Journal of Number Theory 194 (2019) 8–29

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

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

M. Ram Murty [a,*], François Séguin [a], Cameron L. Stewart [b]

[a] Department of Mathematics, Queen's University, Kingston, Ontario K7L 3N6, Canada
[b] Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

ARTICLE INFO

Article history:
Received 16 November 2017
Received in revised form 28 June 2018
Accepted 29 June 2018
Available online 17 July 2018
Communicated by S.J. Miller

MSC:
11N69
11B37
11D59

Keywords:
Artin's conjecture
Recurrence sequences
Thue equation

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

☆ 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.

* Corresponding author.
E-mail addresses: murty@mast.queensu.ca (M.R. Murty), francois.seguin@queensu.ca (F. Séguin), cstewart@uwaterloo.ca (C.L. Stewart).

https://doi.org/10.1016/j.jnt.2018.06.017

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

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

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 mod 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]. (See also [14] and [17].) 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.

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

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