lemma 3.1. *There exists a constant $C > 0$ such that for any $\frac{1}{2} \leqslant \alpha < 1$ the region*

$$\mathcal{R}(\alpha, y) := \{s\colon \operatorname{Re}(s) \geqslant \alpha,\ |\operatorname{Im}(s)| \leqslant y\},$$

contains at most $(Q^2 y)^{C(1-\alpha)+o(1)}$ zeros of primitive Dirichlet L-functions with conductor below Q. It is permissible to take $C = \frac{12}{5}$.

Proposition 3.2. *Let β be a real number with $0 < \beta < 1 - 3C(1-\alpha)$. Let $K = [y^\beta]$ and put $Z = y^K$. There exist $\gg Z^{1-\beta+o(1)}$ square-free numbers q having exactly K prime factors each from the interval $[y/2, y]$, and such that for every non-trivial character* (mod q) *the corresponding L-function has no zeros in $\mathcal{R}(\alpha, y)$.*

Proof. Clearly there are $\binom{\pi(y)-\pi(y/2)}{K}$ square-free integers q having exactly K prime factors each from the interval $[y/2, y]$. We must exclude those moduli for which there exists a non-trivial character whose L-function has a zero in $\mathcal{R}(\alpha, y)$. A bad modulus q must be divisible by some number d with j prime factors (so $(y/2)^j \leqslant d \leqslant y^j$ and $1 \leqslant j \leqslant K$) such that there is a primitive character mod d whose L-function has a zero in $\mathcal{R}(\alpha, y)$. By Lemma 3.1 there are at most $y^{(2j+1)(C(1-\alpha)+o(1))}$ possibilities for d. Given a d there are at most $\binom{\pi(y)-\pi(y/2)}{K-j}$ multiples of d that must be excluded. Thus we must exclude at most

$$\sum_{j=1}^{K} y^{(2j+1)(C(1-\alpha)+\epsilon)} \binom{\pi(y)-\pi(y/2)}{K-j}$$

moduli. Since $\beta < 1 - 3(1-\alpha)$ this is small compared to $\binom{\pi(y)-\pi(y/2)}{K}$ and so we have $\gg \binom{\pi(y)-\pi(y/2)}{K} = Z^{1-\beta+o(1)}$ suitable moduli q. $\square$

Proposition 3.3. *Let $X = Z^\gamma$ and suppose that $\gamma(1-\alpha-\beta) > 1$. Let q be one of the moduli produced in Proposition* 3.2. *Then there are $\gg Z^{(1-\beta)\gamma-1+o(1)}$ integers $\ell \leqslant X$ with each ℓ being square-free, divisible only by primes below y, and $\ell \equiv 1$* (mod q).

Assuming this proposition for the moment we show how to deduce Theorem 2.

Proof of Theorem 2. Let α, β, and γ be as in Lemma 3.1, Propositions 3.2 and 3.3. That is

$$\frac{1}{2} \leqslant \alpha < 1, \qquad 0 < \beta < 1 - 3C(1-\alpha), \quad \text{and} \quad \gamma(1-\alpha-\beta) > 1. \tag{3.1}$$

By Propositions 3.2 and 3.3 we know that there are at least $Z^{(1-\beta)(1+\gamma)-1+o(1)}$ pairs (ℓ, q) satisfying the conclusions of those propositions. Consider the ratio $(\ell-1)/q$ which is an integer which lies below $2^K X/Z < Z^{\gamma-1+o(1)}$. If

$$(1-\beta)(1+\gamma) - 1 > \gamma - 1, \tag{3.2}$$

then there is a popular value m which occurs as the ratio $(\ell-1)/q$ at least $Z^{1-\beta-\beta\gamma+o(1)}$ times. Take $N = m\prod_{p\leqslant y} p$ and note that if $(\ell-1)/q = m$ then qm and $\ell = qm+1$ are consecutive divisors of N. Therefore

$$\#\{d\colon d(d+1) \mid N\} \geqslant Z^{1-\beta-\beta\gamma+o(1)} \geqslant \exp\bigl((\log N)^\beta\bigr),$$

since by the prime number theorem $N = e^{y+o(y)}$, and $\log Z = (1+o(1))y^\beta \log y$.

To complete the proof we need only find the largest β for which (3.1) and (3.2) hold. A little calculation shows that it is best to take γ slightly larger than $3C + \sqrt{9C^2+3C}$, take $\alpha = 1 - \frac{1+1/\gamma}{3C+1}$, and β is then slightly smaller than $(1+3C+\sqrt{9C^2+3C})^{-1}$. Since $C = \frac{12}{5}$ is permissible we conclude that $\beta = \frac{1}{16}$ is allowed. $\square$

It remains finally to prove Proposition 3.3. To this end we require the following lemma.

Lemma 3.4. *Let $q \leqslant Z$ be one of the moduli produced in Proposition* 3.2 *so that $L(s,\chi)$ has no zeros in the region $\mathcal{R}(\alpha, y)$, and suppose that $\beta < 1-\alpha$. For any complex number s with* $\mathrm{Re}(s) > 0$ *we define*

$$F(s,\chi;y) = \sum_{\substack{\ell=1\\ p|\ell \Rightarrow p\leqslant y}}^{\infty} \frac{\mu(\ell)^2\chi(\ell)}{\ell^s} = \prod_{p\leqslant y}\left(1+\frac{\chi(p)}{p^s}\right).$$

For any $\epsilon > 0$, if $|t| \leqslant y/2$ then we have

$$\left|F(\alpha+\epsilon+it,\chi;y)\right| \ll_\epsilon (qy)^\epsilon,$$

while if $|t| > y/2$ we have

$$\left|F(\alpha+\epsilon+it,\chi;y)\right| \ll \exp\bigl(y^{1-\alpha}\bigr).$$

Proof. Taking logarithms it suffices to estimate $\sum_{p\leqslant y}\chi(p)p^{-\alpha-\epsilon-it}$. Since $\alpha < 1$ this is trivially $\leqslant y^{1-\alpha}$ and the second assertion follows.

If $z \leqslant y$ then note that

$$\begin{aligned}\sum_{n\leqslant z}\Lambda(n)\chi(n)n^{-it} &= \frac{1}{2\pi i}\int_{1+\frac{1}{\log y}-i\infty}^{1+\frac{1}{\log y}+i\infty} -\frac{L'}{L}(w+it,\chi)\frac{z^w}{w}\,dw\\ &= -\sum_{\substack{\rho\\ |\rho-it|\leqslant z/2}}\frac{z^{\rho-it}}{\rho-it} + O\bigl(\log^2 qy\bigr),\end{aligned}$$

by following closely the standard argument in prime number theory leading to the 'explicit formula' for primes (see for example H. Davenport [2]); here ρ runs over non-trivial zeros of $L(s,\chi)$. By assumption $\mathrm{Re}(\rho) \leqslant \alpha$ for each zero counted in our sum. Since there are $\ll \log qy$ zeros in each interval $k \leqslant |\rho - it| \leqslant k+1$ for $0 \leqslant k \leqslant y$ we conclude that

$$\sum_{n\leqslant z}\Lambda(n)\chi(n)n^{-it} \ll z^\alpha \log(qy)\log z + \log^2(qy) \ll z^\alpha\log(qy)\log z.$$

Trivially we also have that this sum is bounded by $\ll z$. Using these two estimates and partial summation we easily deduce that

$$\sum_{2\leqslant n\leqslant z}\frac{\Lambda(n)\chi(n)}{n^{\alpha+\epsilon+it}\log n} \ll (\log qy)^{1-\frac{\epsilon}{1-\alpha}}.$$

This proves the lemma. $\square$

Proof of Proposition 3.3. Using the orthogonality of characters (mod q) we see that

$$\sum_{\substack{\ell\equiv 1 \ (\mathrm{mod}\, q)\\ p|\ell\Rightarrow p\leqslant y}} \mu(\ell)^2 e^{-\ell/x} = \frac{1}{\phi(q)} \sum_{\substack{(\ell,q)=1\\ p|\ell\Rightarrow p\leqslant y}} e^{-\ell/x} + \frac{1}{\phi(q)} \sum_{\substack{\chi \ (\mathrm{mod}\, q)\\ \chi\neq\chi_0}} \sum_{p|\ell\Rightarrow p\leqslant y} \chi(\ell)\mu(\ell)^2 e^{-\ell/x}. \tag{3.3}$$

We now obtain an upper bound for the contribution from non-trivial characters to (3.3). For any $c > 0$ we have

$$\sum_{p|\ell\Rightarrow p\leqslant y} \chi(\ell)\mu(\ell)^2 e^{-\ell/x} = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} F(s,\chi;y)x^s \Gamma(s)\, ds.$$

We take $c = \alpha + \epsilon$ and estimate the integral using Lemma 3.4. Since $|\Gamma(c+it)|$ decays exponentially in $|t|$ by Stirling's formula, we obtain that the above is $\ll x^{\alpha+\epsilon}(qy)^{\epsilon}$. Thus we conclude that

$$\sum_{\substack{\ell\equiv 1 \ (\mathrm{mod}\, q)\\ p|\ell\Rightarrow p\leqslant y}} \mu(\ell)^2 e^{-\ell/x} = \frac{1}{\phi(q)} \sum_{\substack{(\ell,q)=1\\ p|\ell\Rightarrow p\leqslant y}} e^{-\ell/x} + O\big(x^{\alpha+\epsilon}(qy)^{\epsilon}\big). \tag{3.4}$$

We take $x = X/\log X$ in (3.4) and note that

$$\sum_{\substack{\ell\leqslant X\\ \ell\equiv 1 \ (\mathrm{mod}\, q)\\ p|\ell\Rightarrow p\leqslant y}} \mu(\ell)^2 \geqslant \sum_{\substack{\ell\equiv 1 \ (\mathrm{mod}\, q)\\ p|\ell\Rightarrow p\leqslant y}} \mu(\ell)^2 e^{-\ell/x} + O(1).$$

Now

$$\sum_{\substack{(\ell,q)=1\\ p|\ell\Rightarrow p\leqslant y}} \mu(\ell)^2 e^{-\ell/x} \gg \sum_{\substack{\ell\leqslant x\\ (\ell,q)=1\\ p|\ell\Rightarrow p\leqslant y}} \mu(\ell)^2 \geqslant \binom{\pi(y)-\omega(q)}{[\log x/\log y]} = Z^{\gamma(1-\beta)+o(1)}.$$

Using (3.4), and recalling that $q \leqslant Z$ and the hypothesis that $\gamma(1-\beta) - 1 > \gamma\alpha$, we obtain (choosing ϵ small enough) the proposition. □

Acknowledgments

This work was completed when both authors were visiting the Centre de Rechereches Mathématiques (CRM) in Montréal. We are grateful to the CRM for their support and excellent working conditions. We are also grateful to Antal Balog and Andrew Granville for their interest and encouragement.

References

[1] A. Balog, P. Erdős, G. Tenenbaum, On arithmetic functions involving consecutive integers, in: B.C. Berndt, et al. (Eds.), Analytic Number Theory, Proc. Conf. in Honor of Paul T. Bateman, Birkhäuser, 1990, pp. 77–90.

[2] H. Davenport, Multiplicative Number Theory, Springer Grad. Texts in Math., vol. 74, 2000.

[3] R. de la Bretèche, Sur une classe de fonctions arithmétiques liées aux diviseurs d'un entier, Indag. Math. 11 (2000) 437–452.

[4] R. de la Bretèche, Nombre de valeurs polynomiales qui divisant un entier, Math. Proc. Cambridge Philos. Soc. 131 (2001) 193–209.

[5] P. Erdős, R.R. Hall, On some unconventional problems on the divisors of integers, J. Aust. Math. Soc. 25 (1978) 479–485.

[6] P. Erdős, G. Tenenbaum, Sur les fonctions arithmétiques liées aux diviseurs consécutifs, J. Number Theory 31 (1989) 285–311.

[7] P. Erdős, C. Stewart, R. Tijdeman, Some Diophantine equations with many solutions, Compos. Math. 66 (1988) 37–56.

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

[9] A. Granville, On pairs of coprime integers with no large prime factors, Expo. Math. 9 (1991) 335–350.

[10] A. Hildebrand, On a conjecture of A. Balog, Proc. Amer. Math. Soc. 95 (1985) 517–523.

[11] H. Iwaniec, E. Kowalski, Analytic Number Theory, Amer. Math. Soc. Colloq. Publ., vol. 53, 2004.

[12] J. Lagarias, K. Soundararajan, Smooth solutions to the equation $a + b = c$, preprint.