Taylor & Francis
Taylor & Francis Group

Experimental Mathematics

ISSN: 1058-6458 (Print) 1944-950X (Online) Journal homepage: https://www.tandfonline.com/loi/uexm20

On Toric Orbits in the Affine Sieve

Alex Kontorovich & Jeffrey Lagarias

To cite this article: Alex Kontorovich & Jeffrey Lagarias (2019): On Toric Orbits in the Affine Sieve, Experimental Mathematics, DOI: 10.1080/10586458.2019.1616337

To link to this article: https://doi.org/10.1080/10586458.2019.1616337

Published online: 19 Jun 2019.

EXPERIMENTAL MATHEMATICS
https://doi.org/10.1080/10586458.2019.1616337

Taylor & Francis
Taylor & Francis Group

On Toric Orbits in the Affine Sieve

Alex Kontorovich[a,b] and Jeffrey Lagarias[c]

[a]Department of Mathematics, Rutgers University, New Brunswick, NJ, USA; [b]Institute for Advanced Study, Princeton, NJ, USA; [c]Department of Mathematics, University of Michigan, Ann Arbor, MI, USA

ABSTRACT
We give a detailed analysis of a probabilistic heuristic model for the failure of "saturation" in instances of the Affine Sieve having toral Zariski closure. Based on this model, we formulate precise conjectures on several classical problems of arithmetic interest and test these against empirical data.

KEYWORDS
affine sieve; prime factors; Fibonacci numbers; Lucas numbers; Mersenne primes

1. Introduction

The Fundamental Theorem of the Affine Sieve, introduced by [Bourgain et al. 10] and proved by [Salehi Golsefidy-Sarnak 13] extends the Brun sieve to orbits of affine-linear group actions. The goal of this article is to study the behavior of prime factors of orbits outside the scope of this theorem.

More precisely, let $\Gamma < \mathrm{GL}_N(\mathbb{Q})$ be a finitely generated group, that is, $\Gamma = \langle A_1, A_2, \ldots, A_k \rangle$, fix a base point $\mathbf{v}_0 \in \mathbb{Q}^N$, and let

$$\mathcal{O} := \Gamma \cdot \mathbf{v}_0 \subset \mathbb{Z}^N$$

be the orbit of $\mathbf{v}_0$ under Γ, assumed to be integral.[1] Let $\Omega(n)$ denote the number of primes dividing an integer n, counted with multiplicity. Given $R \geq 1$, an integer n with $\Omega(n) \leq R$ is called R-almost prime. Fix a polynomial $f(x_1, x_2, \ldots, x_N) \in \mathbb{Q}[x_1, \ldots, x_N]$ taking integer values on $\mathcal{O}$, and let

$$\mathcal{O}_R := \{\mathbf{v} \in \mathcal{O} : \Omega(f(\mathbf{v})) \leq R\}$$

be the points in $\mathcal{O}$ taking R-almost prime values under f. The pair $(\mathcal{O}, f)$ is said to *saturate* if there exists some $R < \infty$ so that

$$\mathrm{Zcl}(\mathcal{O}_R) = \mathrm{Zcl}(\mathcal{O}). \tag{1–1}$$

Here, Zcl refers to Zariski closure in affine space.[2] The *saturation number* is the least R for which (1–1) holds; this can be determined exactly or at least well-approximated in some special instances, see [Kontorovich 14] for more discussion. Let $V(f)$ be the affine $\mathbb{Q}$-variety given by $f = 0$. In general, we assume that f is non-constant on (any irreducible component of) $\mathrm{Zcl}(\mathcal{O})$. This is equivalent to

$$\dim\big(V(f) \cap \mathrm{Zcl}(\mathcal{O})\big) < \dim \mathrm{Zcl}(\mathcal{O}), \tag{1–2}$$

viewing the Zariski closure $\mathrm{Zcl}(\mathcal{O})$ inside $\mathbb{C}^N$. Then, the fundamental theorem of [Salehi Golsefidy and Sarnak 13, Theorem 1] states the following.

Theorem 1.1 ([Salehi Golsefidy and Sarnak 13]). *Let Γ be a finitely generated subgroup of $GL_N(\mathbb{Q})$ having Zariski closure $\mathbb{G} = \mathrm{Zcl}(\Gamma)$ in $GL_N(\mathbb{C})$. Let $\mathbf{v}_0 \in \mathbb{Q}^N$ and let $\mathcal{O} = \Gamma \mathbf{v}_0 \subset \mathbb{Z}^N$ be the Γ-orbit of $\mathbf{v}_0$. Suppose that $f(x) \in \mathbb{Q}[x_1, \ldots, x_N]$ is such that $f(\mathcal{O}) \subset \mathbb{Z}$ and (1–2) is satisfied.[3] Then the pair $(\mathcal{O}, f)$ saturates, as long as no algebraic torus[4] is a homomorphic image of the connected component $\mathbb{G}_0$ of the identity of $\mathbb{G}$.*

CONTACT Alex Kontorovich alex.kontorovich@rutgers.edu Department of Mathematics, Rutgers University, New Brunswick, NJ 08901-8554, USA.

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/uexm.

[1]One can work more generally with entries in the ring of S-integers $\mathbb{Z}_S$, but we restrict to $\mathbb{Z}$ for ease of exposition. Note that there exist $\Gamma < \mathrm{GL}_N(\mathbb{Q})$ for which no vector $\mathbf{v}_0 \neq (0, \ldots, 0)$ gives an integral orbit, e.g., $\Gamma = \langle A \rangle$ with $A = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$.

[2]Recall that this Zariski closure can be thought of as the common zero set of all polynomials $p(x_1, x_2, \ldots, x_N) \in \mathbb{C}[x_1, \ldots, x_N]$ inside affine space $\mathbb{A}^N(\mathbb{C}) = \mathbb{C}^N$ that vanish on $\mathcal{O}$.

[3]We need not assume any restriction on the orbit like "primitivity" (that the $\gcd(f(\mathcal{O})) = 1$) since the fixed prime factors, if any, can be accounted for in the value of R.

[4]For example, $(\mathbb{C}^\times)^n$.

In [Salehi Golsefidy and Sarnak 13, Appendix], Salehi Golsefidy-Sarnak gave a heuristic argument, based on the Borel-Cantelli lemma, that the condition of having no tori is necessary in certain cases. Their model considered an algebraic torus (i.e., Γ is a free abelian group of rank D with generators $A_1, \ldots, A_D \in \mathrm{GL}_N(\mathbb{Z})$, and there is a $g \in \mathrm{GL}_N(\mathbb{C})$ so that for all j, the matrices gA_jg^{-1} are diagonal) and the test polynomial $f(x_{1,1}, \ldots, x_{N,N}) = \prod_{j=1}^{k} f_j(\mathbf{x})$, with $f_j(\mathbf{x}) = j + \sum_{m,n=1}^{N} x_{m,n}^2$. This test polynomial f has (at least) k irreducible factors over $\mathbb{Q}[x_{1,1}, \ldots x_{N,N}]$, all of the same degree (so they have roughly the same "size" on points of $\mathcal{O}$). Their heuristic was that the prime factorizations of the k elements $f_j(\mathbf{x})$ evaluated at a point $\mathbf{x} \in \mathcal{O}$ ought to be "independent," at least at the level of the number of prime factors, $\Omega(f_j(\mathbf{x}))$, since they are just integer shifts of each other.

In this article, we refine this heuristic and make precise predictions on the failure of saturation in the toric case, which we then test empirically in a number of natural settings of classical interest.

1.1. Main probabilistic model

We model the values of the k irreducible factors of f as k randomly and independently chosen integers in an exponentially growing interval, depending on a parameter n. The parameter n is to be viewed as modeling elements of a toral orbit, which grow exponentially.

Theorem 1.2. *Let $k \geq 1$ be a fixed integer. Fix a constant $C > 1$ and for each $n \geq 1$, draw an integer vector*

$$(x_{1,n}, x_{2,n}, \ldots, x_{k,n}) \in [1, C^n]^k$$

with uniform distribution. Then with probability one,

$$\liminf_{n \geq 1} \frac{\Omega(x_{1,n} \cdot x_{2,n} \cdots x_{k,n})}{\log n} = \beta_k, \tag{1–3}$$

where β_k denotes the unique solution in $[0, k-1]$ to

$$\beta_k(1 - \log \beta_k + \log k) = k-1, \tag{1–4}$$

with $\beta_1 = 0$ and $\beta_k > 0$ for $k \geq 2$.

The constants β_k are absolute, in particular, independent of C. The first few values of β_k are

$$\beta_2 = 0.373365, \beta_3 = 0.913728, \beta_4 = 1.52961,$$
$$\beta_5 = 2.19252, \ldots, \beta_{10} = 5.8754, \ldots$$

Note that the expected size[5] of $\Omega(m)$ for a random integer m is $\log \log m$, and of course

$$\Omega(x_{1,n} \cdot x_{2,n} \cdots x_{k,n}) = \sum_j \Omega(x_{j,n}),$$

whence the expected size of this sum is $k \log \log C^n \sim k \log n$. Thus, we may interpret (1–3) as showing that, up to a multiplicative constant k/β_k, one never sees (asymptotically) a deficient number of prime factors.

To test the validity of this model empirically, it will be useful to understand how large n should be to experimentally observe the behavior (1–3). Naively we may expect from this equation that the largest $\mathfrak{n} = n_{\max}$ for which $x_{1,n} \cdots x_{k,n}$ is R-almost prime satisfies:

$$\frac{R}{\log \mathfrak{n}} \approx \beta_k,$$

or

$$\mathfrak{n} \approx \exp(R/\beta_k). \tag{1–5}$$

It turns out that the probabilistic model sometimes makes a different prediction.

Theorem 1.3. *Fix $k \geq 2$, $C > 1$, and for each $n \geq 1$, draw a vector*

$$\mathbf{x}_n = (x_{1,n}, x_{2,n}, \ldots, x_{k,n}) \in [1, C^n]^k$$

uniformly. Let $\mathcal{X} = (\mathbf{x}_1, \mathbf{x}_2, \ldots)$ be a random variable consisting of a sequence of independent such draws, one for each n. For any fixed $R \geq k$, consider the random variable

$$\mathfrak{n} = \mathfrak{n}(R; \mathcal{X}) := \max\{n : \Omega(x_{1,n} \cdots x_{k,n}) \leq R\},$$

with $\mathfrak{n} = 0$ if there are no such n, and $\mathfrak{n} = \infty$ if the event occurs infinitely often. Then

(1) with probability one,

$$\mathfrak{n} < \infty, \tag{1–6}$$

and moreover,

(2) for all $m \geq k-1$, the m-th moment of $\mathfrak{n}$ diverges,

$$\mathbb{E}[\mathfrak{n}^m] = \infty. \tag{1–7}$$

Remark 1. In the case $k = 1$ not covered in Theorem 1.3, one has instead that with probability one, $\mathfrak{n} = +\infty$.

[5]For example, in the normal order sense of the [Hardy and Ramanujan 17] theorem, further refined in the Erdős-Kac theorem.

Remark 2. In many natural examples treated below we have $k=2$, where Theorem 1.3 for $m=1$ asserts the expected value of $\mathfrak{n}(R)$ is infinite for all $R \geq 2$. In such examples, one should not expect $\mathfrak{n}(R)$ to behave nicely like $\exp(R/\beta_2)$, as suggested naively by (1–5). One may interpret the infinite expected value as saying that for $k=2$ there may exist extremely large "sporadic" solutions to $\Omega(x_{1,n}, \ldots, x_{k,n}) = R$.

Remark 3. The proofs of Theorems 1.2 and 1.3 apply and give the same result in the more general case of $\mathbf{x}_n$ chosen from non-identically growing intervals, that is $(x_{1,n}, \ldots, x_{k,n}) \in [1, C_1^n] \times [1, C_2^n] \cdots \times [1, C_k^n]$, for fixed constants $C_1, \ldots, C_k > 1$.

1.2. The Toral Affine Sieve Conjecture

The probabilistic model above motivates a heuristic prediction concerning the number of prime factors of certain sequences associated with toric orbits, namely the (rank one) "Toral Affine Sieve Conjecture" stated below. We will derive as consequences of this conjecture other predictions in several settings of classical interest.

Conjecture 1.1. (Toral Affine Sieve Conjecture). *Let $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ be a hyperbolic matrix, that is, one having two distinct real eigenvalues; equivalently*

$$\mathrm{tr}(\gamma)^2 - 4\det(\gamma) > 0.$$

Let $\Gamma = \langle \gamma \rangle^+ := \{\gamma^n : n \geq 0\}$ be the semigroup generated by γ, and suppose that $\mathbf{v}_0 \in \mathbb{Q}^2 \setminus (0,0)$ is a non-zero vector such that the orbit $\mathcal{O} := \Gamma \cdot \mathbf{v}_0 \subset \mathbb{Z}^2$ is integral and infinite. Then

$$\liminf_{(x,y)\in\mathcal{O}} \frac{\Omega(xy)}{\log\log|xy|} \geq \beta_2 \approx 0.373365. \qquad (1\text{–}8)$$

Since the Zariski closure of Γ in $GL(2,\mathbb{C})$ is an algebraic torus, and since the orbit $\mathcal{O}$ is assumed to be infinite, it is a one-dimensional torus, so it follows that the Zariski closure of $\mathcal{O}$ in $\mathbb{C}^2$ has $\dim(\mathrm{Zcl}(\mathcal{O})) = 1$ in (1–2). We have taken the test function $f(x,y) = xy$, whence $V(f) \cap \mathrm{Zcl}(\mathcal{O})$ is finite, having dimension 0. The points in $(x_n, y_n) := \gamma^n \mathbf{v}_0 \in \mathcal{O}$ grow exponentially, that is, there are $C > c > 1$ so that

$$c^n < |x_n y_n| = |f(\gamma^n \mathbf{v}_0)| < C^n.$$

In consequence, the factor $\log\log|xy|$ in (1–8) can be replaced by $\log n$, that is, (1–8) is equivalent to

$$\liminf_{n\to\infty} \frac{\Omega(x_n y_n)}{\log n} \geq \beta_2.$$

The conjecture is based on applying the model of Theorem 1.2 with $k=2$ having two "independent" factors (x_n, y_n) for $f(\gamma^n \mathbf{v}_0)$. In the "generic" situation, we might have equality in these limits. However, there are cases of orbits whose limiting values involve β_k for larger k, see the examples in §2.

Remark 4. We did not need to assume in Conjecture 1.1 any coprimality condition (e.g., $\gcd(\mathcal{O}) = 1$) on the orbit. Indeed, if all entries of $\mathbf{v} = (x,y) \in \mathcal{O}$ have a common factor, then this factor, divided by $\log\log|xy|$, is irrelevant in the lim inf in (1–8).

1.3. Consequences

The basic Conjecture 1.1 implies other striking predictions, of which we present two below; The first applies to integer points on affine quadrics, and the second applies to the continued fraction convergents of quadratic surds.

Theorem 1.4. *Let $Q(x,y) = Ax^2 + Bxy + Cy^2$ be an indefinite (i.e., $D = B^2 - 4AC$ is positive), non-degenerate (D is not a square) binary quadratic form over $\mathbb{Z}$. Fix a square-free $t \in \mathbb{Z}$ so that the set $V(\mathbb{Z})$ of $\mathbb{Z}$ points of the affine quadric $V = V_{Q,t}$ given by*

$$V : Q(x,y) = t$$

is non-empty. Then, assuming Conjecture 1.1,

$$\liminf_{\substack{(x,y)\in V(\mathbb{Z}) \\ |xy|\to\infty}} \frac{\Omega(xy)}{\log\log|xy|} \geq \beta_2.$$

Theorem 1.5. *Let α be a real quadratic irrational, and let p_n/q_n denote the n-th convergent of its ordinary continued fraction expansion. Then, assuming Conjecture 1.1,*

$$\liminf_{n} \frac{\Omega(p_n q_n)}{\log n} \geq \beta_2.$$

These two theorems will not be surprising to experts, but the (conditional) conclusions, particularly the appearance of the precise number $\beta_2 \approx 0.373365$, are unexpected.

1.4. Organization

In §2, we give a number of illustrative examples and numerics which, one may argue, provide support for the heuristic provided by the probabilistic model in the context of Conjecture 1.1. We prove Theorem 1.2 in §3, followed by Theorem 1.3 in §4. In the final §5, we sketch proofs of Theorems 1.4 and 1.5.

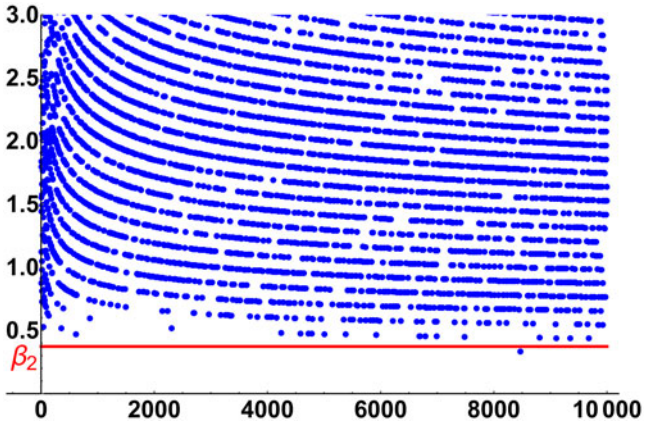

Figure 1. A plot of $n < 10\ 000$ vs. $\Omega(F_nL_n)/\log\log(F_nL_n)$. Also shown is the horizontal line $y = \beta_2 \approx 0.37$.

1.5. Notation

We use the following standard notation. We use the symbol $f \sim g$ to mean $f/g \to 1$. The symbols $f \ll g$ and $f = O(g)$ are used interchangeably to mean the existence of an implied constant $C > 0$ so that $f(x) \leq Cg(x)$ holds for all $x > C$; moreover $f \asymp g$ means $f \ll g \ll f$. Unless otherwise specified, implied constants depend at most on k, which is treated as fixed. The letter $\varepsilon > 0$ is an arbitrarily small constant, not necessarily the same at each occurrence. The Gamma function is denoted $\Gamma(z)$, and a product $\prod_p$ denotes a product over primes. The floor function, $\lfloor \cdot \rfloor$, returns the largest integer not exceeding its argument.

2. Examples and numerics

It should be clear that running decent numerics to test Conjecture 1.1 is a daunting task. Indeed, toric orbits increase exponentially in size and hence become ever more difficult to factor. Thankfully, others have already exerted tremendous effort in tabulating prime factorizations for certain sequences of classical interest, in particular, the Fibonacci, Lucas, and Mersenne numbers. We mine their factorization data to test our predictions for Conjecture 1.1 and its consequences. We have made the raw data and Mathematica file used to construct the figures available at http://sites.math.rutgers.edu/~alexk/files/AllOmegasData.nb.

2.1. Fibonacci and Lucas numbers factorization statistics

Let F_n and L_n denote the nth Fibonacci and Lucas numbers, respectively. Recall that both sequences are defined by the same recursive relation, $F_{n+1} = F_n + F_{n-1}$ and $L_{n+1} = L_n + L_{n-1}$, but differ in the initialization, namely, $F_1 = F_2 = 1$, while $L_1 = 1, L_2 = 3$. They are related by

$$F_{2n} = F_nL_n. \tag{2–1}$$

Both sequences have been completely factored for $1 \leq n \leq 1\ 000$ and partially factored for n going up to 10 000, see the Website [Mer].

In the following calculations, when we encounter in the (incomplete) factorization data a composite number having no known prime factors, we treat that number as a product of exactly two primes (which may be an undercount in Ω). We use this data to study orbits giving several different combinations of Fibonacci numbers and Lucas numbers.

Example 2.1. One can easily verify that, if one takes

$$\gamma = \begin{pmatrix} 1/2 & 1/2 \\ 5/2 & 1/2 \end{pmatrix}, \quad \Gamma = \langle \gamma \rangle^+, \quad \mathbf{v}_0 = (1,1)^t,$$

then the orbit $\mathcal{O} = \Gamma \cdot \mathbf{v}_0 = \{(F_n, L_n) : n \geq 1\}$. A plot of n versus

$$\frac{\Omega(F_nL_n)}{\log\log(F_nL_n)} \tag{2–2}$$

appears in Figure 1. This plot seems to give rather good evidence for equality with $\beta_2 \approx 0.37$ in (1–8).

The data in Figure 1 exhibit several interesting features.

i. The plot in Figure 1 appears to be a union of curves, and a moment's thought reveals that these are roughly the level sets of $y = R/\log x$ for various integer values of R. Conjecture 1.1 predicts that the number of elements on each curve is finite, since each curve eventually dips below the line $y = \beta_2$.

ii. From Figure 1, one notices a single value of $n < 10\ 000$ for which (2–2) seems to dip below $\beta_2 \approx 0.37$. This occurs at $n = 8\ 467$, for which L_n is prime and F_n is composite, with each number spanning 1 770 decimal digits. Since we do not know any factors of F_n, we follow our protocol, declaring that $\Omega(F_nL_n) = 3$. But the true value could perhaps be higher, in which case there may be no values of n up to 10 000 of (2–2) dipping below β_2. Since Conjecture 1.1 only predicts a $\liminf$, it is not inconsistent that infinitely many points in the plot dip below β_2, as long as the amount by which they dip below decreases.

iii. The data in Figure 1 also provide an instance of (the conditional) Theorem 1.4, since the pairs (F_n, L_n) are integer solutions to the Pellian binary quadratic form

$$x^2 - 5y^2 = \pm 4.$$

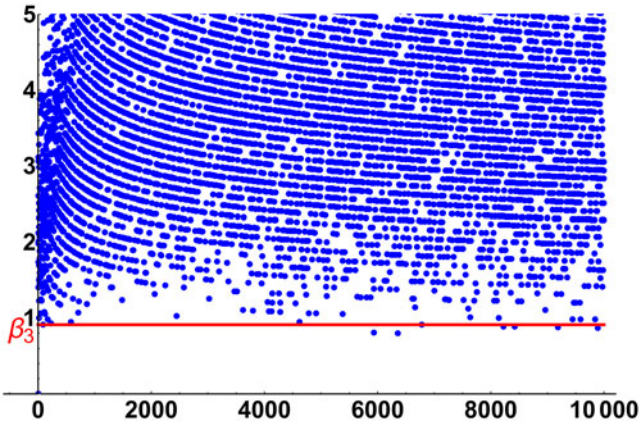

Figure 2. A plot of $n < 10\ 000$ vs. $\Omega(F_nF_{n+1})/\log\log(F_nF_{n+1})$. Also shown is the horizontal line $y = \beta_3 \approx 0.91$.

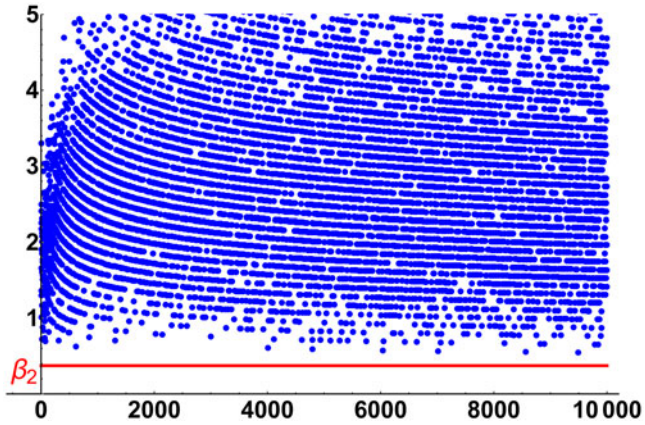

Figure 3. A plot of $n < 10\ 000$ vs. $\Omega(L_nL_{n+1})/\log\log(L_nL_{n+1})$. Also shown is the horizontal line $y = \beta_2$.

iv. While Figure 1 may seem promising toward Conjecture 1.1, this computation is limited to the humble scale $n = 10\ 000$, where $\log n \approx \log\log(F_nL_n) \approx 10$. With current computing technology, it would be difficult to go significantly farther.

One may object to using the Fibonacci and Lucas sequences to test Conjecture 1.1 on the grounds that their factorizations have extra internal structure: They are "strong divisibility sequences"; i.e., $m|n \Rightarrow a_m|a_n$. While it seems likely that this fact could affect some statistics of total number of primes seen in individual draws, (see, e.g., [Bugeaud et al. 05]), it appears not to affect the predicted lim inf value of β_2 in (2–2), exhibited in Figure 1. In any case, the effect of strong divisibility should only be to increase the limiting value, which Figure 1 suggests is not the case for F_nL_n.

Example 2.2. Next we consider the simpler setting of consecutive Fibonacci numbers:

$$\gamma = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \Gamma = \langle\gamma\rangle^+, \quad \mathbf{v}_0 = (1,0)^t,$$
$$\mathcal{O} = \Gamma \cdot \mathbf{v}_0 = \{(F_{n+1}, F_n)^t\}.$$

Conjecture 1.1 predicts a lower bound for the lim-inf of $\Omega(F_nF_{n+1})/\log\log(F_nF_{n+1})$ of $\beta_2 \approx 0.37$. But a moment's inspection of Figure 2 reveals that the truth seems to be closer to $\beta_3 \approx 0.91$. The increase occurs because one of the indices n or $n+1$ is even, and according to (2–1) a Fibonacci number of even index splits into a Fibonacci number times a Lucas number. Thus, this sequence F_nF_{n+1} behaves like the product of three independent sequences, suggesting a predicted lim-inf lower bound from Conjecture 1.1 with $k = 3$ of β_3, not β_2.

Example 2.2 illustrates that Conjecture 1.1 must be stated with an inequality in (1–8); one cannot necessarily determine *a priori* from the data of $\mathcal{O}$ whether there is a "non-obvious" factorization. Indeed, if in Example 2.2 we keep Γ as is but change $\mathbf{v}_0$ to $\mathbf{v}_0 = (1,2)^t$, then the orbit $\mathcal{O} = \{(L_{n+1}, L_n)^t\}$ becomes consecutive Lucas numbers instead of Fibonacci numbers. Lucas numbers do not exhibit an extra strong divisibility factorization, and the liminf appears restored (though now not very convincingly) to β_2, see Figure 3.

Example 2.3. The previous example suggests the following refinement of Example 2.1. One can easily produce orbits which separately capture the even and odd index Fibonacci/Lucas pairs (F_{2n}, L_{2n}) and (F_{2n+1}, L_{2n+1}). These terms appear together inside the orbit of Figure 1. Now in Figure 4, we show what happens if the odd values are suppressed: The even values exhibit an increased beta-value, again to β_3.

Example 2.4. We consider pairs (F_{2n}, F_{2n+2}) of consecutive even-indexed Fibonacci numbers. This sequence was already discussed in the initial Bourgain-Gamburd-Sarnak article on the Affine Sieve, see [Bourgain et al. 10, Section 2.1]. It is obtained by taking $\gamma = \begin{pmatrix} 3 & 1 \\ -1 & 0 \end{pmatrix}$, which has powers

$$\gamma^n = \begin{pmatrix} 3 & 1 \\ -1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{2n+2} & F_{2n} \\ -F_{2n} & -F_{2n-2} \end{pmatrix},$$

and acting on $\mathbf{v}_0 = (1,0)^t$ to give the orbit $\mathcal{O} = \{(F_{2n}, F_{2n+2})^t\}$. Then

$$f(\gamma^n\mathbf{v}_0) = F_{2n}F_{2n-2} = F_nL_nF_{n-1}L_{n-1},$$

where we have again invoked the Fibonacci identity (2–1). As a consequence, we expect four "independent" factors, so the liminf in (1–8) should

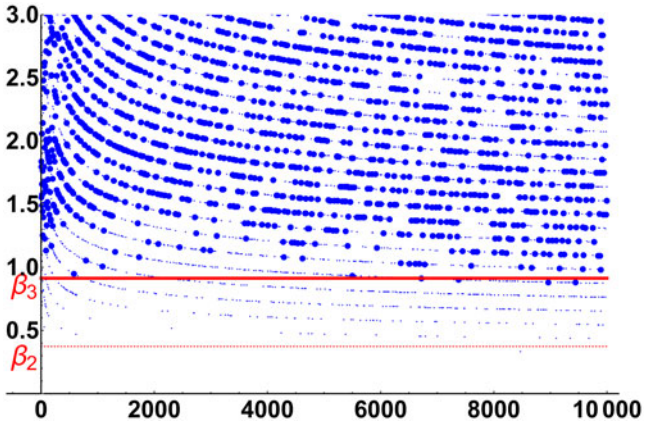

Figure 4. A plot of $n < 10\ 000$ vs. $\Omega(F_nL_n)/\log\log(F_nL_n)$, with the even index values with large marks and the odd index values with small marks. Also shown are the horizontal lines $y = \beta_2, \beta_3$. Compare to Figure 1.

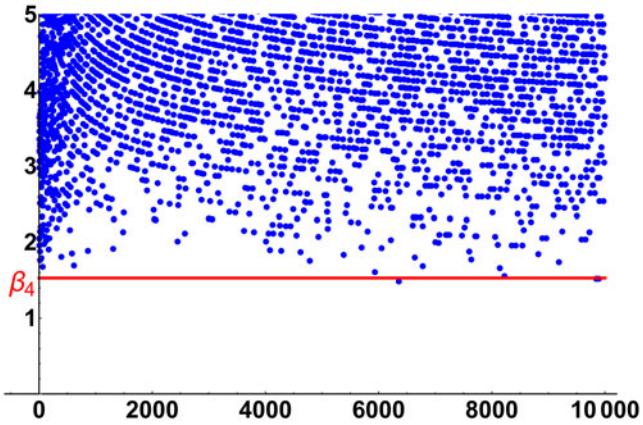

Figure 5. A plot of $n < 10\ 000$ vs. $\Omega(F_{2n}F_{2n+2})/\log\log(F_{2n}F_{2n+2})$. Also shown is the horizontal line $y = \beta_4$.

be no smaller than $\beta_4 \approx 1.52961$. See Figure 5, which agrees with this prediction. But on further inspection, it turns out that the lim-inf here should be β_5, not β_4! Indeed, one of the indices n or $n-1$ is even, so one of the factors F_n or F_{n-1} in $f(\gamma^n \mathbf{v}_0)$ should always decompose further into a Fibonacci/Lucas pair. We do not fully understand why the numerics do not agree with this prediction, although it is plausible that the under-estimation of Ω in inconclusive factorizations may at this point be making a significant contribution.

2.2. Mersenne number factorization statistics

For our last numerical example, we move to Mersenne numbers, $M_n := 2^n - 1$, whose factorizations have also been extensively mined.

Example 2.5. To produce the orbit $\mathcal{O} = \{(M_{n+1}, M_n)\}$, consider as before $\Gamma = \langle\gamma\rangle^+$ and $\mathcal{O} = \Gamma \cdot \mathbf{v}_0$, where:

$$\gamma = \begin{pmatrix} 3 & -2 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{v}_0 = (1,0)^t, \quad \gamma^n \mathbf{v}_0 = (M_{n+1}, M_n)^t.$$

The first 500 values of $\Omega(M_n)$ appear in OEIS (A046051), and the (sometimes partial) factorizations up to 10 000 were kindly provided to us by Sean Irvine using factordb.com. These were used to make Figure 6, showing that the liminf of $\Omega(M_nM_{n+1})/\log\log(M_nM_{n+1})$ appears to be tending toward β_3. This is consistent with the fact that one of n or $n+1$ is even, and for the even indices, Mersenne numbers $M_{2\ell}$ factor as $2^{2\ell} - 1 = (2^\ell - 1)(2^\ell + 1)$.

2.3. Extreme Fibonacci and Lucas values with a fixed number of prime factors

Let us now consider Theorem 1.3 and the (naïve) heuristic (1–5) in the case of the Fibonacci and Lucas sequences, for fixed $R = 2$.

Example 2.6. Define the set

$$\Sigma_{FF} := \{n \geq 2 : \Omega(F_nF_{n+2}) = 2\}$$

to be the indices n for which F_n and F_{n+2} are simultaneously prime. Applying (1–5) with $R = k = 2$ would suggest that

$$\max \Sigma_{FF} \stackrel{?}{\approx} \exp(2/\beta_2) \approx 212. \tag{2–4}$$

One can now examine the sequence [OEI a] of n for which F_n are prime, to find that

$$\{3, 5, 11, 431, 569\} = \Sigma_{FF} \cap [1,\ 1\ 000\ 000]. \tag{2–5}$$

Similarly, consider the set

$$\Sigma_{LL} := \{n \geq 2 : \Omega(L_nL_{n+2}) = 2\}$$

of indices n for which L_n and L_{n+2} are simultaneously prime; presumably (2–4) should also hold for Σ_{LL}. As before, one can examine the sequence [OEI b] of n for which L_n are prime, to find that

$$\{2, 5, 11, 17\} = \Sigma_{LL} \cap [1,\ 1\ 000\ 000]. \tag{2–6}$$

Both these results are compatible, at least to first order, with the naive heuristic (2–4).

Example 2.7. Next define

$$\Sigma_{FL} := \{n \geq 2 : \Omega(F_nL_n) = 2\}$$

to be the indices n for which the Fibonacci and Lucas sequences are simultaneously prime. As aforesaid, the naive heuristic (1–5) predicts $\max \Sigma_{FL} \stackrel{?}{\approx} \exp(2/\beta_2) \approx 212$. Using the sequences [OEI a] and [OEI b] of n for which F_n and L_n are primes, respectively, however,

we find

$$\{4, 5, 7, 11, 13, 17, 47, 148\ 091\} \overset{*}{=} \Sigma_{FL} \cap [1,\ \ 1\ 000\ 000]. \tag{2–7}$$

The "$*$" here is to note that for the largest index $\mathfrak{n} := 148\ 091$, the corresponding $F_{\mathfrak{n}}$ and $L_{\mathfrak{n}}$ (each having around 30 000 decimal digits) have not been certified prime.[6] The pair $(F_{\mathfrak{n}}, L_{\mathfrak{n}})$, if indeed both entries are prime, would have

$$\frac{\Omega(F_{\mathfrak{n}}, L_{\mathfrak{n}})}{\log\log(F_{\mathfrak{n}} L_{\mathfrak{n}})} \overset{?}{\approx} \frac{2}{\log \mathfrak{n}} \approx 0.167988,$$

so if we extended Figure 1 to $n < 150\ 000$, we would see a huge dip below β_2 at $\mathfrak{n}$. In light of (2–4), this certainly constitutes a massively "sporadic" solution to (2–3). However, the existence of such a solution is not shocking, as it is predicted to sometimes occur by the probabilistic model of Theorem 1.3 (see Remark 2). It seems likely to us (though again, this may be naïve) that the left side of (2–7) is actually an equality to Σ_{FL}.[7]

3. Proof of Theorem 1.2

3.1. Analysis of β_k

Fix an integer $k \geq 1$ let β_k solve (1–4). We first analyze this equation.

Lemma 3.1. *For real $k \geq 1$ the function*

$$f_k(t) := t(1 - \log t + \log k) - (k-1)$$

is increasing on $0 < t < k$. It has a unique root $t = \beta_k \in (0, k-1]$.

Proof. The derivative of f is $f_k'(t) = -\log t + \log k$, which is clearly positive on $(0, k)$. For $k = 1$ it has by inspection a root at $\beta_0 = 0 = k-1$. For $k > 1$, near the origin,

$$\lim_{t \to 0^+} f_k(t) = -(k-1) < 0,$$

and at $t = k-1$, we have

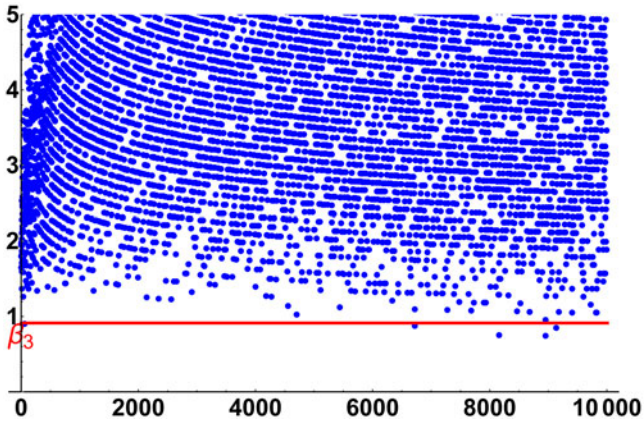

Figure 6. A plot of $n < 10\ 000$ vs. $\Omega(M_n M_{n+1})/\log n$. Also shown is the horizontal line $y = \beta_3$.

$$f_k(k-1) = (k-1)\log\left(\frac{k}{k-1}\right) > 0.$$

Hence, $f_k(t)$ has a unique root in this interval.

Remark 5. One can solve for β_k explicitly in terms of the inverse function $g(z)$ to $z \mapsto ze^z$ on the positive real axis. Namely, one finds

$$\beta_k = \frac{1-k}{g\left(\frac{1-k}{ek}\right)},$$

where $e = 2.718\ldots$. We will not need this fact, nor the fact that $\beta_k = k - 1 - O(1/k)$ for k large, which can be shown in a variety of ways.

3.2. Analysis of the behavior of Ω

We next record a uniform asymptotic formula for

$$\mathcal{N}_r(T) := \#\{x < T : \Omega(x) = r\},$$

that is, the number of positive integers up to T having exactly r prime factors, counted with multiplicity. For fixed r, the formula

$$\mathcal{N}_r(T) \sim \frac{T}{\log T} \frac{(\log\log T)^{r-1}}{(r-1)!}, \qquad (T \to \infty) \tag{3–1}$$

is well known, but we shall require an estimate when r is an increasing function of T. Such an estimate can be obtained based on a method of [Selberg 54]. A treatment is given in Tenenbaum [Selberg 54, Chap. II.6, Theorem 5], as stated below.

[6] The probable primality of $F_{\mathfrak{n}}$ was found by T. D. Noe while that of $L_{\mathfrak{n}}$ by de Water; see OEIS for further credits. Both numbers have passed numerous pseudoprimality tests. Assuming GRH, one would need to run about $(30\ 000)^4$ trials (that is, $(\log F_{\mathfrak{n}})^2$ tests at a cost of $(\log F_{\mathfrak{n}})^2$ each, ignoring epsilons) of the Miller primality test to certify these entries prime. Unconditionally, the exponent 4 would be replaced by a 6, see [Lenstra and Pomerance 11]. One could alternatively try the elliptic curve primality test, which is also unconditional and in practice runs faster, though a worst-case execution time is currently unknown.

[7] In some very special cases, one can completely determine sets like Σ_{FL}. Indeed, see [Bober et al. 09], where all solutions to $x^2 - 3y^2 = 1$ with $\Omega(xy) \leq 3$ are effectively listed.

The result is given in terms of the function

$$\nu(z) := \frac{1}{\Gamma(z+1)} \prod_p \left(\left(1 - \frac{z}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^{z} \right).$$

This infinite product converges on $\Re(z) > 0$, giving in this region a non-vanishing meromorphic function with simple poles at $z = p$ for all primes p. Note also that $\lim_{z \to 0^+} \nu(z) = 1$; hence for real $z \in [0, 3/2]$, say, $\nu(z)$ is bounded above and below by positive constants.

Proposition 3.1 ([Tenenbaum 95, eqn. (20), p. 205]). *For $T \geq 3$, we have uniformly in*

$$1 \leq r \leq \frac{3}{2} \log \log T$$

that

$$\mathcal{N}_r(T) = \frac{T}{\log T} \frac{(\log \log T)^{r-1}}{(r-1)!} \left(\nu\left(\frac{r-1}{\log \log T}\right) + O\left(\frac{r}{(\log \log T)^2}\right) \right), \tag{3–2}$$

with an absolute implied constant.

This asymptotic continues to hold up to $r < (2-\epsilon) \log \log T$, but not beyond this point, as ν has a pole at $z = 2$. A different asymptotic formula takes over at $r > (2+\epsilon) \log \log T$, see [Nicolas 84], but it will not be needed for our purposes.

For our application, we derive from (3–2) a simplified estimate.

Lemma 3.2. *Let $r = \gamma \log \log T$ with $\frac{1}{\log \log T} \leq \gamma < \frac{3}{2}$. Then as $T \to \infty$,*

$$\mathbb{P}[\Omega(x) = r] := \frac{\mathcal{N}_r(T)}{T} \asymp (\log T)^{\gamma - \gamma \log \gamma - 1 + o(1)}, \tag{3–3}$$

with absolute implied constants.

Proof. First recall that, on $[0, 3/2]$, the function $\nu(\cdot)$ is bounded above and below by positive constants. Then inserting the Stirling's formula estimate,

$$(r-1)! \asymp r^{r-1/2} e^{-r}, \qquad (1 \leq r < \infty)$$

into (3–2) yields

$$\begin{aligned} \mathbb{P}[\Omega(x) = r] &\asymp \frac{1}{\log T} \left(\frac{\log \log T}{r} \right)^{r-1} r^{-\frac{1}{2}} e^{r} \\ &= \frac{1}{\log T} (\gamma)^{-\gamma \log \log T - 1} (\gamma \log \log T)^{-\frac{1}{2}} (\log T)^{\gamma} \\ &= \gamma^{-\frac{3}{2}} (\log \log T)^{-\frac{1}{2}} (\log T)^{-1 - \gamma \log \gamma + \gamma}, \end{aligned}$$

from which the estimate (3–3) follows, since $\gamma \geq 1/\log \log T$. □

3.3. Estimate for a single draw

To prove Theorem 1.2, we first obtain upper and lower bounds on the probability density function for a single draw.

Theorem 3.1. *Let $k \geq 1$ be fixed. For any integer $T \geq 2$, draw a vector*

$$(x_1, x_2, \ldots, x_k) \in [1, T]^k$$

uniformly. For any small $\varepsilon > 0$, there is a $\delta = \delta(\varepsilon) > 0$ so that for all $T > T_0(\varepsilon)$,

$$\mathbb{P}\left[\Omega(x_1 x_2 \cdots x_k) \leq (\beta_k + \varepsilon) \log \log T\right] \gg_\varepsilon \frac{1}{(\log T)^{1-\delta}}, \tag{3–4}$$

and, for $k \geq 2$,

$$\mathbb{P}\left[\Omega(x_1 x_2 \cdots x_k) \leq (\beta_k - \varepsilon) \log \log T\right] \ll_\varepsilon \frac{1}{(\log T)^{1+\delta}}. \tag{3–5}$$

3.3.1. Proof of the lower bound (3–4)

Suppose $k \geq 1$ and write $k\gamma = \beta_k + \varepsilon$, so that $0 < \gamma < 1$, and let

$$r := \lfloor \gamma \log \log T \rfloor.$$

Then

$$\mathbb{P}\left[\Omega(x_1 \ldots x_k) \leq k\gamma \log \log T\right] \geq \prod_{j=1}^{k} \mathbb{P}\left[\Omega(x_j) = r\right].$$

Inserting (3–3) gives

$$\mathbb{P}\left[\Omega(x_1 \ldots x_k) \leq k\gamma \log \log T\right] \gg \left[(\log T)^{\gamma - \gamma \log \gamma - 1 + o(1)} \right]^k.$$

Write $\alpha = k\gamma$; then as $T \to \infty$ the exponent of $\log T$ approaches the limiting value

$$\gamma k - \gamma k \log \gamma - k = \alpha - \alpha \log \alpha + \alpha \log k - k = f_k(\alpha) - 1.$$

By Lemma 3.1, since $\alpha = k\gamma = \beta_k + \varepsilon > \beta_k$, and $f_k(\beta_k) = 0$, we conclude that as $T \to \infty$ the limiting exponent exceeds –1 by the positive amount $f_k(\alpha) > 0$. Therefore, we can pick $\delta(\varepsilon) > 0$ and $T_0(\varepsilon)$ depending on ε (and k, which is fixed) so that (3–4) holds.

3.3.2. Proof of the upper bound (3–5)

The upper bound estimate (3–5) is more subtle and requires $k \geq 2$. Again take a fixed $\varepsilon > 0$ and define γ by $k\gamma = \beta_k - \varepsilon$ taking ε small enough that $0 < \gamma < 1$, which is possible since $\beta_k > 0$. Since

$$\Omega(x_1 \cdots x_k) = \Omega(x_1) + \cdots + \Omega(x_k),$$

we have that

$$\mathbb{P}\big[\Omega(x_1 \ldots x_k) \le k\gamma \log\log T\big] = \sum_{r_1+\cdots+r_k \le k\gamma \log\log T} \mathbb{P}\big[\Omega(x_1)=r_1, \ldots \Omega(x_k)=r_k\big]$$

We upper bound the total number of summands trivially by

$$\sum_{r_1+\cdots+r_k \le k\gamma \log\log T} 1 \ll (\log\log T)^k = (\log T)^{o(1)}.$$

It remains to upper bound the contribution of an individual summand

$$\max_{r_1+\cdots+r_k \le k\gamma \log\log T} \mathbb{P}\big[\Omega(x_1)=r_1, \ldots \Omega(x_k)=r_k\big].$$

Write each r_j as

$$r_j = \gamma_j \log\log T,$$

so that

$$\gamma_1 + \cdots + \gamma_k \le k\gamma < \beta_k < k-1. \tag{3–6}$$

On average, these γ_j's are less than one, but individually they could in principle be large, and we can apply (3–3) only when $\gamma_j < 3/2$. Let $\ell \subset \{1, \ldots, k\}$ denote the indices j for which $\gamma_j < 3/2$ is "low," and let $h := \{1, \ldots, k\} \setminus \ell$ be the "high" indices. Abusing notation, we use the same symbol for their cardinalities, e.g.,

$$\ell + h = k.$$

We have that

$$k\gamma \ge \sum_{j\in h} \gamma_j \ge \frac{3}{2} h,$$

so

$$\ell \ge k\left(1 - \frac{2}{3}\gamma\right) > \frac{1}{3}k,$$

and

$$\sum_{j\in\ell} \gamma_j = \sum_j \gamma_j - \sum_{j\in h} \gamma_j \le k\gamma - \frac{3}{2}h. \tag{3–7}$$

For $j \in h$, we estimate $\mathbb{P}[\Omega(x_j) = r_j] \le 1$ trivially. This gives a bound

$$\mathbb{P}\big[\Omega(x_1)=r_1, \ldots \Omega(x_k)=r_k\big] \le \prod_{j\in\ell} \mathbb{P}\big[\Omega(x_j)=r_j\big] \ll (\log T)^{o(1)} \prod_{j\in\ell} (\log T)^{\gamma_j - \gamma_j \log \gamma_j - 1},$$

using (3–3). The exponent in this expression, subject to (3–7), is maximized if, for all $j \in \ell$, we set all values equal $\gamma_j = \eta$, in which case,

$$\mathbb{P}\big[\Omega(x_1)=r_1, \ldots \Omega(x_k)=r_k\big] \ll (\log T)^{\ell(\eta - \eta\log\eta - 1) + o(1)}. \tag{3–8}$$

Now, we have

$$\eta = \eta(\gamma, k, \ell) := \frac{k\gamma}{\ell} - \frac{3h}{2\ell} = \frac{3}{2} - \frac{k}{\ell}\left(\frac{3}{2} - \gamma\right).$$

We bound the exponent (3–8), varying ℓ. Viewing ℓ as a continuous variable, we have

$$\eta' := \frac{\partial \eta}{\partial \ell} = \frac{k}{\ell^2}\left(\frac{3}{2} - \gamma\right) = \frac{1}{\ell}\left(\frac{3}{2} - \eta\right).$$

The derivative of the exponent of $\log T$ in the ℓ-variable is then

$$\frac{\partial}{\partial \ell}[\ell(\eta - \eta\log\eta - 1)] = \eta - \eta\log\eta - 1 - \ell\eta'\log\eta = \eta - \frac{3}{2}\log\eta - 1,$$

which by inspection is a positive function of $\eta \in (0,1)$. It follows that the exponent is maximized at the largest allowable value of ℓ, namely the integer $\ell = k$, so $h = 0$. For this value of ℓ, we have $\eta = \gamma$, whence as $T \to \infty$ the exponent of $\log T$ in (3–8) approaches the limiting value

$$k(\gamma - \gamma\log\gamma - 1) = \alpha - \alpha\log\alpha + \alpha\log k - k = f_k(\alpha) - 1.$$

where we have again set $\alpha = k\gamma = \beta_k - \varepsilon$. Again using Lemma 3.1, this limiting exponent is less than –1 since $\alpha < \beta_k$ gives $f_k(\alpha) < 0$. Thus, we can choose $\delta(\varepsilon)$ and a $T_0(\varepsilon)$ so that (3–5) holds. This completes the proof of Theorem 3.1.

3.4. Proof of *Theorem 1.2*

It is now a simple matter to deduce Theorem 1.2 from Theorem 3.1. Instead of a single draw, here we have a sequence of independent draws, one for each $n = 1, 2, \ldots$, and with $T = C^n$. By (3–5),

$$\mathbb{P}\left[\frac{\Omega(x_{1,n}x_{2,n}\cdots x_{k,n})}{\log n} \le (\beta_k - \varepsilon)\big(1 + \log\log C/\log n\big)\right] \ll_\varepsilon \frac{1}{n^{1+\delta}},$$

and $\sum_{n\ge 1} 1/n^{1+\delta} < \infty$. Thus by the Borel-Cantelli Lemma, the probability of these events occurring infinitely often is zero; that is, with probability one, we have

$$\liminf_n \frac{\Omega(x_{1,n}x_{2,n}\cdots x_{k,n})}{\log n} \ge \beta_k - \varepsilon.$$

Similarly, the independent events

$$\left[\frac{\Omega(x_{1,n}x_{2,n}\cdots x_{k,n})}{\log n} \le (\beta_k+\varepsilon)\big(1+\log\log C/\log n\big)\right]$$

occur with probability at least $1/n^{1-\delta}$, the sum of which diverges. By the second Borel-Cantelli Lemma, infinitely many occur with probability one, so

$$\liminf_n \frac{\Omega(x_{1,n}x_{2,n}\cdots x_{k,n})}{\log n} \le \beta_k+\varepsilon.$$

This proves Theorem 1.2.

4. Proof of Theorem 1.3

Let $k \ge 1$, $C > 1$, and $R \ge 1$ be fixed throughout this section (unlike the previous section, where R was growing). In particular, the estimate (3–1) is perfectly valid here and will be used regularly. In this section, we allow implied constants to depend on k, C and R, since they are fixed.

For each $n \ge 1$, we choose uniformly a vector $\mathbf{x}_n = (x_{1,n}, \ldots, x_{k,n}) \in [1, C^n]^k$, and let

$$\mathfrak{n} = \mathfrak{n}(R) = \max\big\{n \ge 1 : \Omega(x_{1,n}\cdots x_{k,n}) \le R\big\},$$

with $\mathfrak{n} = 0$ if this set is empty and $\mathfrak{n} = \infty$ if it is unbounded.

First note that (1–6) follows immediately from Theorem 1.2. Indeed, if $\mathfrak{n}(R) = \infty$, then $\Omega(x_{1,n}\cdots x_{k,n}) = R$ occurs for infinitely many n's. But then

$$\liminf_{n\ge 1} \frac{\Omega(x_{1,n}\cdots x_{k,n})}{\log n} = 0,$$

contradicting (1–3). Hence, this event has probability zero.

To prepare for the proof of (1–7), we record the following computations. Recall that implied constants in this section may depend on k, C, and R.

Lemma 4.1. *Let $k \ge 1$ and $R \ge 1$ be fixed. Then for $t \ge 1$,*

$$\mathbb{P}\big[\Omega(x_{1,t}\cdots x_{k,t}) \le R\big] \ll \frac{(\log t)^{k(R-1)}}{t^k}. \tag{4–1}$$

Assuming further that $R \ge k$, we have that

$$\mathbb{P}\big[\Omega(x_{1,t}\cdots x_{k,t}) \le R\big] \gg \frac{(\log t)^{R-k}}{t^k}. \tag{4–2}$$

Proof. The event $\Omega(x_{1,t}\cdots x_{k,t}) \le R$ is contained inside the intersection of the events $\Omega(x_{j,t}) \le R$, for all $j = 1, 2, \ldots, k$. Thus, using (3–1) gives

$$\mathbb{P}\big[\Omega(x_{1,t}\cdots x_{k,t}) \le R\big] \le \prod_{j=1}^{k} \mathbb{P}\big[\Omega(x_{j,t}) \le R\big] \ll \left[\frac{1}{\log C^t}\frac{(\log\log C^t)^{R-1}}{(R-1)!}\right]^k,$$

from which (4–1) follows immediately.

Now assume that $R/k \ge 1$. Then, the event $\Omega(x_{1,t}\cdots x_{k,t}) \le R$ contains the intersection over all $j = 1, 2, \ldots, k$ of the nonempty events $\Omega(x_{j,t}) \le R/k$. So

$$\mathbb{P}\big[\Omega(x_{1,t}\cdots x_{k,t}) \le R\big] \ge \prod_{j=1}^{k} \mathbb{P}\left[\Omega(x_{j,t}) \le \frac{R}{k}\right] \gg \left[\frac{1}{\log C^t}\frac{(\log\log C^t)^{\frac{R}{k}-1}}{(\frac{R}{k}-1)!}\right]^k,$$

which implies (4–2).

Lemma 4.2. *If $R \ge k \ge 1$ are fixed, then for all sufficiently large t,*

$$\mathbb{P}[\mathfrak{n}(R) = t] \gg \frac{(\log t)^{R-k}}{t^k}.$$

Proof. Consider the event $\mathfrak{n}(R) = t$. This occurs if and only if $\Omega(x_{1,t}\cdots x_{k,t}) \le R$ and, for all larger integers $s > t$, we have that $\Omega(x_{1,s}\cdots x_{k,s}) > R$. That is,

$$\mathbb{P}[\mathfrak{n}(R) = t] = \mathbb{P}\big[\Omega(x_{1,t}\cdots x_{k,t}) \le R\big] \cdot \prod_{s>t}\big(1-\mathbb{P}\big[\Omega(x_{1,s}\cdots x_{k,s}) \le R\big]\big) \gg \frac{(\log t)^{R-k}}{t^k}\cdot\prod_{s>t}\left(1-K\frac{(\log s)^{k(R-1)}}{s^k}\right),$$

where we used (4–2) and (4–1). (Here, $K > 0$ is a constant depending at most on k, C, and R.) Since $s \ge 2$, the infinite product converges absolutely. It bounds the result below by a uniform positive constant for all sufficiently large t that avoid possible nonpositive terms for small s in the infinite product.

Proof of Theorem 1.3. Assume that $R \ge k \ge 1$ and let $m \ge k-1$. Consider the m-th moment of $\mathfrak{n}$, namely,

$$\mathbb{E}[\mathfrak{n}^m] = \sum_{t\ge 0} t^m\ \mathbb{P}[\mathfrak{n}(R) = t] \gg \sum_{t\ge 0} t^m \frac{(\log t)^{R-k}}{t^k},$$

where we used Lemma 4.2. Since $m-k \ge -1$, this sum diverges.

Note the case $R = k = 1$ gives divergence of the $m = 0$-th moment; that is, if $k = 1$ then $\mathfrak{n} = \infty$ with probability 1.)

5. Proofs of theorems 1.4 and 1.5

Assume Conjecture 1.1 in this section.

Proof of Theorem 1.4. Let $V : Q = t$ have $V(\mathbb{Z}) \neq \emptyset$. As is well known and in this case essentially goes back to Gauss, $V(\mathbb{Z})$ decomposes into a finite number of Γ-orbits,

$$V(\mathbb{Z}) = \sqcup_{j=1}^{m} \Gamma \cdot \mathbf{v}_j,$$

where $\Gamma = O_Q(\mathbb{Z})$ is the orthogonal group fixing Q (see, e.g., [Cassels 78] or [Kontorovich 16, §2]). Since Q is indefinite, the Zariski closure of Γ is a torus,

$$\mathbb{G} = \mathrm{Zcl}(\Gamma) = O(1,1).$$

Thus, up to finite index, $\Gamma = \langle \gamma \rangle$ for some hyperbolic matrix γ. By Conjecture 1.1, each orbit $\mathcal{O}_j = \Gamma \cdot \mathbf{v}_j$ has

$$\liminf_{(x,y)\in\mathcal{O}_j} \frac{\Omega(xy)}{\log\log|xy|} \geq \beta_2,$$

and hence the same holds for all of $V(\mathbb{Z})$.

Proof of Theorem 1.5. Let α be a quadratic surd having ordinary continued fraction expansion $\alpha = [a_0, a_1, a_2, \ldots]$ with partial quotients p_n/q_n, given in matrix form by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} p_n \\ q_n \end{pmatrix}.$$

Now, α has an eventually periodic continued fraction expansion

$$\alpha = [a_0; a_1, \ldots a_k, \overline{a_{k+1}, \ldots, a_{k+\ell}}].$$

After the first few terms, the sequence $(p_n, q_n)^t$ decomposes into finitely many Γ-orbits, where

$$\Gamma = \langle \gamma \rangle, \quad \gamma = M\begin{pmatrix} 0 & 1 \\ 1 & a_{k+1} \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & a_{k+\ell} \end{pmatrix}M^{-1},$$

with

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & a_k \end{pmatrix}.$$

The base points of the orbits are given by

$$\mathbf{v}_j := M\begin{pmatrix} 0 & 1 \\ 1 & a_{k+1} \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & a_{k+j} \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad 0 \leq j \leq \ell - 1.$$

We may apply Conjecture 1.1 to each orbit, since they are infinite, and use the asymptotic $\log\log p_n q_n \sim \log n$. This establishes the claim. □

Acknowledgments

The authors thank Jonathan Bober, Andrew Granville, Peter Sarnak, and Alireza Salehi Golsefidy for enlightening discussions, comments, and suggestions, and most of all, Danny Krashen and Sean Irvine for the highly nontrivial and time-consuming task of computing Ω for Lucas, Fibonacci, and Mersenne numbers from cumbersome online databases of their factorizations.

Funding

Kontorovich is partially supported by an NSF CAREER grant DMS-1455705, an NSF FRG grant DMS-1463940, US-Israel Binational Science Foundation Grant #2014099, a Simons Fellowship, a von Neumann Fellowship at IAS, and the IAS's NSF grant DMS-1638352. Lagarias is partially supported by NSF grants DMS-1401224 and DMS-1701576.

ORCID

Alex Kontorovich http://orcid.org/0000-0001-7626-8319
Jeffrey Lagarias http://orcid.org/0000-0002-4157-5527

References

[Bourgain et al. 10] J. Bourgain, A. Gamburd, and P. Sarnak. "Affine Linear Sieve, Expanders, and Sum-product." *Invent. Math.* 179:3 (2010), 559–644.

[Bober et al. 09] J. Bober, J. Lagarias, and B. Schmuland. "Very Composite Numbers: 11334 [2008, 71]." *The American Mathematical Monthly.* 116:9 (2009), 847–848.

[Bugeaud et al. 05] Y. Bugeaud, F. Luca, M. Mignotte, and S. Siksek. "On Fibonacci Numbers with Few Prime Divisors." *Proc. Japan Acad. Ser. A Math. Sci.* 81:2 (2005), 17–20.

[Cassels 78] J. W. S. Cassels. *Rational Quadratic Forms. Number 13 in London Mathematical Society Monographs.* London: Academic Press, 1978.

[Hardy and Ramanujan 17] G. H. Hardy, and S. Ramanujan. "The Normal Number of Prime Factors of a Number *n*, Quart." *J. Pure Appl. Math.* 48 (1917), 76–97.

[Kontorovich 14] A. Kontorovich. "Levels of Distribution and the Affine Sieve." *Ann. Fac. Sci. Toulouse Math.* 23:5 (2014), 933–966.

[Kontorovich 16] A. Kontorovich. "Applications of thin orbits." In *Dynamics and Analytic Number Theory, Volume 437 of London Math. Soc. Lecture Note Ser.* pages 289–317 Cambridge: Cambridge University Press, 2016.

[Lenstra and Pomerance 11] H. W. Lenstra, Jr., and C. Pomerance. "Primality Testing with Gaussian Periods." *J. European Math. Society.* to appear. http://www.math.dartmouth.edu/~carlp/aks041411.pdf.

[Mer] http://mersennus.net/fibonacci/. Contact: marin.mersennus@gmail.com

[Nicolas 84] J.-L. Nicolas. "Sur la distribution des nombres entiers ayant une quantité fixée de facteurs premiers." *Acta Arith.* 44:3 (1984), 191–200.

[OEI a] Online Encyclopedia of Integer Sequences (OEIS), published electronically at https://oeis.org, 2019, Sequence A001605. https://oeis.org/A001605.

[OEI b] Online Encyclopedia of Integer Sequences (OEIS), published electronically at https://oeis.org, 2019, Sequence A001606. https://oeis.org/A001606.

[Salehi Golsefidy and Sarnak 13] A. Salehi Golsefidy, and P. Sarnak. "The Affine Sieve." *J. Amer. Math. Soc.* 26:4 (2013), 1085–1105.

[Selberg 54] A. Selberg. "Note on a paper by L. G. Sathe." *J. Indian Math. Soc.* 18 (1954), 53–57. [Also in: A. Selberg, *Collected Papers, Vol. 1*, Berlin: Springer-Verlag, 1989, pp. 418–422.]

[Tenenbaum 95] G. Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory, Volume 46 of Cambridge Studies in Advanced Mathematics*. Cambridge: Cambridge University Press, 1995. translated from the second french edition (1995) by C. B. Thomas.