The final publication is available at Elsevier via https://dx.doi.org/10.1016/j.jnt.2018.06.017 © 2019. This manuscript version is made available under the CC-BY-NC-ND 4.0 license https://creativecommons.org/licenses/by-nc-nd/4.0/

Accepted Manuscript

A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences

M. Ram Murty, François Séguin, Cameron L. Stewart

PII: S0022-314X(18)30190-2
DOI: https://doi.org/10.1016/j.jnt.2018.06.017
Reference: YJNTH 6082

To appear in: *Journal of Number Theory*

Received date: 16 November 2017
Revised date: 28 June 2018
Accepted date: 29 June 2018

Please cite this article in press as: M.R. Murty et al., A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences, *J. Number Theory* (2018), https://doi.org/10.1016/j.jnt.2018.06.017

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

A LOWER BOUND FOR THE TWO-VARIABLE ARTIN CONJECTURE AND PRIME DIVISORS OF RECURRENCE SEQUENCES

M. RAM MURTY, FRANÇOIS SÉGUIN, AND CAMERON L. STEWART

ABSTRACT. In 1927, Artin conjectured that any integer other than -1 or a perfect square generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ for infinitely many p. In 2000, Moree and Stevenhagen considered a two-variable version of this problem, and proved a positive density result conditionally to the generalized Riemann Hypothesis by adapting a proof by Hooley for the original conjecture. In this article, we prove an unconditional lower bound for this two-variable problem. In particular, we prove an estimate for the number of distinct primes which divide one of the first N terms of a non-degenerate binary recurrence sequence. We also prove a weaker version of the same theorem, and give three proofs that we consider to be of independent interest. The first proof uses a transcendence result of Stewart, the second uses a theorem of Bombieri and Schmidt on Thue equations and the third uses Mumford's gap principle for counting points on curves by their height. We finally prove a disjunction theorem, where we consider the set of primes satisfying either our two-variable condition or the original condition of Artin's conjecture. We give an unconditional lower bound for the number of such primes.

1. INTRODUCTION

In this article we study the two-variable analogue of Artin's conjecture on primitive roots. Artin's original conjecture suggested that for any integer a other than -1 and perfect squares, there are infinitely many primes p for which a generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Specifically, Artin conjectured that the set

$$P_a(X) = \left\{p \leq X \text{ prime } : \langle a \bmod p\rangle = (\mathbb{Z}/p\mathbb{Z})^\times\right\}$$

has positive density in the set of all primes. We can trace the origin of this problem all the way back to Gauss. It was apparently popular at the time to study decimal expansions of certain rational numbers. In his Disquisitiones Arithmeticae, Gauss describes the period of the decimal expansion of $\frac{1}{p}$ in terms of the order of $10 \bmod p$. Some other such specific cases of this were considered before 1927, at which time Artin formulated the above conjecture.

As of now, the conjecture is still open. There is actually no a for which we know $P_a(X)$ goes to infinity as X goes to infinity. However, there have been major partial results since, the conditional proof by Hooley [10] under the assumption of the generalized Riemann Hypothesis being among the most important, as are the works of Gupta and Murty [7] and Heath-Brown [8]. For example, we know that given three mutually coprime numbers a, b, c, there are infinitely many primes p for which at least one of a, b, c is a primitive root mod p.

Many variations on Artin's original conjecture have since been studied. Moree and Stevenhagen [15] considered a two-variable variant where the set of interest is

$$S = \left\{p \text{ prime } : b \bmod p \in \langle a \bmod p\rangle \subseteq (\mathbb{Z}/p\mathbb{Z})^\times\right\}$$

for given a and b. They adapted Hooley's argument, as well as using some work by Stephens ([22]), to show a positive density result for such primes, conditionally under the generalized Riemann Hypothesis. In this article, we prove an unconditional lower bound on the number of primes in this set. Specifically, we prove the following result.

Date: July 16, 2018.

2010 *Mathematics Subject Classification.* 11N69, 11B37, 11D59 .

Key words and phrases. Artin's conjecture, Recurrence sequences, Thue equation.

Research of the first and third author partially supported by an NSERC Discovery grant. Research of the second author partially supported by a FRQNT B2 Research Scholarship. Research of the third author supported in part by the Canada Research Chairs Program.

ACCEPTED MANUSCRIPT

Theorem 1.1. *Let $a, b \in \mathbb{Z}^*$ with $|a| \neq 1$. Then,*

$$\left|\left\{p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p\rangle \subset \mathbb{F}_p^*\right\}\right| \gg \log x.$$

We do so by proving in section 2 a more general result about binary recurrence sequences.

Theorem 1.2. *Let $\{u_n\}_{n=1}^{\infty}$ be a non-degenerate binary recurrence sequence with the n-th term given by (2.1). Let ϵ be a positive real number. There exists an effectively computable positive number C, depending at most on ϵ, a, b, α and β, such that if N exceeds C, then*

$$\omega\left(\prod_{\substack{n=1\\ u_n\neq 0}}^{N} u_n\right) > \left(1 - 1/\sqrt{2} - \epsilon\right) N.$$

Here, $\omega(n)$ denotes the number of distinct prime factors of n.

We also prove a more precise result for the specific case of Lucas sequences.

Theorem 1.3. *Let $\{t_n\}_{n=1}^{\infty}$ be a non-degenerate Lucas sequence. Then,*

$$\omega\left(\prod_{n=1}^{N} t_n\right) \geq N - 9.$$

Equality holds when t_n satisfies

$$t_n = t_{n-1} - 2t_{n-2} \quad for \quad n = 2, 3, ...$$

and $N = 30, 31, 32, 33$ or 34.

We finally conjecture the following stronger statement.

Conjecture 1.4. *There exist positive numbers C_1 and C_2, which depend at most on a, b, α and β, such that if $\{u_n\}_{n=1}^{\infty}$ is a non-degenerate binary recurrence sequence, then*

$$C_1 N \log N \leq \omega\left(\prod_{\substack{n=1\\ u_n\neq 0}}^{N} u_n\right) \leq C_2 N \log N.$$

It can be shown that the lower bound obtained from this conjecture could be used to improve Theorem 1.1 by replacing $\log x$ with $\log x \log\log x$ in the lower bound.

We shall also give several proofs, which we believe to be of independent interest, for the following theorem, which is a weaker version of Theorem 1.1.

Theorem 1.5. *Let $a, b \in \mathbb{Z}^*$ with $|a| \neq 1$. Then,*

$$\left|\left\{p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p\rangle \subset \mathbb{F}_p^*\right\}\right| \gg \log\log x.$$

The last theorem we prove is a disjunction theorem.

Theorem 1.6. *Let $a, b \in \mathbb{Z}^*$ with $(a, b) = 1$. Then,*

$$\left|\left\{p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p\rangle \text{ or } \langle b \bmod p\rangle = \mathbb{F}_p^*\right\}\right| \gg \frac{x}{(\log x)^2}.$$

This theorem suggests that it might be possible to prove positive density of this set unconditionally. It is worth noting that unlike the original Artin conjecture, the set S is known to be infinite. Moree and Stevenhagen included in [15] a modification of a simple argument by Pólya (found in [18]) that proves the infinitude unconditionally. However, their argument does not seem to provide any explicit function going to infinity as a lower bound.

We will start by proving Theorem 1.2 in section 4 after a few preliminaries in sections 2 and 3. Theorem 1.3 will be proven in section 5. Then, we will use Theorem 1.2 to prove Theorem 1.1 in section 6. Our three proofs for Theorem 1.5 are in sections 7, 8 and 9 respectively. Finally, we will prove Theorem 1.6 in section 11.

ACCEPTED MANUSCRIPT

2. Prime divisors of terms of recurrence sequences

For any non-zero integer n let $\omega(n)$ denote the number of distinct prime factors of n. Let r and s be integers with $r^2+4s \neq 0$. Let u_0 and u_1 be integers and put

$$u_n = ru_{n-1} + su_{n-2} \text{ for } n \geq 2.$$

Then,

$$u_n = a\alpha^n + b\beta^n, \tag{2.1}$$

where α and β are the roots of the polynomial

$$x^2 - rx - s$$

and

$$a = \frac{u_0\beta - u_1}{\beta - \alpha}, \qquad b = \frac{u_1 - u_0\alpha}{\beta - \alpha}.$$

The sequence $\{u_n\}_{n=0}^{\infty}$ is called a *binary recurrence sequence*. It is said to be *non-degenerate* if $ab\alpha\beta \neq 0$ and α/β is not a root of unity.

Lemma 2.1. *For non-degenerate binary recurrence sequences, if $|\alpha| \geq |\beta|$, then*

$$|\alpha| \geq \sqrt{2}.$$

Proof. Actually, we will prove that $|\alpha| \geq (1+\sqrt{5})/2$. This is stronger than the stated lemma, but the bound of $\sqrt{2}$ is sufficient for our application, and will be used for simplicity.

If α and β are integers this is obvious. Also, since $r = \alpha + \beta$, it cannot be the case that only one of α and β is an integer.

Suppose that α and β are not integers. If $\mathbb{Q}(\alpha)$ is an imaginary quadratic field, $\frac{\alpha}{\beta}$ is a root of unity, which again contradicts the hypothesis.

We therefore assume that $\mathbb{Q}(\alpha)$ is totally real. Then, $\alpha = a + b\sqrt{D}$ and $\beta = a - b\sqrt{D}$ for some $D \geq 2$ and a, b in $\mathbb{Z}$, or in $\mathbb{Z}\left[\frac{1}{2}\right]$ if $D \equiv 1 \bmod 4$. Note that $b \neq 0$ since we assumed that α, β were not integers. Also, $a \neq 0$ as otherwise $\alpha/\beta = -1$ which is a root of unity.

Since $|\alpha| \geq |\beta|$, a and b must have the same sign, and so $|\alpha| = |a| + |b|\sqrt{D}$.

If $D \not\equiv 1 \bmod 4$, then $|a| + |b|\sqrt{D} \geq 1 + \sqrt{2} \geq \frac{1+\sqrt{5}}{2}$.

If $D \equiv 1 \bmod 4$, then $D \geq 5$ and so $|a| + |b|\sqrt{D} \geq \frac{1+\sqrt{5}}{2}$. □

In 1921 Polya [18] showed that

$$\omega\left(\prod_{\substack{n=1 \\ u_n \neq 0}}^{N} u_n\right) \to \infty \; as \; N \to \infty; \tag{2.2}$$

Gelfond [6] and Mahler [13] in 1934 and Ward [27] in 1954 gave alternative proofs of (2.2). In 1987 Shparlinski [21] showed that

$$\omega\left(\prod_{\substack{n=1 \\ u_n \neq 0}}^{N} u_n\right) \gg N/\log N, \tag{2.3}$$

improving on an earlier result of his [20], where he had established (2.3) with its righthand side replaced by $\sqrt{N}$. It should be noted that Shparlinski's result (2.3) applies not just to binary recurrence sequences but to non-degenerate sequences of order k with $k \geq 2$.

Theorem 1.2 is an improvement upon (2.3) for binary recurrence sequences. It is the key result we need to establish Theorem 1.1.

A *Lucas sequence* is a non-degenerate binary recurrence sequence $\{t_n\}_{n=0}^{\infty}$ with $t_0 = 0$ and $t_1 = 1$. Thus, $a = \frac{1}{\alpha-\beta}$ and $b = \frac{-1}{\alpha-\beta}$, so that from (2.1), we have

$$t_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{2.4}$$

ACCEPTED MANUSCRIPT

for $n \geq 0$. The divisibility properties of Lucas sequences have been extensively studied, see for example [12, 4, 25], and for these binary recurrence sequences, Theorem 1.3 gives an improvement on Theorem 1.2.

It is not difficult to show that if $\{u_n\}_{n=1}^{\infty}$ is a non-degenerate binary recurrence sequence then

$$\omega\left(\prod_{\substack{n=1\\u_n\neq 0}}^{N} u_n\right) \ll_{a,b} N^2/\log N. \tag{2.5}$$

To see this suppose that u_n is given by (2.1) with $|\alpha| \geq |\beta|$. Then,

$$|u_n| \leq (|a|+|b|)|\alpha|^n$$

and therefore,

$$\left|\prod_{\substack{n=1\\u_n\neq 0}}^{N} u_n\right| \leq (|a|+|b|)^N |\alpha|^{N(N+1)/2}. \tag{2.6}$$

Let $2 = p_1, p_2, \ldots$ be the sequence of prime numbers. By the Prime Number Theorem

$$\prod_{i=1}^{t} p_i = e^{(1+o(1))t\log t}. \tag{2.7}$$

Observe that if

$$\prod_{i=1}^{t} p_i \geq \left|\prod_{\substack{n=1\\u_n\neq 0}}^{N} u_n\right|.$$

then

$$\omega\left(\prod_{\substack{n=1\\u_n\neq 0}}^{N} u_n\right) \leq t.$$

Thus (2.5) follows from (2.6), (2.7), and Lemma 2.1.

We hypothesize that those bounds could be improved according to Conjecture 1.4.

3. Preliminaries for the proof of Theorem 1.2

The first two results we require concern prime divisors of Lucas numbers.

Proposition 3.1. *Let $\{t_n\}_{n=0}^{\infty}$ be a Lucas sequence, as in (2.4), with $|\alpha| \geq |\beta|$. If p is a prime number not dividing $\alpha\beta$, then p divides t_n for some positive integer n and if ℓ is the smallest such n, then*

$$\frac{\log p - \frac{\log 2}{2}}{\log|\alpha|} \leq \ell \leq p+1.$$

Proof. Apart for the lower bound, this is Lemma 7 of [23]. The lower bound follows from $p \leq |t_\ell| \leq \sqrt{2}\,|\alpha|^\ell$.

Indeed, note that $|\alpha-\beta| = \left|\sqrt{r^2+4s}\right|$ and therefore either $|\alpha-\beta| \geq \sqrt{2}$, in which case the triangle inequality yields the desired result, or $|\alpha-\beta| = 1$. In this case, we have that

$$|t_n| = |\alpha|^n \left|\frac{2}{r+1}\right|^n \leq \alpha^n \leq \sqrt{2}\alpha^n$$

since the cases $r = 0, -1, -2$ are either degenerate or can't yield $r^2 - 4s = 1$. □

For any rational number x let $|x|_p$ denote the p-adic value of x, normalized so that $|p|_p = p^{-1}$.

ACCEPTED MANUSCRIPT

Proposition 3.2. *Let $\{t_n\}_{n=0}^{\infty}$ be a Lucas sequence, as in (2.4), with $\alpha+\beta$ and $\alpha\beta$ coprime. Let p be a prime number which does not divide $\alpha\beta$, let ℓ be the smallest positive integer for which p divides t_ℓ and let n be a positive integer. If ℓ does not divide n, then*

$$|t_n|_p = 1.$$

If $n=\ell k$ for some positive integer k, we have, for $p>2$,

$$|t_n|_p = |t_\ell|_p \, |k|_p \,,$$

while for $p=2$,

$$|t_n|_2 = \begin{cases} |t_\ell|_2 & \text{for } k \text{ odd} \\ 2\,|t_{2\ell}|_2\,|k|_2 & \text{for } k \text{ even.} \end{cases}$$

Proof. This is Lemma 8 of [23] and it is based on work of Carmichael [4], see also [25]. □

In addition to the results about Lucas sequences, we need an estimate from below for the size of the n-th term of a non-degenerate binary recurrence sequence.

Proposition 3.3. *Let u_n be the n-th term of a non-degenerate binary recurrence sequence as in (2.1). There exist positive numbers c_0 and c_1, which are effectively computable in terms of a and b, such that for all $n>c_1$,*

$$|u_n| \geq |\alpha|^{n-c_0\log n}.$$

Proof. This is Lemma 6 in [23] and is a consequence of Baker's theory of linear forms in logarithms. □

4. The proof of Theorem 1.2

It suffices to prove the result under the assumption that $\alpha+\beta$ and $\alpha\beta$ are coprime or, equivalently, that r and s are coprime. We shall also suppose, without loss of generality, that

$$|\alpha| \geq |\beta|.$$

In the following discussion, every c_i will denote a positive number effectively computable in terms of a, b, α and β. For any prime p let $[p]$ denote the principal ideal generated by p in the ring of algebraic integers of $\mathbb{Q}(\alpha)$. Put

$$a' = (\alpha-\beta)a, \;\; b' = (\alpha-\beta)b.$$

Let p be a prime which divides $\alpha\beta$ and let $\mathfrak{p}$ be a prime ideal which divides $[p]$. Then, since $\alpha+\beta$ and $\alpha\beta$ are coprime integers, $\mathfrak{p}$ divides either $[\alpha]$ or $[\beta]$. Thus, by (2.1) for $m>c_1$ we have

$$|u_m|_p \geq \left|a'b'\right|_p. \tag{4.1}$$

It follows from Proposition 3.3 that u_m is non-zero for $m>c_2$. Put

$$\gamma = 1-1/\sqrt{2}.$$

Then γN exceeds both c_1 and c_2 for $N>c_3$. For each positive integer N with $N>c_3$, put

$$S = S(N) := \prod_{\gamma N < n \leq N} u_n.$$

Our proof proceeds by a comparison of estimates for S.

By Proposition 3.3, there exists c_4 such that

$$|S| \geq \prod_{\gamma N < n \leq N} |\alpha|^{n-c_4\log n}$$

and so

$$|S| \geq |\alpha|^{\frac{(1-\gamma^2)N^2}{2} - c_5 N\log N}. \tag{4.2}$$

Plainly,

$$|S| = \prod_{p\mid S} |S|_p^{-1}.$$

ACCEPTED MANUSCRIPT

We first estimate $|S|_p^{-1}$ for primes p which divide $\alpha\beta$. By (4.1), we have

$$|S|_p^{-1} \leq \left|a'b'\right|_p^{-N}.$$

We shall now estimate $|S|_p^{-1}$ for primes p which divide S but do not divide $\alpha\beta$. For each such prime p, we let $n(p)$ be the smallest integer with $\gamma N < n(p) \leq N$ for which

$$\left|u_{n(p)}\right|_p \leq |u_n|_p \qquad \text{for } \gamma N < n \leq N.$$

For positive integers m and r with $m \geq r$,

$$u_m - \beta^r u_{m-r} = a'\alpha^{m-r} t_r, \tag{4.3}$$

with t_r as in (2.4).

Let $|\ \ |_p$ denote an extension of $|\ \ |_p$ from $\mathbb{Q}$ to $\mathbb{Q}(\alpha)$. For each integer r with $1 \leq r < n(p) - \gamma N$,

$$|a'b't_r|_p \leq |a't_r|_p = |a'\alpha^{n(p)-r}t_r|_p$$

and, by (4.3) with $m = n(p)$,

$$|a'\alpha^{n(p)-r}t_r|_p \leq \max(|u_{n(p)}|_p, |\beta^r u_{n(p)-r}|_p).$$

Since $|\beta|_p = 1$,

$$\max(|u_{n(p)}|_p, |\beta^r u_{n(p)-r}|_p) = \max(|u_{n(p)}|_p, |u_{n(p)-r}|_p) = |u_{n(p)-r}|_p,$$

and we deduce that

$$|a'b't_r|_p \leq |u_{n(p)-r}|_p$$

for $1 \leq r < n(p) - \gamma N$. Hence,

$$\left|\prod_{\gamma N < n < n(p)} u_n\right|_p \geq \prod_{1 \leq r < n(p) - \gamma N} \left(|t_r|_p \left|a'b'\right|_p\right).$$

Letting $\ell = \ell(p)$ be the smallest integer for which $p | t_\ell$, we have by Proposition 3.1 and Proposition 3.2 that if $p > 2$,

$$\prod_{1 \leq r < n(p) - \gamma N} |t_r|_p = |t_\ell|_p^{s_1} \left|s_1!\right|_p,$$

where $s_1 = \left\lfloor \frac{n(p) - \gamma N}{\ell} \right\rfloor$, while for $p = 2$,

$$\prod_{1 \leq r < n(2) - \gamma N} |t_r|_2 = |t_\ell|_2^{s_1} \left|\frac{t_{2\ell}}{t_\ell}\right|_2^{s_2} \left|s_2!\right|_2,$$

with $s_2 = \left\lfloor \frac{n(2) - \gamma N}{2\ell} \right\rfloor$.

Next, on setting $m - r = n(p)$ and letting r run over those integers such that $n(p) + r \leq N$, we find that for $p > 2$

$$\prod_{n(p) < n \leq N} |u_n|_p \geq |t_\ell|_p^{s_3} \left|s_3!\right|_p \left|a'b'\right|_p^{N - n(p)},$$

while for $p = 2$,

$$\prod_{n(2) < n \leq N} |u_n|_2 \geq |t_\ell|_2^{s_4} \left|\frac{t_{2\ell}}{t_\ell}\right|_2^{s_4} \left|s_4!\right|_2 \left|a'b'\right|_p^{N - n(2)},$$

where

$$s_3 = \left\lfloor \frac{N - n(p)}{\ell} \right\rfloor \quad \text{and} \quad s_4 = \left\lfloor \frac{N - n(2)}{2\ell} \right\rfloor.$$

Putting all this together gives, for $p > 2$,

$$|S|_p^{-1} \leq |t_\ell|_p^{-s} \left|s!\right|_p^{-1} \left|a'b'\right|_p^{-N} \left|u_{n(p)}\right|_p^{-1}$$

ACCEPTED MANUSCRIPT

where $s = \left\lfloor \frac{N-\gamma N}{\ell} \right\rfloor$. As $|t_\ell|_p^{-1} \le |t_\ell| \le 2\,|\alpha|^\ell$, we find that

$$|S|_p^{-1} \le 2^{\frac{N}{\ell(p)}}\,|\alpha|^{N-\gamma N}\,|N!|_p^{-1}\,\left|a'b'\right|_p^{-N}\,\left|u_{n(p)}\right|_p^{-1}$$

for $p > 2$. For $p = 2$ we similarly have

$$|S|_2^{-1} \le 4^{\frac{N}{\ell(2)}}\,|\alpha|^{2(N-\gamma N)}\,|N!|_2^{-1}\,\left|a'b'\right|_2^{-N}\,\left|u_{n(2)}\right|_2^{-1}.$$

Putting $T = \omega(S)$, we may suppose $T < N$ for otherwise we are done. Inserting the above estimates, we obtain

$$S = \prod_{p|S} |S|_p^{-1} \le \left(\prod_{p|S} 4^{\frac{N}{\ell(p)}}\right) |\alpha|^{(N-\gamma N)(T+1)}\,N!\,\left|a'b'\right|^N \prod_{p|S} \left|u_{n(p)}\right|_p^{-1}. \tag{4.4}$$

We need to estimate the right hand side and compare it with (4.2). Note that

$$\begin{aligned}\prod_{p|S} 4^{\frac{N}{\ell(p)}} &\le \prod_{\substack{p|S\\ p<T/\log T}} 4^N \cdot \prod_{\substack{p|S\\ p>T/\log T}} 4^{\frac{N}{\ell(p)}}\\ &\le 4^{NT/\log T} \cdot \prod_{\substack{p|S\\ p>T/\log T}} 4^{\frac{N}{\ell(p)}}.\end{aligned}$$

However, by Proposition 3.1,

$$\ell(p) \ge \frac{\log p - \log 2}{\log|\alpha|} > \frac{\log T - \log\log T - \log 2}{\log|\alpha|}.$$

As $|\alpha| \ge \sqrt{2}$, we deduce

$$\prod_{p|S} 4^{\frac{N}{\ell(p)}} < e^{c_8 N^2/\log N}.$$

Inserting this in inequality (4.4) and using $N! \le N^N$, we get

$$\prod_{p|S} |S|_p^{-1} < e^{c_9 N^2/\log N}\,|\alpha|^{N(1-\gamma)T} \prod_{p|S} \left|u_{n(p)}\right|_p^{-1}.$$

For each n, we have $|u_n| \le (|a|+|b|)\,|\alpha|^n$, since $|\alpha| \ge |\beta|$. Put

$$K \coloneqq \{n(p) : p|S\}.$$

Then, $|K| \le T$. Thus,

$$\prod_{p|S} \left|u_{n(p)}\right|_p^{-1} \le \prod_{k\in K} |u_k| \le \prod_{k\in K} (|a|+|b|)\,|\alpha|^k \le (|a|+|b|)^T\,|\alpha|^{NT-\frac{T(T-1)}{2}}.$$

Putting everything together, we get

$$\prod_{p|S} |S|_p^{-1} \le e^{c_{10}N^2/\log N}\,|\alpha|^{(2-\gamma)NT-\frac{T^2}{2}},$$

and as $|\alpha| \ge \sqrt{2}$, we get from (4.2)

$$|\alpha|^{\frac{N^2(1-\gamma^2)}{2}} < e^{c_{11}N^2/\log N}\,|\alpha|^{(2-\gamma)NT-\frac{T^2}{2}}.$$

Therefore $T > (1-1/\sqrt{2}-\epsilon)N$ for $N > c_{12}$ since the roots of the quadratic $x^2-(4-2\gamma)x+1-\gamma^2$ are γ and $\gamma+2\sqrt{2}$.

ACCEPTED MANUSCRIPT

5. The proof of Theorem 1.3

Let $\{t_n\}_{n=1}^{\infty}$ be a non-degenerate Lucas sequence with n-th term given by (2.4). We may assume, without loss of generality, that $\alpha+\beta$ and $\alpha\beta$ are coprime. A primitive divisor of t_n is a prime p which divides t_n but does not divide $(\alpha-\beta)^2 t_2 \cdots t_{n-1}$. In [24], Stewart showed that there are only finitely many Lucas sequences, with $\alpha+\beta$ and $\alpha\beta$ coprime, for which t_n does not possess a primitive divisor when $n>4$ and $n\neq 6$, and these sequences may be explicitly determined. It then follows that the number of distinct prime factors of $\prod_{n=1}^{N} t_n$ is at least $N-5$ whenever $\{t_n\}_{n=1}^{\infty}$ is not an exceptional sequence. Bilu, Hanrot and Voutier [1] determined the complete list of exceptional sequences, and by examining the list we see that whenever $\{t_n\}_{n=1}^{\infty}$ is a non-degenerate Lucas sequence,

$$\omega\left(\prod_{n=1}^{N} t_n\right) \geq N-9,$$

with equality holding when t_n satisfies

$$t_n = t_{n-1} - 2t_{n-2} \ \ for \ \ n=2,3,...$$

and $N = 30, 31, 32, 33$ or 34.

6. Proof of Theorem 1.1

First, notice that the set of interest

$$S_x = \left\{p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p\rangle \subset \mathbb{F}_p^*\right\}$$

can be expressed as

$$S_x = \{p \leq x \text{ prime } : p|(a^n-b) \text{ for some } n\}.$$

Suppose that p divides a^n-b with $n \leq \left\lfloor \frac{\log x}{\log a} \right\rfloor =: N$. Then, $p \leq a^n - b < a^n \leq x$.

Therefore, it is clear that

$$\#S_x \gg \#\{p \text{ prime } : p|(a^n-b) \text{ for some } n \leq N\}.$$

Consider the binary recurrence sequence given by $u_n = a^n - b$ (here α, β, a and b in (2.1) are respectively a, 1, 1 and b). Then, by Theorem 1.2,

$$\#\{p : p|a^n - b \text{ for some } n \leq N\} \gg N$$

for $N = \left\lfloor \frac{\log x}{\log|a|} \right\rfloor$, and so

$$\#\{p \leq x : p|a^n - b \text{ for some } n\} \gg \log x.$$

7. Theorem 1.5 via the greatest prime factor of terms of recurrence sequences

The first proof uses the following result by Stewart about the growth of the largest prime divisor in a type of recurrence sequence.

For any integer n let $P(n)$ denote the greatest prime factor of n with the convention that $P(0) = P(1) = P(-1)$.

Theorem 7.1 (Stewart [26]). *Let u_n, as in (2.1), be the n-th term of a non-degenerate binary recurrence sequence. There exists a positive number C, which is effectively computable in terms of a, b, α and β, such that, for $n > C$,*

$$P(u_n) > \sqrt{n}\exp(\log n/104\log\log n).$$

We actually need a special case of this result. Note that for $\alpha = 1$, $x = a$, $\beta = b$ and $y = 1$, the above theorem yields

$$P(a^n - b) \gg_{a,b} \sqrt{n}\exp(\log n/104\log\log n).$$

This is what we will be using.

ACCEPTED MANUSCRIPT

Proof of Theorem 1.5. We will prove the theorem for the case $a, b > 0$ for simplicity. The proof can be easily adapted to the general case. See the remark for more details. Again, let

$$S_x = \left\{p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p \rangle \subset \mathbb{F}_p^*\right\}.$$

Using the same argument as in section 6, we have

$$\#S_x \gg \#\{p \text{ prime } : p|(a^n - b) \text{ for some } n \leq N\},$$

for $N := \left\lfloor \frac{\log x}{\log a} \right\rfloor$.

Consider the sequence $\xi_n = a^n - b$ for $N - y \leq n \leq N$ where y is a parameter to be chosen later. As noted above, $p|\xi_n$ in this range implies $p \leq x$. Now consider $P(a^n - b)$, the largest prime factor of $a^n - b$, for each of those n. Those yield y primes, albeit a priori not necessarily distinct.

Suppose that for some m and n with $N - y \leq m < n \leq N$, we have

$$P(a^n - b) = P(a^m - b) =: q.$$

Then, $a^n \equiv b \bmod q$ and $a^m \equiv b \bmod q$, so

$$a^{nm} \equiv b^n \equiv b^m \bmod q,$$

meaning that q divides $b^n - b^m$.

From Theorem 7.1, we know that q exceeds b for x large enough, and so q does not divide b. We conclude that $q|(b^{n-m} - 1)$. In particular, we have that $q \leq b^{n-m} - 1 < b^{n-m}$. However, $n - m \leq y$, and so choosing $y = \frac{\log(C_1\sqrt{N})}{\log b}$ yields

$$P(a^n - b) = q < b^{n-m} \leq C_1\sqrt{N},$$

which is a contradiction to Theorem 7.1 for properly chosen C_1.

We therefore have y distinct primes in the set S_x, where

$$y = \frac{\log\log x}{2\log b} + C' \gg \log\log x.$$

□

8. Theorem 1.5 via Thue equations

The second proof of Theorem 1.5 uses a result on Thue equations. Recall that a Thue equation is an equation of the form

$$F(x, y) = h,$$

where $F(x, y) = a_0x^r + a_1x^{r-1}y + \cdots + a_ry^r$ is an integral binary form of degree at least 3. We have the following result for the number of solutions to such an equation.

Theorem 8.1 (Bombieri, Schmidt [3])**.** *Let $F(x, y)$ be an irreducible binary form of degree $r \geq 3$ with rational integral coefficients. The number of primitive solutions of the equation*

$$|F(x, y)| = h$$

does not exceed

$$c_1r^{t+1},$$

where c_1 is an absolute constant and t is the number of distinct prime factors of h.

We now proceed with our second proof of Theorem 1.5. For this particular proof, we require the extra condition that a and b are coprime. However, this condition is not too restrictive and we believe the proof to still have its merits.

Proof of Theorem 1.5. Suppose that $(a, b) = 1$. As in the previous proof, notice that

$$S_x = \{p \leq x \text{ prime } : p|(a^n - b) \text{ for some } n\}.$$

Fix x. Then, again,

$$\#S_x \gg \#\{p \text{ prime } : p|(a^n - b) \text{ for some } n \leq N\} \tag{8.1}$$

where $N := \left\lfloor \frac{\log x}{\log a} \right\rfloor$. Denote by k the quantity on the right hand side of (8.1).

ACCEPTED MANUSCRIPT

Since there are at most k primes dividing the numbers $a^n - b$ with n varying, we can write

$$a^n - b = p_1^{\alpha_1(n)} p_2^{\alpha_2(n)} \cdots p_k^{\alpha_k(n)}$$

with p_i distinct primes, and $\alpha_i(n) = \mathrm{ord}_{p_i}(a^n - b)$.

For every fixed n, we have

$$a^\delta a^{3j} - p_1^{\epsilon_1} \cdots p_k^{\epsilon_k} p_1^{3j_1} \cdots p_k^{3j_k} = b$$

where δ and ϵ_i are the residue of n and $\alpha_i(n)$ modulo 3 respectively ($\delta, \epsilon_i \in \{0, 1, 2\}$). We obtain the equation

$$a^\delta \left(a^j\right)^3 - \left(p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}\right) \left(p_1^{j_1} \cdots p_k^{j_k}\right)^3 = b.$$

As n varies, we obtain at most 3^{k+1} different equations of the form

$$a^\delta X^3 - \left(p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}\right) Y^3 = b.$$

The binary form on the left hand side is irreducible unless $\delta = 0$ and all $\epsilon_i = 0$. This last case is easily dismissed because, by (2.2), $|S_x|$ goes to infinity in x, and therefore so does Y. However, $X^3 - Y^3 = b$ implies that both $X - Y$ and $X^2 + XY + Y^2$ divide b. However, since b is fixed, this implies that there are only finitely many choices for X and Y, which is a contradiction.

Also, every single $n \leq N$ gives a different solution to one of those equations. All the solutions are primitive since $(a, b) = 1$. Therefore, one equation has at least $\frac{N}{3^{k+1}}$ solutions.

Let $C = c_1 3^{1+t}$, where t is the number of prime factors of b, and c_1 is the constant appearing in Theorem 8.1. Then, $\frac{N}{3^{k+1}} > C$ would be a contradiction to Theorem 8.1, and so we have that

$$\frac{N}{3^{k+1}} \leq C,$$

that is $N \ll 3^k$ and so $\log N \ll k$. Recall from the definition of N that $N \gg \log x$, hence

$$\log\log x \ll_{a,b} k,$$

which completes the proof. It is worth noting that the dependence on a and b can easily be made explicit as

$$k \gg \log\log x - \log\log a - \omega(b),$$

where $\omega(b)$ denotes the number of distinct prime factors of b, and the implicit constant is absolute. □

9. Theorem 1.5 via Mumford's gap principle

This proof uses Mumford's theorem about counting points on curves using a height function.

Theorem 9.1 (Mumford [9], [16]). *Let C/K be a curve of genus $g \geq 2$ defined over a number field. Then, there is a constant c depending on C/K and the height function H used, such that*

$$\#\{P \in C(K) : H(P) \leq T\} \leq c \log\log T$$

for all $T \geq e^e$, where H is a fixed multiplicative height function on C.

It is important to note that we can make the constant c in Theorem 9.1 depend only on the field $\overline{K}$. As such, we can apply the theorem to quadratic twists of the same curve with the same constant for each of them. See [11, Lemma 5] for a proof of this fact.

Proof of Theorem 1.5. The general idea of this proof is similar to that of section 8. As before,

$$\#S_x \gg \#\{p \text{ prime } : p | (a^n - b) \text{ for some } n \leq N\} \tag{9.1}$$

where $N := \left\lfloor \frac{\log x}{\log a} \right\rfloor$. Denote by k the quantity on the right hand side of (9.1).

Again, write

$$a^n - b = p_1^{\alpha_1(n)} p_2^{\alpha_2(n)} \cdots p_k^{\alpha_k(n)}$$

ACCEPTED MANUSCRIPT

with p_i distinct primes, and $\alpha_i(n) = \mathrm{ord}_{p_i}(a^n - b)$. This time, we consider only the n divisible by 5, and write

$$a^{5j} - p_1^{\epsilon_1} \cdots p_k^{\epsilon_k} p_1^{2j_1} \cdots p_k^{2j_k} = b,$$

where ϵ_i are the residue of $\alpha_i(n)$ modulo 2, so we obtain the equation

$$\left(p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}\right) \left(p_1^{j_1} \cdots p_k^{j_k}\right)^2 = \left(a^j\right)^5 - b.$$

Now, consider the curve given by the equation

$$C_b : Y^2 = X^5 - b.$$

We know this to be a hyperelliptic curve over $\mathbb{Q}$, and thus a curve of genus $g \geq 2$. Also, if we let $D_n = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$, we can consider the quadratic twist

$$C_{b,D_n} : D_n Y^2 = X^5 - b.$$

However, any point (x, y) on this new curve would give

$$\begin{aligned} D_n y^2 &= x^5 - b \\ (\sqrt{D_n} y)^2 &= x^5 - b, \end{aligned}$$

and so simply amounts to a point on $C_b\left(\mathbb{Q}\left(\sqrt{D_n}\right)\right)$.

From above, we see that every $n \equiv 0 \bmod 5$ gives a solution to the curve C_{b,D_n}. Since the X coordinate of those points are distinct, it is clear that the points are distinct. As n varies over multiples of 5 between 0 and N, we get $\left\lfloor \frac{N}{5} \right\rfloor$ distinct solutions to at most 2^k different curves. It follows that one of these curves has at least $\frac{N}{5 \cdot 2^k}$ solutions.

Consider the "naïve" multiplicative height function on C_{b,D_n} given by $H(P) = \max\{|x|, |d|\}$, where $P = \left(\frac{x}{d^2}, \frac{y}{d^3}\right)$ with x, y and d integers, and $(x, d) = (y, d) = 1$.

Then, note that all the solutions produced above for the curves C_{b,D_n} have height at most a^N. We then apply Mumford's theorem with this height function to conclude that

$$\#\left\{P \in C_{b,D_n}(\mathbb{Q}) : H(P) \leq a^N\right\} \leq c \log\log a^N.$$

By the previous comment on quadratic twists,

$$\#\left\{P \in C_b\left(\mathbb{Q}\left(\sqrt{D_n}\right)\right) : H(P) \leq a^N\right\} \leq c \log\log a^N.$$

Note that our previous comment about the independence of the constant on the field in Mumford's theorem allows us to have the constant c here be independent of n. Hence, by the above

$$\frac{N}{5 \cdot 2^k} \leq c \log\log a^N,$$

and therefore $k \gg \log N \gg \log\log x$. □

We want to point out that even if all three proofs give bounds of the same order of magnitude with respect to x, the dependence of the implied constants on a and b vary for each approach. For example, the proof in section 8 reduces the dependence on b dramatically. Note also that the dependence on b of the implicit constant in section 9 is harder to make explicit as the constant given from Mumford's theorem depends on b. However, we see that the proof of section 8 requires an extra condition on a and b to use Theorem 8.1, albeit a mild one.

In any case, as all three proofs use ideas fundamentally different from each other, we believe that they are of independent interest.

ACCEPTED MANUSCRIPT

10. Second order recurrence sequences

In [15], Moree and Stevenhagen actually consider the two-variable problem with a and b rational numbers (and then disregard the finitely many primes dividing their numerators or denominators). Here, for clarity, we restricted our attention to integers. However, it is not very hard to retrieve our results in the case where a and b are rational numbers.

Write $a = \frac{a_1}{a_2}$ and $b = \frac{b_1}{b_2}$ with $\gcd(a_1, a_2) = \gcd(b_1, b_2) = 1$. Then, the set of primes we are interested in counting,

$$S_x = \left\{p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p \rangle \subset \mathbb{F}_p^*\right\},$$

can be written as

$$S_x = \{p \leq x \text{ prime } : p | (b_2 a_1^n - b_1 a_2^n) \text{ for some } n\}.$$

The sequence $(b_2 a_1^n - b_1 a_2^n)$ is a linear recurrence sequence of order 2 and so we may again apply Theorem 7.1.

For the proof of section 9, it is also easy to generalize the argument. Indeed, following the same notation, we can write for $n \equiv 0 \bmod 10$

$$b_2 a_1^n - b_1 a_2^n = p_1^{2j_1+\epsilon_1} \cdots p_k^{2j_k+\epsilon_k}$$
$$\left(p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}\right) \left(\frac{p_1^{j_1} \cdots p_k^{j_k}}{a_1^{n/2}}\right)^2 = b_2 \left(\frac{a_1^{n/5}}{a_2^{n/5}}\right)^5 - b_1,$$

which gives the rational solution $\left(\frac{a_1^{n/5}}{a_2^{n/5}}, \frac{p_1^{j_1} \cdots p_k^{j_k}}{a_1^{n/2}}\right)$ to the hyperelliptic curve $D_n Y^2 = b_2 X^5 - b_1$. Since Mumford's theorem considers any rational solutions, and since the height of these solutions is again at most $\max\{|a_1^N|, |a_2^N|\} \sim x$, the rest of the proof goes through unchanged.

The proof in section 8 is trickier to generalize. Indeed, the result from Bombieri and Schmidt we use considers only integral solutions to the Thue equation.However, similarly to what we did above, we need here a bound on the number of S-integer solutions to the Thue equation. This is given by Evertse in [5].

Theorem 10.1 (Evertse, [5]). *Let $F(X, Y)$ be an irreducible binary form of degree $n \geq 3$, and let $\{p_1, \ldots, p_t\}$ be a (possibly empty) set of distinct prime numbers. Then, the equation*

$$|F(x, y)| = p_1^{k_1} \cdots p_t^{k_t}$$

has at most

$$2 \times 7^{n^3(2t+3)}$$

solutions $(x, y, k_1, \ldots, k_t) \in \mathbb{Z}^{t+2}$ with $(x, y) = 1$.

Therefore, for $a = r/s$ and $b = u/v$ rational numbers, we get the equation

$$vr^\delta \left(r^j\right)^3 - \left(vp_1^{\epsilon_1} \cdots p_k^{\epsilon_k}\right) \left(p_1^{j_1} \cdots p_k^{j_k}\right)^3 = s^{3j+\delta} u.$$

We can therefore apply the above theorem and follow the same argument as before.

11. Proof of Theorem 1.6

This proof mainly relies on the following theorem of Gupta and Murty.

Theorem 11.1 (Gupta, Murty [7]). *Fix a, b coprime integers. There exists a constant $c > 0$ such that*

$$\#\left\{p \leq x \text{ prime } : p - 1 = 2P_2(x) \text{ and } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1\right\} \geq \frac{cx}{(\log x)^2},$$

where $P_2(x)$ is the set of numbers n that can be written either as $n = q_1$ or as $n = q_1 q_2$, in both cases with q_1 and q_2 primes such that $x^{1/4+\epsilon} < q_1 < q_2$.

ACCEPTED MANUSCRIPT

Proof of Theorem 1.6. We start by considering only the primes in the set

$$T_x = \left\{ p \leq x \text{ prime } : p-1 \in 2P_2(x) \text{ and } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1 \right\},$$

and ask how many of them are also in our set of interest

$$S'_x = \left\{ p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p \rangle \text{ or } \langle b \bmod p \rangle = \mathbb{F}_p^* \right\}.$$

Let $p \in T_x$, and let $f_p(a)$ and $f_p(b)$ denote the order of a and b respectively in $\mathbb{F}_p^\times$. Since by assumption both a and b are not squares modulo p, it follows that 2 divides $f_p(a)$ and $f_p(b)$. From the definition of T_x, either $p-1 = 2q_1$ or $p-1 = 2q_1q_2$ with q_1, q_2 primes, and $x^{1/4+\epsilon} < q_1 < q_2$.

Case 1 Suppose $p-1 = 2q_1$. Since $f_p(a) \neq 2$, then $f_p(a) = 2q_1$ and so a is a primitive root for $\mathbb{F}_p^\times$. p is therefore trivially in S'_x.

Case 2 Suppose $p-1 = 2q_1q_2$. There are three possibilities.

Case 2.1 $f_p(a) = 2q_1q_2$. Then, a is a primitive root modulo p.

Case 2.2 $f_p(a) = 2q_2$.

Case 2.3 $f_p(a) = 2q_1$. We now show that this case does not happen too often. Here, clearly, $x^{1/4+\epsilon} < q_1 < \sqrt{x}$. We then count the number of $p \in T_x$ that produce this situation. We do so by splitting the range of the possible q_1.

Case 2.3a Suppose that $x^{1/4+\epsilon} < q_1 < \frac{\sqrt{x}}{\log x}$. Since $f_p(a) = 2q_1$, p divides $a^{2q_1} - 1$, and the number of such primes when ranging over possible q_1 is

$$\ll \sum_{x^{1/4+\epsilon} < q_1 < \sqrt{x}/\log x} \frac{2q_1}{\log x} \ll \frac{x}{(\log x)^3},$$

where we use that $\omega(n) \ll \log n / \log\log n$. This is a result due to Ramanujan. In fact, he proves [19] that

$$\omega(n) \leq \frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right).$$

Case 2.3b Suppose that $\frac{\sqrt{x}}{\log x} \leq q_1 < \sqrt{x}$. Since $p-1 = 2q_1q_2$, then we know that $\frac{p-1}{2q_1}$ has no small prime factor (in particular is equal to q_2). By a theorem of Bombieri, Friedlander and Iwaniec [2], we know that for fixed $q_1 < \sqrt{x}$,

$$\# \left\{ p \leq x \text{ prime } : \frac{p-1}{2q_1} \text{ has no small prime factors} \right\} \ll \frac{x}{q_1 (\log x)^2}.$$

Thus, summing over all possible q_1 in the range, we get that the number of primes p that contribute to this case is

$$\ll \frac{x}{(\log x)^2} \sum_{\frac{\sqrt{x}}{\log x} \leq q_1 < \sqrt{x}} \frac{1}{q_1}.$$

Since we know that $\sum_{p<x} \frac{1}{p} = \log\log x + c + O\left(\frac{1}{\log x}\right)$, we get

$$\begin{aligned}
\sum_{\frac{\sqrt{x}}{\log x} \leq q_1 < \sqrt{x}} \frac{1}{q_1} &= \log\log\sqrt{x} - \log\log\frac{\sqrt{x}}{\log x} + O\left(\frac{1}{\log x}\right) \\
&= \log\left(\frac{\frac{1}{2}\log x}{\frac{1}{2}\log x - \log\log x}\right) O\left(\frac{1}{\log x}\right) \\
&= -\log\left(1 - \frac{2\log\log x}{\log x}\right) + O\left(\frac{1}{\log x}\right).
\end{aligned}$$

ACCEPTED MANUSCRIPT

For x large enough, $\frac{2\log\log x}{\log x}$ is small, and for small y, $-\log(1-y) \sim y$. We then get

$$\sum_{\frac{\sqrt{x}}{\log x} \leq q_1 < \sqrt{x}} \frac{1}{q_1} \ll \frac{\log\log x}{\log x}.$$

Therefore,

$$\frac{x}{(\log x)^2} \sum_{\frac{\sqrt{x}}{\log x} \leq q_1 < \sqrt{x}} \frac{1}{q_1} \ll \frac{x \log\log x}{(\log x)^3}.$$

From the bounds we get in cases 2.3a and 2.3b, we conclude that the number of primes p in T_x yielding the case 2.3 is negligible compared to the total number of primes in T_x, which is at least $\frac{cx}{(\log x)^2}$. We thus have that

$$|\{p \in T_x : a \text{ is a primitive root } \bmod p \text{ or } f_p(a) = 2q_2\}| \gg \frac{x}{(\log x)^2}.$$

We can repeat the whole argument for b instead of a with T_x replaced with the set above. We then get

$$\left|\left\{p \leq x \text{ prime } : \begin{array}{c} a \text{ is a primitive root } \bmod p \text{ or } f_p(a) = 2q_2 \text{ and} \\ b \text{ is a primitive root } \bmod p \text{ or } f_p(b) = 2q_2 \end{array}\right\}\right| \gg \frac{x}{(\log x)^2}.$$

Now, if either a or b is a primitive root modulo p, then $p \in S'_x$. Also, if $f_p(a) = f_p(b) = 2q_2$, then $\langle b\rangle = \langle a\rangle$ and so $p \in S'_x$ as well.

We thus conclude that $|S'_x| \gg \frac{x}{(\log x)^2}$ as desired. □

12. Concluding remarks

The original Artin conjecture was proved conditionally on the generalized Riemann hypothesis by Hooley ([10]). The two-variable Artin conjecture was also proved conditionally on the generalized Riemann hypothesis by Moree and Stevenhagen ([15]). However, Theorem 1.6 suggests that we might not need the generalized Riemann hypothesis to show that at least one of them is true.

13. Acknowledgments

We would like to thank Professors Pieter Moree, Damien Roy, Peter Stevenhagen and the referee for helpful comments on a previous version of this paper.

References

[1] Y. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539**, 75-122 (2001)
[2] E. Bombieri, J.B. Friedlander, H. Iwaniec, Primes in Arithmetic Progressions to Large Moduli II, *Math. Ann.* **277**, 361–393 (1987)
[3] E. Bombieri, W.M. Schmidt, On Thue's equation, *Invent. Math.* **88**, 69–81 (1987)
[4] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Annals of Math. (2) **15**, 30–70 (1913)
[5] J.-H. Evertse. On equations in S-units and the Thue-Mahler equation. *Invent. Math.*, **75** no.3, 561–584 (1984)
[6] A. O. Gelfond, Selected Works [in Russian], Nauka, Moscow (1973)
[7] R. Gupta, M. Ram Murty, A remark on Artin's conjecture. *Invent. Math.* **78**, 127–130 (1984)
[8] D. R. Heath-Brown, Artin's conjecture for primitive roots, *The Quarterly Journal of Mathematics* **37** no. 1, 27–38 (1986)
[9] M. Hindry, J. H. Silverman, Diophantine Geometry: An introduction, GTM 201, Springer-Verlag, Berlin (2000)
[10] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225**, 209–220 (1967)
[11] J. Lee, M. Ram Murty, An application of Mumford's gap principle, *Journal of Number Theory* **105**, 333–343 (2004)
[12] E. Lucas, Théorie des fonctions numériques simplement périodiques, *American J. Math.* **1**, 184-240, 289-321 (1878)
[13] K. Mahler, Eine arithmetische Eigenschaft der rekurrierenden Reihen, *Mathematica(Leiden)* **3**, 153-156 (1934-1935). Retrieved June 19, 2018 from `https://carma.newcastle.edu.au/mahler/docs/025.pdf`
[14] P. Moree, Artin's primitive root conjecture - a survey, *Integers* **12** no.6, 1305–1416 (2012)
[15] P. Moree, P. Stevenhagen, A Two-Variable Artin Conjecture, *Journal of Number Theory* **85**, 291–304 (2000)
[16] D. Mumford, A Remark on Mordell's Conjecture, *American Journal of Mathematics* **87** no. 4, 1007–1016 (1965)

ACCEPTED MANUSCRIPT

[17] M. Ram Murty, On Artin's Conjecture, *Journal of Number Theory* **16**, 147–168 (1983)
[18] G. Pólya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. Reine Angew. Math.* **151**, 1–31 (1921)
[19] S. Ramanujan, Highly Composite Numbers, *Proc. London Math. Soc.* **2** XIV, 347–409 (1915)
[20] I. E. Shparlinski, Prime divisors of recurrence sequences, *Izv. Vyssh. Uchebn. Zaved.* **4**, 100-103 (1980)
[21] I. E. Shparlinski, Number of different prime divisors of recurrence sequences, *Mat. Zametki* **42**, 494-507 (1987)
[22] P.J. Stephens, Prime divisors of second order linear recurrences, *Journal of Number Theory* **8**, 313–332 (1976)
[23] C.L. Stewart, On divisors of terms of linear recurrence sequences, *J. Reine Angew. Math.* **333**, 12–31 (1982)
[24] C.L. Stewart, Primitive divisors of Lucas and Lehmer numbers, *Transcendence Theory: advances and applications*, Academic Press, London, 79–92 (1977)
[25] C.L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. London Math. Soc.* **35**, 425-447 (1977)
[26] C.L. Stewart, On prime factors of terms of linear recurrence sequences, Number Theory and Related Fields: In memory of Alf van der Poorten, J.M.Borwein et al.(eds.) Springer Proceedings in Mathematics and Statistics **43**, 341-359 (2013)
[27] M. Ward, Prime divisors of second-order recurring sequences, *Duke Math. J.* **21**, 607-614 (1954)

DEPARTMENT OF MATHEMATICS, QUEEN'S UNIVERSITY, KINGSTON, ONTARIO K7L 3N6, CANADA.
E-mail address: murty@mast.queensu.ca

DEPARTMENT OF MATHEMATICS, QUEEN'S UNIVERSITY, KINGSTON, ONTARIO K7L 3N6, CANADA.
E-mail address: francois.seguin@queensu.ca

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO N2L 3G1, CANADA.
E-mail address: cstewart@uwaterloo.ca

ACCEPTED MANUSCRIPT