The two-variable Artin conjecture and elliptic analogues

By

François Séguin

A thesis submitted to the Graduate Program in Mathematics & Statistics
in conformity with the requirements for the
Degree of Doctor in Philosophy

Queen's University
Kingston, Ontario, Canada
August, 2018

Abstract

In 1927, Emil Artin conjectured that for any integer a other than -1 or squares, the set of primes p for which a is a primitive root modulo p has positive density in the set of all primes. This was proven subject to the generalized Riemann hypothesis (GRH) by Hooley in 1967. In 2002, P. Moree and P. Stevenhagen formulated an analogous two-variable conjecture, and used a result of Stephens on binary recurrence sequences to prove the conjecture conditionally on GRH. In this thesis, we show unconditional lower bounds for this two-variable conjecture. In particular, we obtain a result about general binary recurrence sequences that can be applied to this problem. We also formulate an analogue of the two-variable conjecture in the context of elliptic curves, and prove an unconditional lower bound for elliptic curves of rank 1. Finally, we obtain some results about the largest prime factor of the nth cyclotomic polynomial evaluated at a fixed integer, and where we let n vary.

Co-authorship

Chapters 2 and 3 are joint work with my supervisor Prof. M. Ram Murty (Queen's University) and with Prof. Cameron L. Stewart (University of Waterloo). The results presented are part of the article [39] (submitted). Chapter 5 is also joint work with my supervisor Prof. M. Ram Murty.

Acknowledgments

I would like to thank my advisor Prof. M. Ram Murty, from whom I learned a lot, both mathematically and philosophically. A particularly valuable lesson I learned is that one cannot be the judge of one's own work. Our role, as mathematicians, is to report and record any and all observations that we make, whether we deem them insignificant or not. Seeing a problem in a slightly different way can sometimes be the key to many locked doors, and a simple comment might be sufficient to do so. Also, we must never let a goal blind us of the wonders we can discover along the way. Setting out to solve a problem merely allows us to embark on a journey of exploration. We will rarely end up exactly where we thought we would. Instead of mindlessly following a constant direction, we must be ready to acknowledge the changing scenery, notice the unexpected phenomena we come across, and reorient ourselves to make the most of our trip.

I would like to thank my spouse Marie-Gabrielle. Her unwavering support made it possible to keep going during the difficult days, and made the joyous periods so much more enjoyable. She gave me the courage I needed to jump in the unknown and pursue my dreams. I will be forever grateful for all the sacrifices she made for me.

I would also like to thank my parents. Their unconditional faith in me helped me believe I was able to accomplish this, and their pride made this accomplishment all the sweeter. They instilled in

me an intellectual curiosity and taught me the value of knowledge. I am incredibly grateful for everything they did for me, and I would not be the same person without them.

Thanks to my peers and friends Siddhi, Neha and Arpita for all their encouragement, help, advice, and suggestions. Their candor and generosity were indispensable in helping me improve many facets of my work.

Thanks to Prof. Francesco Cellarosi and Prof. Alan Ableson for their very helpful advice about teaching and about the academic life in general.

Thanks to Anne Burns and Jennifer Read for their invaluable help with the sometimes kafkaesque administrative intricacies of the academic world.

Finally, I would like to thank Professors Michael Bennett, Oleg Bogoyavlenskij, Mike Roth and Karen Rudie for being on my doctoral committee.

Contents

Chapter 1

Introduction

1.1 Artin's primitive root conjecture

This thesis is concerned with a famous open problem in number theory called the Artin primitive root conjecture. We do not consider this particular conjecture per se, but rather related conjectures suggested by Artin's conjecture. Specifically, we consider a two-variable Artin conjecture, formulated in the works of P.J. Stephens [51] and P. Moree and P. Stevenhagen [30]. We also consider analogues of these conjectures in the theory of elliptic curves. To motivate the reader, we begin with some elementary introduction to the problems.

Given a prime p, we can consider the set of integers modulo p. A set of representatives is $\{0, 1, \ldots, p-1\}$. This set can be viewed as a group by imposing the usual addition law on it. However, if we consider the

non-zero elements, i.e. $\{1, \ldots, p-1\}$, we can also see this as a group by now considering the usual multiplication law. Indeed, it is easy to show that multiplication is well-defined, and that this satisfies all the axioms of a group. We will call this group $(\mathbb{Z}/p\mathbb{Z})^\times$. The subgroup of this group generated by one element a, denoted $\langle a \rangle$, consists simply of the different powers of this element, i.e. $\{a, a^2, a^3, \ldots\}$. Note that by Fermat's little theorem, $a^{p-1} \equiv 1 \bmod p$ and so this subgroup obviously consists of at most $p-1$ elements. It is possible, however, that it consists of fewer elements. The number of elements in this subgroup is called the *order of a modulo p*, and will be denoted in this thesis as $f_a(p)$. It is also (clearly) the smallest positive integer $r > 0$ such that $a^r \equiv 1 \bmod p$. Note that by Lagrange's Theorem, we know that the order of any element will be a divisor of $p-1$.

For example, considering $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$, we have

$$2^1 \equiv 2 \bmod 5$$

$$2^2 \equiv 4 \bmod 5$$

$$2^3 \equiv 4 \cdot 2 \equiv 3 \bmod 5$$

$$2^4 \equiv 3 \cdot 2 \equiv 1 \bmod 5$$

and so the subgroup generated by 2 is $\langle 2 \rangle = \{2, 4, 3, 1\}$ which is the whole group. When this happens, we call this element a *primitive root modulo p*. This is equivalent to saying that the order of the element is equal to $p-1$. Basic number theoretic arguments tell us that there are always exactly

$\phi(p-1)$ such elements in the group $(\mathbb{Z}/p\mathbb{Z})^\times$ for any p, where $\phi(p-1)$ denotes the number of positive integers smaller than and coprime to $p-1$. In particular, a primitive root modulo p is not unique. In our example above, the subgroup generated by 3 is $\langle 3\rangle = \{3,4,2,1\}$, meaning that just like 2, 3 is also a primitive root modulo 5.

Now considering the different group $(\mathbb{Z}/7\mathbb{Z})^\times = \{1,2,3,4,5,6\}$, we can again look at the subgroup generated by 3. We get $\langle 3\rangle = \{3,2,6,4,5,1\}$, meaning that 3 is also a primitive root modulo 7. However, this need not be the case all the time. For example, the subgroup generated by 2 here, $\langle 2\rangle = \{2,4,1\}$, is not the whole group.

Specifically, one can ask for which primes p is 2 a primitive root modulo p, and similarly for 3. Is there a finite number of such primes? If not, how "dense" is the set of those primes amongst the set of all primes?

The first person we know who tried to answer (partially) these questions is Gauss in 1801. Gauss focused specifically on the case $a = 10$, asking what is the order of 10 in the group $(\mathbb{Z}/p\mathbb{Z})^\times$ for different primes p. Why focus on 10? It turns out that when trying to write the fraction $1/p$ in its decimal expansion, the period with which the digits repeat is specifically the order of 10 in $(\mathbb{Z}/p\mathbb{Z})^\times$. This can easily be seen by trying to do long division on 1 divided by p. Indeed, let us take $p = 7$ as an example:

$$
\begin{array}{r}
0.\overline{142857} \\
7\overline{)1.000000} \\
\underline{7} \\
30 \\
\underline{28} \\
20 \\
\underline{14} \\
60 \\
\underline{56} \\
40 \\
\underline{35} \\
50 \\
\underline{49} \\
1
\end{array}
$$

We can see that the remainder after the first step is specifically $10 - 7k$ where k is the first digit in the solution (after the decimal point). This is equivalent to saying that the first remainder is (the representative between 0 and 6 of) $10^1 \bmod 7$. Similarly, the remainder after two steps is simply $10^2 \bmod 7$ and after n steps, $10^n \bmod 7$. Since the process repeats specifically when the remainder is 1 (the number we started with), we know that the period is the step for which the remainder is 1. This is equivalent to asking which is the smallest $n > 0$ for which $10^n \equiv 1 \bmod 7$, which is specifically the order of 10 in the group $(\mathbb{Z}/p\mathbb{Z})^\times$. Here, $10 \equiv 3 \bmod 7$, and as we showed earlier, 3 is a primitive root modulo 7, meaning that the order of 10 is $p - 1 = 6$, which is in effect the largest possible period.

Gauss then asked, how many primes p are there for which the decimal expansion of $1/p$ repeats with period $p - 1$? This is exactly the question we formulated above.

We needed to wait until 1927 before these questions were asked in full generality. At that time, Emil Artin proposed the following conjectural answer to those questions (See [29] for a historical account).

Conjecture 1.1 (Artin's Primitive Root Conjecture)**.** *Let a be any non-zero integer other than -1 or a perfect square. Then, there exist infinitely many primes p for which a is a primitive root modulo p. More specifically, the set of those primes is of positive density in the set of all primes. This means that if we denote by $N_a(x)$ the number of primes less than or equal to x for which a is a primitive root modulo p, i.e.*

$$N_a(x) = \#\left\{p \leq x \text{ prime} : \langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^\times\right\}$$

then, as $x \to \infty$,

$$N_a(x) \sim A(a)\frac{x}{\log x},$$

with $A(a) > 0$.

Here is Artin's heuristic argument on which he based the conjecture. Notice that a is a primitive root modulo p if and only if

$$a^{(p-1)/q} \not\equiv 1 \bmod p$$

for all prime divisors q of $p-1$. Indeed, otherwise, the order of a would divide $(p-1)/q$. According to a principle of Dedekind, $a^{(p-1)/q} \equiv 1 \bmod p$ if and only if p splits completely in $K_q = \mathbb{Q}(\zeta_q, \sqrt[q]{a})$, the splitting field of $X^q - a$. By the Chebotarev Density Theorem, the set of those primes has density $1/[K_q : \mathbb{Q}]$. Heuristically, the probability of a prime p not splitting completely in K_q is therefore

$$1 - \frac{1}{[K_q : \mathbb{Q}]}$$

and so the probability of a being a primitive root modulo p is expected to be

$$\prod_{q \text{ prime}} \left(1 - \frac{1}{[K_q : \mathbb{Q}]}\right).$$

This is the density that was originally conjectured in 1927 by Artin as $A(a)$. The first person to raise an issue with this expression for the density was Lehmer [27] in 1960 who noticed that it did not quite match several machine computations he carried out. It is possible that Artin himself was also aware of an issue with it as early as 1958 as he does discuss the possibility in correspondences with Lehmer. In 1964, Hasse [21] provided a correction for the density, that turned out to be incorrect in certain particular cases. It took Heilbronn in 1968 to provide and publish (see [60]) a corrected conjecture when he realized that the events "p splits completely in K_q" are not necessarily independent for different choices of p and q.

In 1967, Hooley [24] published a proof of Artin's primitive root conjecture conditional on the generalized Riemann hypothesis (abbreviated GRH). Specifically, the proof uses analogues of the classical Riemann hypothesis for the Dedekind zeta functions associated with the number fields K_q defined above. It is worth noting that Hooley's constant agreed with the conjectured constant of Heilbronn. We will be discussing Hooley's argument in greater detail in Chapter 6.

There are now many partial results other than Hooley's conditional proof. Most notably, Gupta and Murty [14] showed, using a theorem of

Fouvry and Iwaniec [11], that for any three distinct primes p, r and s, at least one element of the set

$$\{qs^2, q^2r, r^2s, qrs, qr^3, rs^3, q^3s, q^3r^2, r^3s^2, q^2s^3, q^3rs^2, q^2r^3s, qr^2s^3\}$$

is a primitive root infinitely often. Following improvements of Fouvry [12] and Bombieri, Friedlander and Iwaniec [2], Heath-Brown remarked [22] that Gupta and Murty's proof could show that one of any three integers q, r, s is a primitive root infinitely often, provided that they are multiplicatively independent and none of $q, r, s, -3qr, -3qs, -3rs, qrs$ is a square. For example, we now know that one of 2, 3 and 5 is a primitive root infinitely often, although we do not know which one. For a more detailed exposition of these results, we refer the reader to [36].

1.2 Variations on the conjecture

Since Hooley's proof, several variations of Artin's conjecture have been studied. We record here a few of them. This list is not meant to be exhaustive; for a more complete account we refer the reader to [29].

Artin's conjecture for number fields

Artin's conjecture can also be thought of in the more general context of algebraic number fields. For a principal ideal domain K and R its ring of integer, if ϵ is a unit, we can ask how many prime ideals $\mathfrak{p}$ there are for

which ϵ generates the group of units of the finite field $R/\mathfrak{p}$. It turns out this question is closely related to the Euclidean algorithm, and as such, results about this problem yield information concerning the Euclidean nature of the ring of integers of some number fields. For example, using Hooley's method, Weinberger proved [59] under GRH that if K is any number field with a ring of integers R, and if R is a principal ideal domain that contains infinitely many units, then R is a Euclidean domain.

There were multiple refinements and applications of this result that removed the assumption of GRH, due to Gupta, Ram Murty and Kumar Murty [17], Harper and Ram Murty [20], Harper [19], Clark and Ram Murty [6] and Ram Murty and Petersen [33] amongst others.

Elliptic Artin conjecture

Fundamentally, Artin's conjecture can be formulated in any context where a structure can be localized at several primes, each localization yielding an abelian group. Then, given an element in the original structure, we can ask for the number of primes p for which this element generates the whole group when localized at p.

As such, we can transport this problem in the world of elliptic curves. Indeed, given an elliptic curve E defined over $\mathbb{Q}$, the reduction of E modulo p is another elliptic curve $\overline{E}$ over the field $\mathbb{F}_p$ for all but finitely many primes p (those dividing the discriminant Δ of E). Disregarding those exceptional primes, given an element A of infinite order on the original elliptic curve

over $\mathbb{Q}$, we can look at the reduction of this point modulo p, $\overline{A}$, and ask for how many primes p does this point generate the whole group $\overline{E}(\mathbb{F}_p)$. This is precisely the question that was asked by Lang and Trotter in 1977 (see [25]).

In fact, following numerical computation, Lang and Trotter conjectured that under suitable conditions for the elliptic curve, this happens with a positive density of primes. This is now known as the Lang-Trotter conjecture. The first obvious potential obstruction to this conjecture is whether it is even the case that $\overline{E}(\mathbb{F}_p)$ is cyclic infinitely often. This issue was first raised by Serre in 1978, and he proceeded to prove the following result [45].

Theorem 1.2 (Serre, 1978)**.** *Assuming GRH, if E is an elliptic curve over $\mathbb{Q}$ with a 2-torsion point (in $\overline{\mathbb{Q}}$) not in $\mathbb{Q}$, then the set of primes p (of good reduction) for which $\overline{E}(\mathbb{F}_p)$ is cyclic has positive density in the set of all primes.*

Serre also gives some description on how to get an explicit density. The proof follows the arguments by Hooley for the conditional proof of the original conjecture.

In 1980, Ram Murty showed [34] that we can remove GRH in the above theorem for the case of complex multiplication elliptic curves. In 1987, he further showed [35] the infinitude of primes making $\overline{E}(\mathbb{F}_p)$ cyclic for a certain family of elliptic curves without complex multiplication. Finally, in 1990, Gupta and Ram Murty showed [16] the following unconditional

theorem.

Theorem 1.3 (Gupta- Murty, 1990)**.** *If E is any elliptic curve over $\mathbb{Q}$ with a 2-torsion point (in $\overline{\mathbb{Q}}$) not in $\mathbb{Q}$, then the set*

$$\#\{p \leq x : E \text{ has good reduction at } p, \overline{E}(\mathbb{F}_p) \text{ is cyclic } \} \gg \frac{x}{\log^2 x}.$$

With these results in hand, the Lang-Trotter conjecture is already more plausible, and Gupta and Murty show ([15]) that it holds under GRH for elliptic curves with complex multiplication.

1.3 The two-variable Artin conjecture

When considering an elliptic curve for which the above cyclicity results do not hold, it is possible to adapt the conjecture to make sense nevertheless. In particular, we can consider several points on the elliptic curve and look at the set of primes p for which the subgroup generated by all those points is the whole group $E(\mathbb{F}_p)$. In this case, we talk about a "higher rank" Artin conjecture.

In particular, we can ask a similar question in the regular setting on integers. Given two integers a and b, we can look at the set

$$\{p \text{ prime } : \langle a, b\rangle = (\mathbb{Z}/p\mathbb{Z})^{\times}\}.$$

However, this is not quite the problem that we are going to be interested in. Rather, we will ask the following: given two integers a and b, consider

first the subgroups generated by a in $(\mathbb{Z}/p\mathbb{Z})^\times$ for all primes p. For how many primes p would considering $\langle a, b\rangle$ instead not give anything different. More simply put, we can consider the set of primes p for which $b \bmod p$ is an element of $\langle a \bmod p\rangle$. We will call this set $S(a, b)$ (or simply S when a and b are clear from context) throughout the rest of this thesis. In short,

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

In [30], Moree and Stevenhagen conjectured that this set actually is of positive density in the set of all primes.

Conjecture 1.4 (Two-variable Artin conjecture)**.** *Let $a, b \in \mathbb{Z}^*$ and $a \neq \pm 1$, then the set*

$$S_x \coloneqq \{p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p\rangle \subseteq (\mathbb{Z}/p\mathbb{Z})^\times\}$$

has positive density in the set of all primes, that is

$$|S_x| \sim A(a, b)\frac{x}{\log x}$$

with $A(a, b) > 0$.

In addition to formulating the conjecture, Moree and Stevenhagen remarked that Stephens's result [51] about prime divisors of second-order linear recurrences, which used the method of Hooley [24], could be used to prove this conjecture conditionally upon GRH.

Theorem 1.5 (Stephens and Moree-Stevenhagen)**.** *Under the generalized Riemann hypothesis, the two-variable Artin conjecture is true. Moreover, if a, b are multiplicatively independent, the density $A(a, b)$ is given by*

$$A(a,b) = c_{a,b} \prod_{p \text{ prime}} \left(1 - \frac{p}{p^3 - 1}\right)$$

where $c_{a,b}$ is a correction constant that can be computed explicitly.

The first part of this thesis will be concerned about finding unconditional results concerning this conjecture. In particular, we will find an unconditional lower bound on $|S_x|$. Then we will formulate further variations on this conjecture as well as prove intermediate results.

1.4 Statement of the main results

In Chapter 2, we shall give several proofs, which we believe to be of independent interest, for the following theorem.

Theorem 2.3. *Let $a, b \in \mathbb{Z}^*$ with $|a| \neq 1$. Then,*

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

We also prove the following disjunction theorem.

Theorem 2.9. *Let $a, b \in \mathbb{Z}^*$ with $(a, b) = 1$. Then,*

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

In Chapter 3 we study the number of prime divisors of non-degenerate binary recurrence sequences. If u_n is a sequence defined recursively by $u_n = ru_{n-1} + su_{n-2}$ for some integers r and s (and defining u_0 and u_1 to be some integers), we say that u_n is a binary recurrence sequence. Given some conditions on r and s making this sequence interesting (non-degenerate), we can show that the nth term of the sequence is given by

$$u_n = a\alpha^n + b\beta^n$$

for some a, b, α, β that can be expressed in terms of r, s, u_0 and u_1.

Recall that $\omega(n)$ is defined as the number of distinct prime factors of n. We prove the following theorem about the number of distinct prime factors of terms of a binary recurrence sequence.

Theorem 3.2. *Let $\{u_n\}_{n=1}^{\infty}$ be a non-degenerate binary recurrence sequence with the n-th term given by $a\alpha^n + b\beta^n$. Let ϵ be a positive real number. There exists an effectively computable positive number C, depending on ϵ, a, b, α and β, such that for N bigger than C,*

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

We then use this result to deduce the following theorem, which is a strict improvement on Theorem 2.3.

Theorem 3.1. *Let $a, b \in \mathbb{Z}^*$ with $|a| \neq 1$. Then,*

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

In Chapter 4, we prove the following elliptic analogue to this result.

Theorem 4.2. *Let $E/\mathbb{Q}$ be an elliptic curve of rank 1, and $A, B \in E(\mathbb{Q})$ points of infinite order. Then,*

$$\left|\left\{p \leq x \text{ prime } : \overline{B} \in \langle \overline{A} \rangle \subseteq E(\mathbb{F}_p)\right\}\right| \gg \sqrt{\log x}$$

where $\overline{A}$ and $\overline{B}$ are the reduction modulo p of A and B respectively.

Also, we show an analogue of a theorem of Pólya (Theorem 2.1) in the context of elliptic curves.

Theorem 4.13. *Let A and B be points of infinite order in $E(\mathbb{Q})$. Then, the set*

$$S_{A,B} = \left\{p \text{ prime } : p \nmid \Delta \text{ and } \overline{B} \in \langle \overline{A} \rangle \subseteq \overline{E}(\mathbb{F}_p)\right\}$$

is infinite.

In Chapter 5, we will be looking at prime divisors of sparse values of cyclotomic polynomials. Precisely, if we fix a to be any positive integer other than 1, we consider the prime divisors of $\Phi_n(a)$ as n varies, where

$$\Phi_n(x) \coloneqq \prod_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} \left(x - e^{2\pi i k/n}\right)$$

is called the nth cyclotomic polynomial.

For a fixed a, recall that $f_a(p)$ is defined as the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$. We then define α_p to be the largest integer for which p^{α_p} divides $a^{f_a(p)} - 1$. By the definition of $f_a(p)$, we know $\alpha_p \geq 1$.

We will then prove the following about the largest prime factor of $\Phi_n(a)$.

Theorem 5.1. *Let $P(m)$ denote the largest prime divisor of m. Let $a > 1$ be an integer. Suppose that there exists a constant κ for which $\alpha_p \leq \kappa$ for all primes p. Then, there exists a positive constant C (depending on a and κ) such that*

$$P\left(\Phi_N(a)\right) > C\phi(N)^2$$

for all N.

There are strong heuristic reasons for the hypothesis in the above theorem. We discuss these in Chapter 5.

Also, it is already known that amongst all the prime divisors of n, only one potentially also divides $\Phi_n(a)$ ([54], see Lemma 5.7 here). We call this prime P_n here. It is also known that P_n divides $\Phi_n(a)$ to at most the first power. We define δ_n to be 1 if P_n divides $\Phi_n(a)$ and 0 otherwise. We will prove the following about those δ_n.

Theorem 5.3. *For some $\theta < 1$,*

$$\sum_{n \leq x} \delta_n \log P_n = O(x^\theta).$$

In particular, the above theorem shows that

$$\sum_{n \leq x} \delta_n = O(x^\theta)$$

so that δ_n is zero most of the time.

We call a prime p a Wieferich prime for a (respectively super-Wieferich prime for a) if p^2 (respectively p^3) divides $a^{p-1} - 1$. Very little is known

about the number of these Wieferich primes. We connect the above analysis to Wieferich primes and show the following theorem.

Theorem 5.18. *Suppose that there are only finitely many super-Wieferich primes. Then, there are infinitely many non-Wieferich primes.*

Then, using methods similar to those used for Theorem 5.3, we prove the following.

Theorem 5.25.

$$\sum_{n\le x}\sum_{d\mid a^n-1}\frac{1}{d} = Rx + o(x)$$

where R is the "Romanoff" constant

$$R = \sum_{\substack{d\ge 1\\(d,a)=1}}\frac{1}{d\, f_a(d)},$$

which gives an improvement on average to a result of Erdős [9].

Finally, in Chapter 6, we will discuss problems for future research.

Chapter 2

First approaches to a lower bound estimate

2.1 Infinitude of primes in the two-variable Artin conjecture

It is worth noting that the two-variable Artin conjecture is in some ways an easier problem than Artin's original conjecture. For example, in the two-variable case, we can deduce relatively easily that the set of primes for which the conjecture is satisfied is infinite. This is an argument due to Pólya [41].

Theorem 2.1. *Let $a, b \in \mathbb{Z}^*$ with $(a, b) = 1$. Then, the set*

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

is infinite.

Recall that $\text{ord}_p(x)$ is defined for a non-zero integer x as the largest integer k for which p^k divides x. This definition can be extended to $\mathbb{Q}$ by defining that

$$\text{ord}_p\left(\frac{x}{y}\right) = \text{ord}_p(x) - \text{ord}_p(y).$$

To prove this theorem, we will be using the following simple fact about $\text{ord}_p(x)$.

Fact 2.2. *For any two integers n and m and any prime p,*

$$\text{ord}_p(n+m) \geq \min(\text{ord}_p(n), \text{ord}_p(m)).$$

Additionally, equality holds when $\text{ord}_p(n) \neq \text{ord}_p(m)$. Equivalently, if the inequality above is strict, then $\text{ord}_p(n) = \text{ord}_p(m)$.

We now prove Theorem 2.1.

Proof. First, define the sequence $x_n = a^n - b$. Then, notice that the set $S_{a,b}$ can be described as $S_{a,b} = \{p \text{ prime } : p|x_n \text{ for some } n\}$. Also, note that $|x_n|$ goes to infinity as n goes to infinity. Thus, x_n cannot contain a bounded subsequence.

For simplicity of notation, call $S_{a,b} = S$. We will show that S is infinite by the method of contradiction. Suppose that $|S| < \infty$, and let $M = |x_0| \cdot \prod_{p \in S} p$, and $\ell = \varphi(M)$. We will show that the subsequence $x_{n_k} = x_{\ell k}$ is bounded. As the terms $x_{\ell k}$ are only divisible by primes $p \in S$, and since S is finite, it suffices to show that $\text{ord}_p(x_{\ell k})$ is bounded for every $p \in S$.

Fix $p \in S$. First suppose that p does not divide a. Then, we have

$$x_{\ell k} - x_0 = a^{\ell k} - 1$$

From the definition of M, we can write $M = M' \cdot p^{\mathrm{ord}_p(x_0)+1}$ with $p \nmid M'$. Then, we write $\ell = \varphi(M') \cdot \varphi(p^{\mathrm{ord}_p(x_0)+1})$ and by Euler's Theorem

$$x_{\ell k} - x_0 = a^{\ell k} - 1 \equiv 0 \pmod{p^{\mathrm{ord}_p(x_0)+1}}.$$

Hence $\mathrm{ord}_p(x_{\ell k} - x_0) \geq \mathrm{ord}_p(x_0) + 1$.

Since $\mathrm{ord}_p(x_{\ell k} - x_0) \geq \mathrm{ord}_p(x_0) + 1 > \min(\mathrm{ord}_p(x_{\ell k}), \mathrm{ord}_p(x_0))$, we conclude from Fact 2.2 that $\mathrm{ord}_p(x_{\ell k}) = \mathrm{ord}_p(x_0)$.

Now suppose that p divides a. Then, for k large enough, $\mathrm{ord}_p(a^{\ell k}) > \mathrm{ord}_p(b)$ and so $\mathrm{ord}_p(x_{\ell k}) = \mathrm{ord}_p(b)$.

We therefore have that the subsequence $x_{\ell k}$ is bounded, which is a contradiction. S must therefore be infinite. □

A careful analysis of this argument does not lead to any reasonable lower bound for the number of such primes. Hence, we adopt different ways to get effective lower bounds. The first lower bound that we will prove is the following.

Theorem 2.3. *Let $a, b \in \mathbb{Z}^*$ with $|a| \neq 1$. Then,*

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

2.2 Theorem 2.3 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 of terms of binary recurrence sequence.

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

Theorem 2.4 (Stewart [56])**.** *Let α, β, u and v be integers such that $\alpha\beta uv \neq 0$, $\alpha \neq \beta$ and $\alpha, \beta \neq \pm 1$. There exists an effectively computable positive number C such that, for $n > C$,*

$$P(u\alpha^n - v\beta^n) > \sqrt{n} \exp\left(\frac{\log n}{104 \log\log n}\right).$$

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

$$P(a^n - b) \gg_{a,b} \sqrt{n} \exp\left(\frac{\log n}{104 \log\log n}\right)$$

for every $n > 0$. This is what we will be using.

Proof of Theorem 2.3. We will prove the theorem for the case $a, b > 0$ for simplicity. The proof can be easily adapted to the general case. See Remark 2.5 below for more details. Let

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

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

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

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

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,

$$a^n \equiv b \bmod q$$

$$a^m \equiv b \bmod q$$

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

and thus q divides $b^n - b^m$.

From Theorem 2.4, 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 $y = \frac{\log\left(C_1\sqrt{N}\right)}{\log b}$ yields

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

which is a contradiction to Theorem 2.4 for properly chosen C_1.

We therefore have y distinct primes in the set $S(x)$, where

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

□

Remark 2.5. The above result still holds for $a, b \in \mathbb{Z}^*$, $a \neq \pm 1$, and the same proof works with a few modifications. The hypothesis that a and b are positive merely simplifies the exposition. Indeed, for arbitrary $a, b \in \mathbb{Z}^*$, define $N \coloneqq \left\lfloor \frac{\log(x-|b|)}{\log|a|} \right\rfloor$. Then, if p divides $a^n - b$ with $n \leq N$, we have

$$p \leq |a^n - b| \leq |a|^n + |b| \leq x - |b| + |b| = x.$$

Also, define $y \coloneqq \frac{\log N}{2\log|b|}$, so that if q divides $b^{n-m} - 1$, we have

$$q \leq |b|^{n-m} + 1 \leq |b|^y + 1 \leq \sqrt{N} + 1$$

again yielding a contradiction.

2.3 Theorem 2.3 via Thue equations

The second proof of Theorem 2.3 uses a result on Thue equations. Recall that a Thue equation is an equation of the form

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

where $F(x, y) = a_0 x^r + a_1 x^{r-1} y + \cdots + a_r y^r$ is an integral binary form of degree at least 3. A solution (x, y) to such an equation is called *primitive* if $\gcd(x, y) = 1$. We have the following result for the number of primitive solutions to such an equation.

Theorem 2.6 (Bombieri, Schmidt [4])**.** *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

$$c_1 r^{t+1},$$

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 2.3. 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. The idea used in this proof is attributed to S. Pillai, and will be used in several other proofs throughout this thesis.

Proof of Theorem 2.3. Suppose that $\gcd(a, b) = 1$. 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,

$$\#S(x) \gg \#\{p \text{ prime } : p|(a^n - b) \text{ for some } n \leq N\} \tag{2.3.1}$$

where $N := \left\lfloor \frac{\log x}{\log a} \right\rfloor$. Denote by k the quantity on the right hand side of (2.3.1).

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

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

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

where δ and ϵ_i are the residue of n and $\alpha_i(n)$ modulo 3 respectively (that is $\delta, \epsilon_i \in \{0, 1, 2\}$). 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 Theorem 2.1 gives us that $|S(x)|$ 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 2.6. Then, $\frac{N}{3^{k+1}} > C$ would be a contradiction to Theorem 2.6, and so we have that

$$\begin{aligned} \frac{N}{3^{k+1}} &\leq C \\ \Rightarrow N &\ll 3^k \\ \Rightarrow \log N &\ll k. \end{aligned}$$

Recall from the definition of N that $N \gg \log x$, and so

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

which completes the proof. It is worth noting that the dependency of the implied constant 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. □

2.4 Theorem 2.3 via Mumford's gap principle

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

Basically, we can think of a height function on a curve C over $\mathbb{Q}$ as some kind of "measure" of the "complexity" of any point $P \in C(\mathbb{Q})$. For example,

let us fix an equation for $C/\mathbb{Q}$ and express P with coordinates $\left(\frac{x}{\xi}, \frac{y}{\eta}\right)$ where x, ξ, y and η are integers such that the fractions are expressed in lowest form. Then, the function $H(P) = \max(|x|, |\xi|)$ is such a (multiplicative) height function. This so-called "naïve" height function will be the one we use in the proof of our next theorem. As such, we will postpone further discussion of height functions until Chapter 4.

Theorem 2.7 (Mumford [23], [31])**.** *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 2.7 depend only on the field $\overline{K}$. Therefore, we can apply the result to quadratic twists of the same curve with the same constant for each of them. See [26, Lemma 5] for a proof of this fact.

Proof of Theorem 2.3. The general idea of this proof is similar to that of section 2.3. As before,

$$\#S(x) \gg \#\{p \text{ prime } : p|(a^n - b) \text{ for some } n \leq N\} \tag{2.4.1}$$

where $N \coloneqq \left\lfloor \frac{\log x}{\log a} \right\rfloor$. Denote by k the quantity on the right hand side of (2.4.1).

Again, 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 $\alpha_i(n) = \mathrm{ord}_{p_i}(a^n - b)$. 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

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

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

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

Any rational point (x, y) on this new curve would give

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

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 $H(P) = \max\{|x|, |\xi|\}$, where $P = \left(\frac{x}{\xi}, \frac{y}{\eta}\right)$ with x, ξ, y and η integers, and $(x, \xi) = (y, \eta) = 1$.

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

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

and so, for some constant c',

$$2^k \geq \frac{c' N}{\log N + \log\log a}.$$

Therefore,

$$k \gg \log N \gg \log\log x.$$

□

2.5 Remarks on the implied constants

We point out that even if all three proofs give bounds of the same order of magnitude with respect to x, the dependency of the implied constants on a and b vary with each approach. For example, the proof in section 2.3 reduces the dependence on b dramatically. Note also that the dependency on b of the implicit constant in section 2.4 is harder to make explicit as the constant given from Mumford's theorem depends on b. However, we see that the proof of section 2.3 requires an extra condition on a and b to use Theorem 2.6, albeit a mild one.

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

2.6 Generalization to rational numbers

In [30], 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 2.4.

For the proof of Section 2.4, it is also easy to generalize the argument. Indeed, following the same notation, we can write for $n \equiv 0 \bmod 10$

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

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 $\max\{\left|a_1^N\right|, \left|a_2^N\right|\} \sim x$, the rest of the proof goes through unchanged.

The proof in Section 2.3 is trickier to generalize. Indeed, the result from Bombieri and Schmidt that 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 [10].

Theorem 2.8. *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

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

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

2.7 A disjunction theorem

We now prove the following disjunction theorem.

Theorem 2.9. *Let* $a, b \in \mathbb{Z}^*$ *with* $(a, b) = 1$. *Then,*

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

The proof for this theorem mainly relies on the following theorem of Gupta and Murty [14].

Theorem 2.10 (Gupta, Murty)**.** *Fix* a, b *coprime integers. There exists a constant* $c > 0$ *such that*

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

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 $x^{1/4+\epsilon} < q_1 < q_2$.

Proof of Theorem 2.9. We start by considering only the primes in the set

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

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

$$S'(x) = \left\{ p \leq x \text{ prime } : \begin{array}{c} b \bmod p \in \langle a \bmod p \rangle \subset \mathbb{F}_p^* \\ \text{or } \langle b \bmod p \rangle = \mathbb{F}_p^* \end{array} \right\}.$$

Let $p \in T(x)$, and as usual let $f_a(p)$ and $f_b(p)$ denote the order of a and b respectively in $\mathbb{F}_p^\times$. Since a and b are not squares modulo p, it follows that 2 divides $f_a(p)$ and $f_b(p)$. Indeed, if g is a generator for $\mathbb{F}_p^\times$, then $a \equiv g^k \bmod p$ for some odd integer k, and so $a^{f_a(p)} \equiv g^{k f_a(p)} \equiv 1 \bmod p$. Therefore, $f_g(p) = p - 1$ divides $k f_a(p)$ and so $f_a(p)$ must be even.

From the definition of $T(x)$, either $p - 1 = 2q_1$ or $p - 1 = 2q_1 q_2$ with q_1, q_2 primes.

Case 1 Suppose $p - 1 = 2q_1$. If we exclude the finitely many primes p for which $f_a(p) = 2$ (the prime divisors of $(a-1)(a+1)$), then $f_a(p) = 2q_1$ and so a is a primitive root for $\mathbb{F}_p^\times$. p is therefore trivially in $S'(x)$.

Case 2 Suppose $p-1 = 2q_1 q_2$, with $q_1 < q_2$. There are three possibilities.

Case 2.1 $f_a(p) = 2q_1 q_2$. Then, a is a primitive root modulo p.

Case 2.2 $f_a(p) = 2q_2$.

Case 2.3 $f_a(p) = 2q_1$. 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 [42] 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 [3], 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

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

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

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

Therefore,

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

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

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

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

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

Now, if either a or b is a primitive root modulo p, then $p \in S'(x)$. Also, if $f_a(p) = f_b(p) = 2q_2$, 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. □

It is worth noting that this last result is very close to obtaining positive density for this particular set of primes. We believe that refining the argument could be able to produce a proof of positive density for this disjunction question. Doing so would essentially prove that at least one of two results, currently only known under GRH, is true unconditionally. It would also give an unconditional proof that either $S(a, b)$ has positive density, or $S(b, a)$ has positive density. It would be interesting to study carefully the different cases individually to see if a proof of the two-variable Artin conjecture can be obtained this way.

Chapter 3

Counting prime divisors of binary recurrence sequences and applications

3.1 Statement of results

We prove an unconditional lower bound on the number of primes in the set $S_{a,b}$ defined in Chapter 2. Specifically, we prove the following result.

Theorem 3.1. *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 3.5 a more general result about binary recurrence sequences.

Theorem 3.2. *Let $\{u_n\}_{n=1}^{\infty}$ be a non-degenerate binary recurrence sequence with the n-th term given by $a\alpha^n+b\beta^n$. Let ϵ be a positive real number. There exists an effectively computable positive number C, depending on ϵ, a, b, α and β, such that for N bigger than C,*

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

3.2 Preliminaries

One way to study the two-variable Artin conjecture is through what we call recurrence sequences. These are sequences where the terms are defined recursively on the previous terms. Here, we will restrict our attention to *binary recurrence sequences* (or *degree two recurrence sequences*). Let r and s be integers with $r^2 + 4s \neq 0$. Let u_0 and u_1 be integers and define recursively the nth term of the sequence to be

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

It turns out that the nth term of any such sequence can be expressed as

$$u_n = a\alpha^n + b\beta^n \tag{3.2.1}$$

where α and β are the roots of the polynomial

$$x^2 - rx - s$$

and

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

Note that we require the condition $r^2 + 4s \neq 0$ to guarantee that α and β are distinct.

The sequence $\{u_n\}_{n=0}^{\infty}$ is called a *binary recurrence sequence*.

If a or α is zero, then the nth term in the sequence is given by $b\beta^n$, which is not as interesting to study. Of course the same thing happens if b or β is zero. Also, if α/β is a root of unity, we can simplify the expression of u_n as

$$u_n = \left(a\left(\frac{\alpha}{\beta}\right)^n - b\right)\beta^n$$

which is again much simpler. As such, we call those two cases *degenerate binary recurrence sequences*. Equivalently, a sequence is said to be *non-degenerate* if $ab\alpha\beta \neq 0$ and α/β is not a root of unity.

Proposition 3.3. *For a non-degenerate binary recurrence sequence given by (3.2.1), if $|\alpha| \geq |\beta|$, then*

$$|\alpha| \geq \sqrt{2}. \tag{3.2.2}$$

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 Pólya [41] showed that

$$\omega\left(\prod_{\substack{n=1\\u_n\neq 0}}^{N} u_n\right) \to \infty \; as \; N \to \infty; \tag{3.2.3}$$

Gelfond [13] and Mahler [28] in 1934 and Ward [58] in 1954 gave alternative proofs of (3.2.3). In 1987 Shparlinski [47] showed that

$$\omega\left(\prod_{\substack{n=1\\u_n\neq 0}}^{N} u_n\right) \gg N/\log N, \tag{3.2.4}$$

improving on an earlier result of his [46] where he had established (3.2.4) with the righthand side of (3.2.4) replaced by $N^{1/2}$. It should be noted that Shparlinski's result (3.2.4) applies not just to binary recurrence sequences but to non-degenerate sequences of order k with $k \geq 2$.

We are able to improve upon (3.2.4) for binary recurrence sequences through Theorem 3.2.

3.3 Remark and conjecture

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

$$\omega\left(\prod_{\substack{n=1\\u_n\neq 0}}^{N} u_n\right) \ll N^2/\log N. \tag{3.3.1}$$

To see this suppose that u_n is given by (3.2.1) with $|\alpha| \geq |\beta|$. Then,

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

and therefore,

$$\left|\prod_{\substack{n=1\\u_n\neq 0}}^{N} u_n\right| \leq (|a| + |b|)^N |\alpha|^{N(N+1)/2}. \tag{3.3.2}$$

Let $p_1, p_2, ...$ be the sequence of all prime numbers. By the Prime Number Theorem

$$\prod_{i=1}^{t} p_i = \exp((1 + o(1))t \log t). \tag{3.3.3}$$

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 (3.3.1) follows from (3.2.2), (3.3.2) and (3.3.3).

In [39], we conjecture the following stronger statement.

Conjecture 3.4. *There exist positive numbers C_1 and C_2, which depend on a, b, α and β, such that if $\{u_n\}_{n=1}^{\infty}$ is a non-degenerate binary recurrence sequence, then*

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

Note that the lower bound obtained from this conjecture could be used to improve Theorem 3.1 by replacing $\log x$ with $\log x \log\log x$ in the lower bound.

3.4 Results on recurrence and Lucas sequences

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 (3.2.1), we have

$$t_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{3.4.1}$$

for $n \geq 0$. The first two results we require concern prime divisors of Lucas numbers.

Proposition 3.5. *Let $\{t_n\}_{n=0}^{\infty}$ be a Lucas sequence, as in (3.4.1), 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 [55]. 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 cannot yield $r^2 - 4s = 1$.

□

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

Proposition 3.6. *Let $\{t_n\}_{n=0}^{\infty}$ be a Lucas sequence, as in (3.4.1), 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 [55] and it is based on the work of Carmichael [5], see also [54]. □

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 3.7. *Let u_n be the n-th term of a non-degenerate binary recurrence sequence as in (3.2.1). 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 [55] and is a consequence of Baker's theory of linear forms in logarithms. □

3.5 Proof of Theorem 3.2

Proof of Theorem 3.2. 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

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

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 (3.2.1) for $m > c_1$ we have

$$|u_m|_p \geq |a'b'|_p . \tag{3.5.1}$$

It follows from Proposition 3.7 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

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

Our proof proceeds by a comparison of estimates for S.

By Proposition 3.7, there exists c_4 such that

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

and so

$$|S| \geq |\alpha|^{\frac{(1-\gamma^2)N^2}{2} - c_5 N \log N}. \tag{3.5.2}$$

Plainly,

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

We first estimate $|S|_p^{-1}$ for primes p which divide $\alpha\beta$. By (3.5.1), we have

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

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 $m \geq r$,

$$u_m - \beta^r u_{m-r} = a'\alpha^{m-r} t_r. \tag{3.5.3}$$

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 (3.5.3) 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

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

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

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

Letting $\ell = \ell(p)$ be the smallest integer for which $p | t_\ell$, we have by Proposition 3.5 and Proposition 3.6 that if $p > 2$,

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

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

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

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 $n(p) + r \le N$, we find that for $p > 2$

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

while for $p = 2$,

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

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 $p > 2$,

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

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

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

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

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

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

$$S = \prod_{p|S} |S|_p^{-1} \leq \left(\prod_{p|S} 4^{\frac{N}{\ell(p)}} \right) |\alpha|^{(N-\gamma N)(T+1)} \, N! \, |a'b'|^N \prod_{p|S} \left|u_{n(p)}\right|_p^{-1}. \quad (3.5.4)$$

We need to estimate the right hand side and compare it with (3.5.2).

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

However, by Proposition 3.5,

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

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

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

Inserting this in inequality (3.5.4) and using $N! \leq N^N$, 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 $|u_n| \leq (|a| + |b|) |\alpha|^n$, since $|\alpha| \geq |\beta|$. Put

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

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

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

Putting everything together, we get

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

and as $|\alpha| \geq \sqrt{2}$, we get from (3.5.2)

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

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 $\gamma + 2\sqrt{2}$. □

3.6 Proof of Theorem 3.1

We immediately use Theorem 3.2 to prove Theorem 3.1.

Proof of Theorem 3.1. 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 (3.2.1) are respectively a, 1, 1 and b). Then, by Theorem 3.2,

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

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

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

□

Chapter 4

The elliptic two-variable Artin conjecture

4.1 Statement of the problem

In Section 1.2, we explained how Lang and Trotter formulated an analogue of Artin's conjecture in the context of elliptic curves. Fundamentally, Artin's conjecture for primitive roots only requires a "global-local" structure, where an element a in the global structure can be localized at primes. We then ask for how many of these primes does the reduction of a generate the full localized structure.

We do have this kind of "global-local" structure in the context of elliptic curves by taking the reduction mod p of an elliptic curve defined over $\mathbb{Q}$ as we will see in the next section. As such, Artin's original conjecture was

extended to the context of elliptic curves in what is now known as the elliptic Artin conjecture, or the Lang-Trotter conjecture.

We can also consider the analogue of the two-variable Artin conjecture in the context of elliptic curves. We would now look at two points A and B on the elliptic curve E defined over $\mathbb{Q}$, and wonder for which primes p is the point B inside the subgroup generated by A on the reduction mod p of E. As for the classical setting, we conjecture that the number of such primes is of positive density in the set of all primes.

Conjecture 4.1 (The elliptic two-variable Artin conjecture)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$, and $A, B \in E(\mathbb{Q})$ be two points of infinite order. Let $\overline{A}$ and $\overline{B}$ denote the reduction of A and B mod p respectively. The set*

$$S_{A,B} = \left\{ p \text{ prime } : p \nmid \Delta \text{ and } \overline{B} \in \langle \overline{A} \rangle \subseteq \overline{E}(\mathbb{F}_p) \right\}$$

has positive density in the set of all primes.

Unfortunately, we were unable at this point to come up with a heuristical argument for the conjecture, or even a conjectural density. The basis for Conjecture 4.1 resides in the fact that most techniques and arguments of the classical case have an analogue in the elliptic setting. However, the question of finding those heuristics is part of the problems we consider for future research, and some discussion about that can be found in Section 6.1.

In this chapter, we prove a partial result towards this conjecture, similar in nature to Theorem 3.1 for the classical case. We do so first in a specific case of elliptic curves, and then discuss a possible approach to generalize to all elliptic curves.

Theorem 4.2. *Let $E/\mathbb{Q}$ be an elliptic curve of rank 1, and $A, B \in E(\mathbb{Q})$ be points of infinite order. Then,*

$$\#\left\{p \leq x \text{ prime } : p \nmid \Delta \text{ and } \overline{B} \in \langle \overline{A} \rangle \subseteq E(\mathbb{F}_p)\right\} \gg \sqrt{\log x}$$

where $\overline{A}$ and $\overline{B}$ are the reduction modulo p of A and B respectively.

We then generalize the argument of Theorem 2.1 to the setting of elliptic curves to show the following.

Theorem 4.3. *Let A and B be points of infinite order in $E(\mathbb{Q})$. Then, the set $S_{A,B}$ is infinite.*

4.2 Preliminaries

The Mordell-Weil group

We review here some basic information about elliptic curves. This review is not meant to be exhaustive, and we refer the reader to [48] for a thorough introduction to elliptic curves.

Formally, an elliptic curve is defined as an algebraic variety of genus 1. Since we will be only dealing with elliptic curves over $\mathbb{Q}$, for our purposes,

it is sufficient to view an elliptic curve E as the set of solutions (x, y) to an equation of the form

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q}$$

(called a Weierstrass equation for E) along with an extra point $\mathcal{O}$, the so-called point at infinity.

To this Weierstrass equation, we associate the quantity

$$\Delta = -16(4a^3 + 27b^2)$$

called the *discriminant* of the Weierstrass equation. Using changes of variables, we can see that the same elliptic curve can be described by different Weierstrass equations. We call a Weierstrass equation a *minimal Weierstrass equation for* E if it has the smallest possible discriminant amongst all its Weierstrass equations. This is an easy way of fixing a canonical such equation for an elliptic curve (although it is not necessarily unique, the associated primes of good reduction will be).

The elliptic curve E is said to be defined over $\mathbb{Q}$ if we can write its equation above with a and b in $\mathbb{Q}$, and we can then consider the set of all *rational* points on this curve (along with the point at infinity) that we denote $E(\mathbb{Q})$.

Note that every rational point P on E (except for $\mathcal{O}$) can be written as

$$P = \left(\frac{x}{d^2}, \frac{y}{d^3}\right) \tag{4.2.1}$$

where x, y, d are integers and $\gcd(x, d) = \gcd(y, d) = 1$ (see [50, III.2]).

It turns out that we can define an addition on this set which makes $E(\mathbb{Q})$ an abelian group, called the Mordell-Weil group of E over $\mathbb{Q}$.

It is a remarkable theorem of Mordell and Weil that this group is actually finitely generated. As such, if we write $E(\mathbb{Q})_{\text{tors}}$ to be the subgroup of all elements of finite order, then we can express the Mordell-Weil group as

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

for some $r \geq 0$. The quantity r is called the *rank* of E over $\mathbb{Q}$. Very few elliptic curves are known to have rank bigger than 1 [43]. In particular, the elliptic curve with the largest exact known rank to date has a rank of 19. Furthermore, we know of only one example with rank at least 28 [7]. There is, however, a "folklore" conjecture that the rank of elliptic curves can get arbitrarily large. Recently, there are conjectures and heuristics [1] put forth that suggest otherwise. So the situation is very much in limbo concerning ranks at the moment.

Reduction mod p

Given any prime p, if p does not divide Δ_E, then the curve

$$\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b}$$

is also an elliptic curve over the field $\mathbb{F}_p$, where $\overline{a}$ and $\overline{b}$ are the reduction of a and b modulo p . We call these *primes of good reduction.* In particular, notice that there are only finitely many primes of bad reduction (i.e. primes which are not of good reduction).

Height functions

In this chapter, we will be using the theory of heights. We give a basic introduction here, but we refer the reader to [48] for a more in-depth presentation, as well as the proofs for the facts that we will be using. Note that all of the following discussion also holds in the more general context of an elliptic curve defined over a number field K. We will only consider $\mathbb{Q}$ here for simplicity.

Let $\mathbb{P}^N(\mathbb{Q})$ denote the N dimensional projective space over $\mathbb{Q}$. For a point $P \in \mathbb{P}^N(\mathbb{Q})$, we want to define the *height* of P as a "measure" of the "complexity" of P. Let us write

$$P = [x_0, \ldots, x_N]$$

with $x_i \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_N) = 1$. We can do so in a unique manner up to sign. Then, a natural choice for the height of P might be

$$H(P) = \max\left(|x_0|, \ldots, |x_N|\right).$$

We call this value the *multiplicative height of* P.

Now, if we consider the elliptic curve $E/\mathbb{Q}$, recall that we define the coordinate ring of $E/\mathbb{Q}$, denoted $\mathbb{Q}[E]$, to be the ring of polynomials modulo those constantly zero on $E/\mathbb{Q}$, as well as the function field of E, denoted $\mathbb{Q}(E)$, to be the field of fractions of the coordinate ring.

Then, we may associate with any f in $\mathbb{Q}(E)$ a surjective morphism

$f^* : E \to \mathbb{P}^1$ as

$$f^*(P) = \begin{cases} [1,0] & \text{if } P \text{ is a pole} \\ [f(P),1] & \text{otherwise} \end{cases}.$$

The *logarithmic height on E relative to f* is defined as the function

$$\begin{aligned} h_f : E(\mathbb{Q}) &\longrightarrow \mathbb{R} \\ h_f(P) &= \frac{1}{2}\log H\left(f^*(P)\right). \end{aligned}$$

As an example, let us take the function $f(x,y) = x$ in the function field $\mathbb{Q}(E)$. Then, for a point P with coordinates as in (4.2.1), we have

$$h_f(P) = \frac{1}{2}\log \max\left(|x|, \left|d^2\right|\right).$$

This is a very useful height function, and is called the *naïve height on E*. As a side note, some authors omit the factor of $1/2$ for the logarithmic height. This factor is there to simplify the statement of some results, and as such does not play a critical role in the definition.

We list here some interesting facts of height functions (see [48, VIII.6]).

Fact 4.4. *Let $f \in \mathbb{Q}(E)$ be an even function (that is $f(-P) = f(P)$), then*

(1) for any $P, Q \in E(\mathbb{Q})$

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O_{E,f}(1)$$

and

(2) for any integer m,

$$h_f(mP) = m^2 h_f(P) + O_{E,f}(1).$$

One would like to remove the dependency on the function f from this definition of height. This is specifically what Néron and Tate did with the canonical height. Here is a summarized description.

Theorem 4.5. *If $f \in \mathbb{Q}(E)$ is a non-constant even function, then*

$$\hat{h}(P) \coloneqq \frac{1}{\deg(f)} \lim_{N\to\infty} 4^{-N} h_f\left(2^N P\right)$$

exists and is independent of f.

The function $\hat{h}$ is called the *canonical height* (or sometimes *Néron-Tate height*) *on E*. The usefulness of this canonical height lies in its miraculous properties which we recall here (see [48, VIII.9.3]).

Fact 4.6. *For any points $P, Q \in E(\mathbb{Q})$,*

(1)

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

(2)

$$\hat{h}(mP) = m^2 \hat{h}(P)$$

(3) $\hat{h}$ is a quadratic form, i.e.

$$\langle P, Q\rangle \coloneqq \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

is a bilinear (height) pairing.

(4) Let $f \in \mathbb{Q}(E)$ be an even function, then

$$(\deg f)\hat{h} = h_f + O_{E,f}(1)$$

Note that from (4) above, if h denotes the naïve height on E, then we have

$$\hat{h} = h + O_E(1).$$

We will discuss any further results on height functions as we need them.

4.3 Proof of Theorem 4.2

We begin by fixing a minimal Weierstrass equation for $E/\mathbb{Q}$. We will adopt the following notation for writing the coordinates of $P \in E(\mathbb{Q})$ as in (4.2.1):

$$P = \left(\frac{x(P)}{d(P)^2}, \frac{y(P)}{d(P)^3}\right)$$

with $(x(P), d(P)) = (y(P), d(P)) = 1$.

Then, note that

$$\begin{aligned} &\overline{B} \in \langle \overline{A} \rangle \quad \text{in } E(\mathbb{F}_p) \\ \Leftrightarrow\ & n\overline{A} - \overline{B} = O \quad \text{in } E(\mathbb{F}_p) \text{ for some } n \geq 1 \\ \Leftrightarrow\ & p | d(nA - B). \end{aligned}$$

We first follow [49] to obtain a key lemma.

Let

$$h(P) = \frac{1}{2} \log \max\{|x(P)|, \left|d(P)^2\right|\}$$

be the naïve height function and let $\hat{h}$ denote the corresponding canonical height function. From properties of height functions (Facts 4.4 and 4.6),

$$h(nP) + O_E(1) = \hat{h}(nP) = n^2\hat{h}(P)$$

and so $h(nP)$ grows larger as n goes to infinity.

One consequence of this is the following.

Lemma 4.7.

$$\log|d(nP)| \leq n^2 C$$

for some constant C.

Proof.

$$\log|d(nP)| \leq h(nP) \leq n^2\hat{h}(P) + O_E(1) \leq n^2 C.$$

□

Actually, Silverman shows, using a strong version of Siegel's Theorem, that both $x(nP)$ and $d(nP)$ must grow large as n goes to infinity.

Lemma 4.8. *[49, Lemma 8] For any $\epsilon > 0$,*

$$(1-\epsilon)n^2\hat{h}(P) + O_{E,\epsilon}(1) \leq \log|d(nP)| \leq n^2\hat{h}(P) + O_E(1).$$

Then, we consider the sequence $d_n = d(nP)$, and we define D_n to be the largest divisor of d_n which is relatively prime to $d_1 d_2 \cdots d_{n-1}$. In other words, D_n is divisible precisely by the primes that appear for the first time in d_n for the sequence d_i. Silverman shows the following lemma.

Lemma 4.9. *[49, Lemma 9] There is a constant $n_0(E)$ such that for any $\epsilon > 0$ and any $n \geq n_0(E)$,*

$$\log |D_n| \geq \left(\frac{1}{3} - \epsilon\right) n^2 \hat{h}(P) - \log(n) + O_{\epsilon,E}(1).$$

Note in particular that for n large enough, $D_n > 1$, meaning that for *every* n from some point on, there is at least one new prime p dividing d_n but none of d_i for $i < n$, which is exactly the result we need.

Lemma 4.10. *There is a constant n_1 depending on E and P such that for any $n \geq n_1$, there exists a prime p_n dividing d_n but not dividing d_i for $i < n$.*

This can be used to immediately prove Theorem 4.2.

Proof of Theorem 4.2. For simplicity, we will prove the theorem in the specific case where $E(\mathbb{Q})$ is torsion-free. The result still holds when $E(\mathbb{Q})$ has a torsion part, and the same argument can be used. Since we suppose that the rank of $E(\mathbb{Q})$ is 1, take the point G to be a generator for $E(\mathbb{Q})$. Then, given our two points A and B, write

$$A = aG$$

$$B = bG.$$

Hence, the elliptic sequence boils down to $NA - B = (Na - b)G$, which is a subsequence of nP in the case $P = G$.

We then claim that

$$\#\{p \leq x \text{ prime } : p|d_{an-b}\} \gg \#\left\{p \text{ prime } : p|d_{an-b}, n \leq C'\sqrt{\log x}\right\}$$

for some constant C'. Indeed, from lemma 4.7, we have that $|d_n| \leq e^{n^2 C}$ for some constant C. Suppose that $p|d_{an-b}$ with $n \leq C'\sqrt{\log x}$. Then,

$$p \leq d_{an-b} \leq e^{C(an-b)^2} \leq x$$

for C' chosen properly.

However, lemma 4.9 gives us that for n large enough, every n yields at least one distinct prime p in the set. Therefore we obtain

$$\#\left\{p \text{ prime } : p|d_{an-b}, n \leq C'\sqrt{\log x}\right\} \gg \sqrt{\log x}.$$

□

Remark 4.11. We do not absolutely need the rank of $E(\mathbb{Q})$ to be 1 for the proof to work. We actually only need the points A and B to lie in a cyclic subgroup of $E(\mathbb{Q})$.

4.4 Local canonical height

We do not see any fundamental obstruction to Theorem 4.2 holding for elliptic curves of higher rank. However, when trying to extend the method of this chapter to those curves, we do face some issues which we were unsuccessful to resolve. In this section and the next, we examine this situation.

Let us follow [61] in the specific case of an elliptic curve over $\mathbb{Q}$. Let $\mathfrak{p}$ be any place of $\mathbb{Q}$, and $\mathbb{Q}_\mathfrak{p}$ the associated local field. Let $\nu_\mathfrak{p}$ denote the associated additive absolute value. Let E be an elliptic curve defined over $\mathbb{Q}$, and fix a minimal Weierstrass equation defining it.

Let $M_\mathbb{Q}$ be the set of all places of $\mathbb{Q}$. In particular, $M_\mathbb{Q}$ consists of all primes p, along with the archimedean place denoted by ∞. For any $x \in \mathbb{Q}^*$, define

$$|x|_p = p^{-\operatorname{ord}_p(x)}$$

for p the non-archimedean places of $M_\mathbb{Q}$, and $|x|_\infty = |x|$ the usual absolute value. Then, we have the additive absolute value associated to the place $\mathfrak{p} \in M_\mathbb{Q}$ as

$$\nu_\mathfrak{p}(x) = -\log |x|_\mathfrak{p} .$$

Note that we have the following *product formula*: for any $x \in \mathbb{Q}^*$,

$$\prod_{\mathfrak{p} \in M_\mathbb{Q}} |x|_\mathfrak{p} = 1$$

and taking logarithms, we obtain the *sum formula*

$$\sum_{\mathfrak{p} \in M_\mathbb{Q}} \nu_\mathfrak{p}(x) = 0.$$

Let $P = (x, y) \in E(\mathbb{Q})$ be a non-zero rational point with $x = \frac{\xi}{\eta}$, for

$\xi, \eta \in \mathbb{Z}, \eta \neq 0$. Define the *ordinary global height* h of P as

$$\begin{aligned} h(P) &:= \frac{1}{2} \log \prod_{\mathfrak{p} \in M_{\mathbb{Q}}} \max\left\{ |\xi|_{\mathfrak{p}}, |\eta|_{\mathfrak{p}} \right\} \\ &= \frac{1}{2} \log \prod_{\mathfrak{p} \in M_{\mathbb{Q}}} \left| \frac{1}{\eta} \right|_{\mathfrak{p}} \max\left\{ |x|_{\mathfrak{p}}, 1 \right\} \\ &= \frac{1}{2} \log \prod_{\mathfrak{p} \in M_{\mathbb{Q}}} \max\left\{ |x|_{\mathfrak{p}}, 1 \right\} \end{aligned}$$

by the product formula. As such, note that $h(P)$ is independent of the fraction representation of x. Also note that when taking $(\xi, \eta) = 1$, the first line above becomes

$$h(P) = \frac{1}{2} \log \max\{|\xi|, |\eta|\}$$

which is the usual definition of the naive height. Applying the logarithm, we obtain the two following corresponding additive expressions

$$\begin{aligned} h(P) &= -\frac{1}{2} \sum_{\mathfrak{p} \in M_{\mathbb{Q}}} \min\{\nu_{\mathfrak{p}}(\xi), \nu_{\mathfrak{p}}(\eta)\} \\ &= -\frac{1}{2} \sum_{\mathfrak{p} \in M_{\mathbb{Q}}} \min\{\nu_{\mathfrak{p}}(x), 0\}. \end{aligned}$$

From this, we define the *ordinary local height* $h_{\mathfrak{p}}$ of $P = (x, y) \in E(\mathbb{Q})$ relative to the place $\mathfrak{p} \in M_{\mathbb{Q}}$ as

$$h_{\mathfrak{p}}(P) = -\frac{1}{2} \min\{\nu_{\mathfrak{p}}(x), 0\}$$

if P is not zero, and to be equal to 0 when P is zero.

As such, we have have

$$h(P) = \sum_{\mathfrak{p} \in M_{\mathbb{Q}}} h_{\mathfrak{p}}(P).$$

Note that when we write $x = \frac{\xi}{\eta}$ in reduced form, then

$$h_p(P) = -\frac{1}{2}\min\{\nu_p(x), 0\} = \frac{1}{2}\nu_p(\eta). \tag{4.4.1}$$

We have the following theorem.

Theorem 4.12. *For an elliptic curve E with discriminant Δ over $\mathbb{Q}_\mathfrak{p}$ with additive absolute value $\nu_\mathfrak{p}$, there exists a unique function*

$$\hat{h}_\mathfrak{p} : E(\mathbb{Q}_\mathfrak{p}) \setminus \{0\} \longrightarrow \mathbb{R}$$

such that

(1) $\hat{h}_\mathfrak{p}$ is equivalent to the ordinary local height $h_\mathfrak{p}$ on $E(\mathbb{Q}_\mathfrak{p})$.

(Actually they are equal except for finitely many places $\mathfrak{p}$.)

(2) $\hat{h}_\mathfrak{p}$ is "almost" a quadratic form on $E(\mathbb{Q}_\mathfrak{p})$, that is,

$$\hat{h}_\mathfrak{p}(P+Q) + \hat{h}_\mathfrak{p}(P-Q) = 2\hat{h}_\mathfrak{p}(P) + 2\hat{h}_\mathfrak{p}(Q) + \nu_\mathfrak{p}(x_P - x_Q) - \frac{1}{6}\nu_\mathfrak{p}(\Delta)$$

where $P = (x_P, y_P), Q = (x_Q, y_Q) \in E(\mathbb{Q}_\mathfrak{p})$ such that none of P, Q, or $P \pm Q$ are zero.

4.5 Application to the elliptic two-variable Artin conjecture

In order to tackle the elliptic two-variable Artin conjecture for general elliptic curves, we need to look at the number of distinct prime divisors of

the sequence d_n^*, where

$$nA - B = \left(\frac{x_n^*}{{d_n^*}^2}, \frac{y_n^*}{{d_n^*}^3} \right).$$

In particular, we would like to show that for "most" n, "most" of the prime divisors of d_n are also prime divisors of d_n^*.

Recall our notation that the point $B \in E(\mathbb{Q})$ is written as

$$B = \left(\frac{x(B)}{d(B)^2}, \frac{y(B)}{d(B)^3} \right).$$

Notice that from (4.4.1) above, we have $h_p(nA - B) = \mathrm{ord}_p(d_n^*)$ and similarly $h_p(nA) = \mathrm{ord}_p(d_n)$. Also, from part (1) of Theorem 4.12, we know that those are respectively essentially $\hat{h}_p(nA - B)$ and $\hat{h}_p(nA)$ (except for finitely many primes p). Therefore, part (2) of Theorem 4.12 for $P = nA$ and $Q = B$ yields (for primes of good reduction)

$$\begin{aligned} \hat{h}_p(nA + B) + \hat{h}_p(nA - B) &= 2\hat{h}_p(nA) + 2\hat{h}_p(B) + \nu_p\left(\frac{x_n}{d_n^2} - \frac{x(B)}{d(B)^2} \right) \\ &= \mathrm{ord}_p\left(x_n d(B)^2 - d_n^2 x(B) \right). \end{aligned} \tag{4.5.1}$$

Therefore, we obtain that the primes dividing the denominator of either $nA - B$ or $nA + B$ are those dividing $x_n d(B)^2 - d_n^2 x(B)$. However, $\overline{B} \in \langle \overline{A} \rangle$ if and only if $\overline{-B} \in \langle \overline{A} \rangle$, and so every one of those primes would be in the set $S_{A,B}$.

Although we were not able to obtain a result similar to Theorem 4.2 for every elliptic curve using these ideas, we can get an analogue of Pólya's argument to show the following theorem.

Theorem 4.13. *Let A and B be points of infinite order in $E(\mathbb{Q})$. Then, the set $S_{A,B}$ is infinite.*

To do so, we will use the following Theorem, used in [50] to show the Lutz-Nagell Theorem.

Theorem 4.14 ([50, p.55])**.** *Let p be a prime, R the ring of rational numbers with denominator prime to p, and let $C(p^\nu)$ be the set of rational points (x, y) on $E(\mathbb{Q})$ for which x has denominator divisible by $p^{2\nu}$, plus the point at infinity $\mathcal{O}$. Then, for every $\nu \geq 1$, the set $C(p^\nu)$ is a subgroup of $E(\mathbb{Q})$. Moreover, there exists a one-to-one homomorphism*

$$\frac{C(p^\nu)}{C(p^{3\nu})} \longrightarrow \frac{p^\nu R}{p^{3\nu} R}.$$

Note in particular that the index $[C(p^\nu) : C(p^{3\nu})]$ divides $p^{2\nu}$ and therefore is finite. As such, we have the following corollary which we will use in the proof of Theorem 4.13.

Corollary 4.15. *Fix $A, B \in E(\mathbb{Q})$. Let p be a prime, and n_p be some integer such that p divides $d(n_p A)$. Then, there exists a positive integer m_p such that*

$$\operatorname{ord}_p\left(d(n_p m_p A)\right) > \operatorname{ord}_p\left(d(B)\right).$$

Proof. This follows directly from Theorem 4.14. Indeed, if p divides $d(n_p A)$ with order ν, then $n_p A \in C(p^\nu)$. Multiplying $n_p A$ by the index $j_p = [C(p^\nu) : C(p^{3\nu})]$, we get that $d(j_p n_p A)$ will be divisible by p with order at least 3ν.

Repeating this process until the order is bigger than $\mathrm{ord}_p(d(B))$, we obtain the result. □

Using this, we now prove Theorem 4.13.

Proof of Theorem 4.13. We first suppose that the set $S_{A,B}$ is finite. Then, we show a contradiction by exhibiting a subsequence of $nA-B$, say n_kA-B, such that $|d(n_kA-B)|$ is bounded. Indeed, by Lemma 4.8 and explicit formulas for addition on elliptic curves it is easy to show that $|d(nA-B)| \to \infty$ as n goes to infinity.

Since the only primes dividing $d(nA-B)$ are those in $S_{A,B}$, it is sufficient to show that $\mathrm{ord}_p(d(n_kA-B))$ is bounded for every $p \in S_{A,B}$.

Define

$$\ell = \prod_{p \in S_{A,B}} m_p \, |E(\mathbb{F}_p)|$$

where m_p are as in Corollary 4.15 (with $n_p = |E(\mathbb{F}_p)|$). Then consider the subsequence $n_k = k\ell$.

Fix $p \in S_{A,B}$. Then,

$$n_kA = n'_k \left(|E(\mathbb{F}_p)| \, A \right) \equiv 0 \bmod p$$

for some n'_k, and so $p | d(n_kA)$ for every $k \geq 1$.

By equation (4.4.1), we have

$$\mathrm{ord}_p(d(n_kA-B)) = 2h_p(n_kA-B)$$

and by Theorem 4.12,

$$\begin{aligned} &= 2\hat{h}_p(n_kA - B) \\ &\leq 2\hat{h}_p(n_kA - B) + 2\hat{h}_p(n_kA + B). \end{aligned}$$

By equation (4.5.1),

$$\begin{aligned} &= 2\,\mathrm{ord}_p\left(x_{n_k}d(B)^2 - d_{n_k}^2x(B)\right) \\ &= 2\min\left(\mathrm{ord}_p(x_{n_k}d(B)^2), \mathrm{ord}_p(d_{n_k}^2x(B))\right) \qquad (4.5.2) \end{aligned}$$

unless $\mathrm{ord}_p(x_{n_k}d(B)^2) = \mathrm{ord}_p(d_{n_k}^2x(B))$, by Fact 2.2. We consider the two cases separately.

Suppose that $\mathrm{ord}_p(x_{n_k}d(B)^2) = \mathrm{ord}_p(d_{n_k}^2x(B))$. Since p divides d_{n_k}, it does not divide x_{n_k} by coprimality. Also, we conclude that p does divide $d(B)$ by the previous equation, and so doesn't divide $x(B)$ by coprimality. We have

$$\mathrm{ord}_p(d(B)^2) = \mathrm{ord}_p(d_{n_k}^2).$$

However, since m_p divides ℓ, we have that $\mathrm{ord}_p(d(B)^2) < \mathrm{ord}_p(d_{n_k}^2)$ which is a contradiction. This case therefore never happens.

From equation (4.5.2), we have

$$\begin{aligned} \mathrm{ord}_p(d(n_kA - B)) &= 2\min\left(\mathrm{ord}_p(x_{n_k}d(B)^2), \mathrm{ord}_p(d_{n_k}^2x(B))\right) \\ &\leq 2\,\mathrm{ord}_p(d_{n_k}^2x(B)) \leq 2\,\mathrm{ord}_p(x(B)) \end{aligned}$$

since p does not divide x_n by coprimality. We conclude that $\mathrm{ord}_p(d(n_kA - B))$ is bounded for every $p \in S_{A,B}$ and we have a contradiction. This completes the proof of the theorem. □

Chapter 5

Prime divisors of sparse values of cyclotomic polynomials

5.1 Statement of the result

Let $f_a(p)$ be the order of a in the group $(\mathbb{Z}/p\mathbb{Z})^\times$. For the sake of readability, we will write $f(p)$ instead of $f_a(p)$ when a is clear from context. Let $\Phi_N(x)$ denote the Nth cyclotomic polynomial.

We call the set of primes such that $a^{p-1} \equiv 1 \bmod p^2$ *Wieferich primes (for a)*. Classically, Wieferich primes usually refer to the specific case where $a = 2$. However, every argument goes through for arbitrary $a \geq 2$. We expect them to be sparse in all the primes. The only Wieferich primes $p \leq 3 \times 10^9$ for $a = 2$ are 1093 and 3511, and those are the only two we know of at the moment. Heuristically, if we think of $(a^{p-1} - 1)/p$ as a

random integer, the probability that p divides it is approximately $1/p$. As such, according to these heuristics, we could expect around

$$\sum_{p \leq x} \frac{1}{p} \ll \log \log x$$

Wieferich primes up to x. As they are expected to be sparse, it is difficult to determine whether there are finitely many or infinitely many of them.

We can then restrict our attention to the set of *super-Wieferich primes (for a)* which are the primes p such that $a^{p-1} \equiv 1 \bmod p^3$. Obviously, they form a subset of the Wieferich primes. However, the same heuristics suggest that the number of such primes is

$$\sum_{p} \frac{1}{p^2} \leq c'$$

that is, there are only finitely many of them. In turn, this suggests that there should be an integer k, independent of p, for which $a^{p-1} \not\equiv 1 \bmod p^k$ for any prime p. Notice that this is an even weaker assumption to make than the finiteness of super-Wieferich primes.

The hypothesis we will be using in the proof of the next result is even weaker. Let p^{γ_p} be the largest power p dividing $a^{p-1} - 1$, and p^{α_p} be the largest power p dividing $a^{f(p)} - 1$. Instead of looking at the γ_p, our hypothesis will concern α_p. Since $f(p) | p - 1$, we can write $f(p)r = p - 1$ so that

$$a^{p-1} = a^{f(p)r} \equiv 1^r \equiv 1 \bmod p^{\alpha_p}$$

and so

$$\alpha_p \leq \gamma_p \tag{5.1.1}$$

for all p. We will be assuming in Theorem 5.1 that α_p is bounded. Again, this would follow from the finiteness of super-Wieferich primes, and is even a substantially weaker condition.

Theorem 5.1. *Let $P(m)$ denote the largest prime divisor of m. Let $a > 1$ be an integer. Suppose that there exists a constant κ for which $\alpha_p \leq \kappa$ for all primes p. Then, there exists a positive constant C (depending on a and κ) such that*

$$P\left(\Phi_N(a)\right) > C\phi(N)^2$$

for all N.

Remark 5.2. Recall that

$$\prod_{d|N} \Phi_d(a) = a^N - 1 \tag{5.1.2}$$

and therefore, $\Phi_N(a)$ divides $a^N - 1$. As such, the above Theorem 5.1 implies that $P(a^N - 1) > C\phi(N)^2$ for N large enough granted that α_p is bounded. Additionally, recall that we have the bound $\phi(N) \gg \frac{N}{\log\log N}$ due to Ramanujan. As such, we get as a corollary that under the same hypothesis on α_p,

$$P(a^N - 1) > C' \frac{N^2}{(\log\log N)^2}.$$

In 1965, Erdős [8] conjectured that

$$\frac{P(2^n - 1)}{n} \to \infty \quad \text{as } n \to \infty.$$

This prompted the study of this special case of Lucas numbers. In 1975, Stewart showed [53] that given $0 < \lambda < 1/\log 2$,

$$\frac{P(a^n - b^n)}{n} \to \infty$$

as n goes to infinity, provided that n only runs through integers with at most $\lambda \log\log n$ prime factors. By a famous theorem of Hardy and Ramanujan [18], "almost all" numbers (in the sense of natural density) satisfy this condition.

In 2002, Ram Murty and Wong [40] proved, conditionally to the *abc* conjecture, that for any $\epsilon > 0$ and $a > b > 0$ integers, then

$$P(a^n - b^n) > n^{2-\epsilon} \tag{5.1.3}$$

for n large enough, which in particular gives a conditional proof of Erdős's conjecture. As remarked above, Theorem 5.1 gives an improvement on this result in the specific case of $b = 1$, mostly by weakening the hypothesis.

In 2004, Murata and Pomerance [32] proved conditionally to the generalized Riemann hypothesis that

$$P(2^n - 1) > \frac{n^{4/3}}{\log\log n}$$

for a set of positive integers n of asymptotic density 1.

Finally, in 2013, Stewart [52] proved Erdős's conjecture unconditionally, specifically by showing that for suitable α and β (for which the corresponding Lucas sequence is non-degenerate),

$$P(\Phi_n(\alpha, \beta)) > n \exp\left(\frac{\log n}{104 \log\log n}\right)$$

for n large enough. Here, $\Phi_n(\alpha, \beta)$ denotes the homogeneous cyclotomic polynomial, and for $\alpha = 2$, $\beta = 1$, we obtain

$$P(\Phi_n(2)) > n \exp\left(\frac{\log n}{104 \log\log n}\right).$$

Note that Erdős's conjecture follows from this for the reasons stated in remark 5.2 above.

These last two results use heavily the method of linear forms in logarithms and methods of transcendental number theory.

The exponents α_p and γ_p have already been introduced. The other exponents β_p and δ_n that we will be using throughout this chapter are defined as follows.

For a prime number p, we define the integer β_p as the largest power of p dividing $\Phi_{f(p)}(a)$, i.e.

$$p^{\beta_p} || \Phi_{f(p)}(a).$$

For any integer $n > 4$, $n \neq 6, 12$, we will see from Lemma 5.7 that there is at most one prime dividing both n and $\Phi_n(a)$, which we will call P_n. We define δ_n as the largest power of P_n dividing $\Phi_n(a)$, i.e.

$$p^{\delta_p} || \Phi_n(a).$$

Actually, in Lemma 5.7 below, we will see that δ_n is always 0 or 1.

We will be proving the following theorem about δ_n.

Theorem 5.3. *For some $\theta < 1$,*

$$\sum_{n \leq x} \delta_n \log P_n = O(x^\theta).$$

This also gives the following obvious corollary.

Corollary 5.4. *For some $\theta < 1$,*

$$\sum_{n \leq x} \delta_n = O(x^\theta).$$

In particular, this shows that δ_n is zero "most of the time".

5.2 Preliminaries about $\Phi_N(a)$

We start by stating a few facts about the cyclotomic polynomials $\Phi_n(x)$.

Proposition 5.5. *For any prime p not dividing m or a,*

$$f_a(p) = m \Leftrightarrow p | \Phi_m(a).$$

Proof. Let p be a prime not dividing m or a.

Suppose that $f(p) = m$. Then,

$$a^m - 1 \equiv 0 \bmod p$$

$$\prod_{d|m} \Phi_d(a) \equiv 0 \bmod p$$

and so $\Phi_d(a) \equiv 0 \bmod p$ for some d dividing m. Suppose that $d \neq m$, then

$$a^d - 1 = \prod_{\delta|d} \Phi_\delta(a) \equiv 0 \bmod p$$

and $a^d - 1 \equiv 0 \bmod p$ for $d < m$ which is a contradiction to the definition of order of $m = f(p)$. We conclude that $d = m$ and so p divides $\Phi_m(a)$.

For the other direction, suppose that p divides $\Phi_m(a)$. Then,

$$a^m - 1 = \prod_{d|m} \Phi_d(a) \equiv 0 \bmod p$$

and so $f(p)$ divides m.

By the above, we know that p divides $\Phi_{f(p)}(a)$. Suppose that $m \neq f(p)$. Then, $f(p)$ divides m properly and we have

$$a^m - 1 = \Phi_m(a)\Phi_{f(p)}(a) \prod_{\substack{d|m \\ d\neq m, f(p)}} \Phi_d(a) \equiv 0 \mod p^2.$$

Since $\Phi_m(a) \equiv \Phi_m(a+p) \bmod p$ and $\Phi_{f(p)}(a) \equiv \Phi_{f(p)}(a+p) \bmod p$, we also have

$$(a+p)^m - 1 = \Phi_m(a+p)\Phi_{f(p)}(a+p) \prod_{\substack{d|m \\ d\neq m, f(p)}} \Phi_d(a+p) \equiv 0 \mod p^2.$$

On the other hand, by the binomial theorem,

$$1 \equiv (a+p)^m = a^m + ma^{m-1}p \equiv 1 + ma^{m-1}p \mod p^2.$$

and hence

$$ma^{m-1} \equiv 0 \bmod p.$$

However, this is a contradiction to the hypothesis that p does not divide m and is coprime to a. We conclude that $m = f(p)$. □

Proposition 5.6.

$$\Phi_N(a) \geq \frac{1}{2} a^{\phi(N)}.$$

See [57] for the proof.

We also need the following description of the primes dividing $\Phi_n(a)$, which is [54, Lemma 6].

Lemma 5.7. *If $n > 4$ and $n \neq 6, 12$, then $P(n/(3,n))$ divides $\Phi_n(a)$ to at most the first power. All other primes factors of $\Phi_n(a)$ are congruent to* 1 (mod n).

Finally, we will need to use the Brun-Titchmarsh Theorem, which we recall here.

Theorem 5.8 (Brun-Titchmarsh)**.** *Let $\theta < 1$ and $d < x^\theta$. For x sufficiently large,*

$$\sum_{\substack{p \leq x \\ p \equiv 1 \bmod d}} \log p \leq \frac{2x \log x}{\phi(d) \log(x/d)}$$

where $\phi(d)$ is Euler's totient function.

5.3 Proof of Theorem 5.1

Recall that we define the integer β_p as the largest power of p dividing $\Phi_{f(p)}(a)$, i.e.

$$p^{\beta_p} || \Phi_{f(p)}(a)$$

and the integer α_p as the largest power of p dividing $a^{f(p)} - 1$, i.e.

$$p^{\alpha_p} || a^{f(p)} - 1.$$

Clearly, $\alpha_p \geq 1$ for every prime p.

Proposition 5.9. *For every prime p coprime to a, $\alpha_p = \beta_p$.*

Proof. Let p be any prime coprime to a. We can factor $a^{f(p)} - 1$ above to get that

$$p^{\alpha_p} || \prod_{d|f(p)} \Phi_d(a).$$

We claim that actually, p cannot divide any factor $\Phi_d(a)$ other than $\Phi_{f(p)}(a)$. Indeed, suppose that p divides $\Phi_d(a)$ for some d strictly dividing $f(p)$. Clearly, p does not divide d as d divides $f(p)$ which divides $p-1$. Therefore, by Proposition 5.5, $f(p) = d$ which is a contradiction. We conclude that

$$p^{\alpha_p} || \Phi_{f(p)}(a)$$

which means $\alpha_p = \beta_p$ for every p. □

Note that we essentially have the prime factorization for $\Phi_n(a)$. If we take any n, then every prime factor p of $\Phi_n(a)$ other than those dividing n are such that $f(p) = n$ by Proposition 5.5. Therefore, by the above, for those primes, $p^{\alpha_p} || \Phi_n(a)$. The only prime factors of $\Phi_n(a)$ for which we don't know the order are those also dividing n. By Lemma 5.7, there is at most one such prime, namely $P_n = P(n/(3, n))$ (when $n > 4$ and not 6 or 12). Additionally, Lemma 5.7 tells us that

$$P_n^{\delta_n} || \Phi_n(a)$$

where δ_n is either 0 or 1. We just proved the following.

Proposition 5.10. *For $n > 4$, $n \neq 6, 12$,*

$$\Phi_n(a) = P_n^{\delta_n} \prod_{\substack{p \mid \Phi_n(a) \\ p \neq P_n}} p^{\alpha_p}.$$

With this description in hand, let us now prove Theorem 5.1.

Proof of Theorem 5.1. We will argue by contradiction. Suppose that $P(\Phi_n(a)) \leq c\phi(n)^2$. Then,

$$\Phi_n(a) \leq P_n^{\delta_n} \prod_{\substack{p \leq c\phi(n)^2 \\ p \neq P_n}} p^{\alpha_p}$$

and by the second part of Lemma 5.7,

$$\leq P_n^{\delta_n} \prod_{\substack{p \leq c\phi(n)^2 \\ p \equiv 1 \bmod n}} p^{\alpha_p}.$$

By taking the logarithm,

$$\log \Phi_n \leq \log P_n^{\delta_n} + \sum_{\substack{p \leq c\phi(n)^2 \\ p \equiv 1 \bmod n}} \alpha_p \log p.$$

Since we assume that $\alpha_p \leq \kappa$ for all p, we have

$$\leq \log P_n^{\delta_n} + \kappa \sum_{\substack{p \leq c\phi(n)^2 \\ p \equiv 1 \bmod n}} \log p$$

and by Theorem 5.8

$$\ll \delta_n \log P_n + \kappa \left(\frac{2c\phi(n)^2}{\phi(n)} \right) \tag{5.3.1}$$

for n large enough.

On the other hand, by Proposition 5.6 we have

$$\Phi_n(a) \geq \frac{1}{2}a^{\phi(n)}$$

and so

$$\log \Phi_n(a) \geq \phi(n) \log a - \log 2. \tag{5.3.2}$$

Putting (5.3.1) and (5.3.2) together, we get that

$$\phi(n) \log a - \log 2 \ll 2\kappa c\phi(n) + \delta_n \log P_n.$$

Note that $\log P_n \leq \log n$. Therefore, if c is sufficiently small, we obtain a contradiction for n large enough. □

As we pointed out, this result is close to (5.1.3) which Murty and Wong obtained assuming the *abc* conjecture. We remark here that assuming a weaker hypothesis, to which we will refer as the *quasi-abc*, we easily get a lower bound on $P(a^n - b)$ for any $a, b \in \mathbb{Z}$ with $a \geq 2$.

Conjecture 5.11 (The quasi-*abc* conjecture)**.** *There exists a constant k such that for any mutually coprime integers a, b and c such that $a + b = c$,*

$$\max\left(|a|, |b|, |c|\right) \leq \mathrm{rad}(abc)^k.$$

Proposition 5.12. *Let a, b be integers, $a \geq 2$. Assuming the quasi-abc conjecture, there exists an effectively computable constant C depending on a and b such that*

$$P(a^n - b) \geq Cn.$$

Proof. We write $a^n - b + b = a^n$ and apply the quasi-*abc* conjecture. There exists a constant k such that

$$a^n \leq \left(ab \prod_{p | a^n - b} p \right)^k$$

and so

$$n \log a \leq k \sum_{p \leq P(a^n - b)} \log p + C'.$$

We know that (see [37, 3.1.2])

$$\sum_{p \leq x} \log p \ll x,$$

by Chebycheff. Therefore, we conclude that

$$P(a^n - b) \geq Cn$$

as required. □

5.4 Preliminaries about $f_a(p)$

We first need the following simple lemma.

Lemma 5.13. *For any prime p and any integer $1 \leq k \leq p^n$,*

$$\mathrm{ord}_p \left(\binom{p^n}{k} \right) = n - \mathrm{ord}_p(k).$$

Proof. For $k = p^n$, this is clear. For any m in the range $1 \leq m < p^n$, by the ultrametric inequality (Fact 2.2), we have that $\mathrm{ord}_p(p^n - m) = \mathrm{ord}_p(m)$.

By definition,

$$k!\binom{p^n}{k} = p^n(p^n-1)\cdots(p^n-(k-1)),$$

and by taking the valuation on both sides

$$\mathrm{ord}_p(k!) + \mathrm{ord}_p\left(\binom{p^n}{k}\right) = n + \mathrm{ord}_p((k-1)!),$$

from which the result follows directly. □

Proposition 5.14. *Let p be any prime, a any non-zero integer and define α_p as $\mathrm{ord}_p(a^{f(p)}-1)$, that is $p^{\alpha_p}||a^{f(p)}-1$. Then, for any $r \geq 0$,*

$$f\left(p^{\alpha_p+r}\right) = p^r f(p).$$

Proof. In this proof we fix p and write $\alpha = \alpha_p$ for simplicity of notation. To begin, notice the following three facts that are true for any r.

(1) $f(p^{\alpha+r})$ divides $p^r f(p^\alpha)$.

Indeed,

$$a^{p^r f(p^\alpha)} = (1+mp^\alpha)^{p^r}$$

for some integer m, and so by the binomial theorem

$$a^{p^r f(p^\alpha)} = \sum_{k=0}^{p^r}\binom{p^r}{k}m^k p^{k\alpha}.$$

We note in passing that for any integer $k > 0$,

$$k \geq p^{\mathrm{ord}_p(k)} \geq 2^{\mathrm{ord}_p(k)} \geq \mathrm{ord}_p(k)+1.$$

For $k > 0$, the kth term in the sum is given by

$$T_k = \binom{p^r}{k} m^k p^{k\alpha}$$

and so

$$\mathrm{ord}_p(T_k) \geq r - \mathrm{ord}_p(k) + k\alpha,$$

and by Lemma 5.13,

$$\begin{aligned} &\geq r - (k-1) + k\alpha \\ &\geq r + \alpha + (\alpha - 1)(k-1) \\ &\geq r + \alpha, \end{aligned}$$

where the last inequality follows from $\alpha \geq 1$. Therefore, we conclude that

$$a^{p^r f(p^\alpha)} \equiv 1 \bmod p^{\alpha+r},$$

meaning that $f(p^{\alpha+r})$ divides $p^r f(p^\alpha)$.

(2) For any m, $f(p^m)$ divides $f(p^{m+1})$.

This is because

$$a^{f(p^{m+1})} \equiv 1 \bmod p^{m+1}$$

and so

$$a^{f(p^{m+1})} \equiv 1 \bmod p^m.$$

Note that this fact actually implies the following

(3) $f(p) = f(p^2) = \ldots = f(p^\alpha)$.

Indeed, for any $1 \leq m \leq \alpha$, $f(p)|f(p^m)$ by the above. On the other hand, $a^{f(p)} - 1 \equiv 0 \bmod p^m$, meaning that $f(p^m)|f(p)$.

Now, to show the statement of Proposition 5.14, we proceed by induction on r. From (3) above, we can instead show that $f\left(p^{\alpha_p + r}\right) = p^r f(p^\alpha)$.

When $r = 1$, we have from (1) above that $f(p^{\alpha+1})|pf(p^\alpha)$. However, $f(p^{\alpha+1})$ must be a multiple of p, as otherwise

$$f(p^{\alpha+1})|f(p^\alpha) = f(p)$$

meaning that

$$a^{f(p)} - 1 \equiv 0 \bmod p^{\alpha+1}$$

which contradicts the definition of α.

On the other hand, by (2) above, $f(p^{\alpha+1})$ must be a multiple of $f(p^\alpha)$. We conclude that $f(p^{\alpha+1}) = pf(p^\alpha)$ which is the base case.

Using induction, we show that $f(p^{\alpha+r}) = p^r f(p^\alpha)$.

As before, using (1) we get

$$f(p^{\alpha+r})|p^r f(p^\alpha).$$

On the other hand, by the induction hypothesis and (2),

$$p^{r-1} f(p^\alpha) = f(p^{\alpha+r-1})|f(p^{\alpha+r}).$$

We get from the above that $f(p^{\alpha+r}) = p^q f(p)$ where q is either r or $r-1$. We are only left to show that q cannot be $r-1$. Suppose it is. Then, on one hand, by definition,

$$a^{f(p^{\alpha+r})} \equiv 1 \bmod p^{\alpha+r}.$$

On the other hand, write $a^{f(p)} = 1 + kp^\alpha$. Then,

$$\begin{aligned} a^{f(p^{\alpha+r})} &= a^{f(p)p^{r-1}} \\ &= (1+kp^\alpha)^{p^{r-1}} \\ &\equiv 1 + kp^{\alpha+r-1} \bmod p^{\alpha+r}. \end{aligned}$$

We can conclude that k must be divisible by p, meaning that $a^{f(p)} = 1 + k'p^{\alpha+1}$, which is a contradiction to the definition of α. □

5.5 Proof of Theorem 5.3

First consider the Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{\log(a^n - 1)}{n^s}.$$

We need the following lemma about $F(s)$.

Lemma 5.15. *We can write the Dirichlet series $F(s)$ as*

$$F(s) = \zeta(s)\left(\sum_p \frac{\alpha_p \log p}{f(p)^s} + D(s)\right)$$

where $D(s)$ is a Dirichlet series absolutely convergent for $\Re(s) > \theta$ for some $\theta < 1$.

To prove this lemma, we will need the following results which can be found in [38].

Theorem 5.16. *For any $\epsilon > 0$,*

$$\sum_{m\geq 1} \frac{1}{m f_a(m)^\epsilon} \leq e^\gamma \log\log a + 2e^\gamma \epsilon^{-1} + C$$

for some constant C.

In the above theorem, the definition of $f_a(p)$ is extended to any integer m as

$$f_a(m) = \inf\left\{r \in \mathbb{Z} : r \geq 1 \text{ and } a^r \equiv 1 \bmod m\right\}.$$

Theorem 5.17. *For any $\epsilon > 0$,*

$$\sum_{p} \frac{\log p}{p f_a(p)^\epsilon} \leq \log\log a + 2\epsilon^{-1} + C$$

for some constant C.

We use this to prove Lemma 5.15.

Proof. First, notice that we can write $\log m = \sum_{d|m} \Lambda(d)$, where Λ is the von Mangoldt function. Therefore, we have the alternative expression for $F(s)$:

$$\begin{aligned} F(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|a^n-1} \Lambda(d) \\ &= \sum_{d=1}^{\infty} \Lambda(d) \sum_{n\,:\,d|a^n-1} \frac{1}{n^s}. \end{aligned}$$

We know that $d|a^n - 1$ if and only if $a^n \equiv 1 \bmod d$ if and only if $f(d)|n$. Thus,

$$\begin{aligned} F(s) &= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \Lambda(d) \sum_{n\,:\,f(d)|n} \frac{1}{n^s} \\ &= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \Lambda(d) \sum_{m=1}^{\infty} \frac{1}{(mf(d))^s} \\ &= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{\Lambda(d)}{f(d)^s} \zeta(s). \end{aligned} \tag{5.5.1}$$

Now we show that

$$\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{\Lambda(d)}{f(d)^s} = \sum_{p} \frac{\alpha_p \log p}{f(p)^s} + D(s)$$

with $D(s)$ as in the statement of the lemma.

We first notice that the summand on the left-hand side is non-zero only when d is a prime power. As such, we have

$$\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{\Lambda(d)}{f(d)^s} = \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \sum_{r=1}^{\infty} \frac{\Lambda(p^r)}{f(p^r)^s}.$$

Note that for a fixed prime p, the summand for r between 1 and α_p will be the same, namely $\frac{\log p}{f(p)^s}$. For $r = \alpha_p + q$, by Proposition 5.14, it will be $\frac{\log p}{p^{qs} f(p)^s}$. We get

$$\begin{aligned}
\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{\Lambda(d)}{f(d)^s} &= \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \left(\frac{\alpha_p \log p}{f(p)^s} + \sum_{q=1}^{\infty} \frac{\log p}{p^{qs} f(p)^s} \right) \\
&= \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\alpha_p \log p}{f(p)^s} + \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\log p}{f(p)^s} \sum_{q=1}^{\infty} \frac{1}{p^{qs}} \\
&= \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\alpha_p \log p}{f(p)^s} + \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\log p}{f(p)^s} \left(\frac{1}{1 - \frac{1}{p^s}} - 1 \right) \\
&= \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\alpha_p \log p}{f(p)^s} + \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\log p}{f(p)^s (p^s - 1)}.
\end{aligned}$$

Consider the series

$$D(s) = \sum_{p:(p,a)=1} \frac{\log p}{f(p)^s (p^s - 1)}.$$

Trying to evaluate the series at $s = 1$, we obtain

$$D(1) = \sum_{p:(p,a)=1} \frac{\log p}{(p-1) f(p)} \leq C' \sum_{p} \frac{\log p}{p f(p)} \leq C''$$

for some constants C' and C'', where the last inequality is obtained from Theorem 5.17. Therefore $D(s)$ is an absolutely convergent series for $s = 1$. However, Landau's Theorem (see [37, 2.5.14]) tells us that a Dirichlet series with non-negative terms must have a singularity at $s = \sigma_0$, where σ_0 is its abscissa of convergence. Since our series $D(s)$ converges at $s = 1$, we conclude that 1 cannot be its abscissa of convergence, and so that $D(s)$ must converge strictly to the left of 1.

Therefore, we have

$$F(s) = \zeta(s)\left(\sum_p \frac{\alpha_p \log p}{f(p)^s} + D(s)\right)$$

with $D(s)$ as required. □

We use this lemma to show Theorem 5.3.

Proof. From Lemma 5.15,

$$\frac{1}{\zeta(s)}\sum_{n=1}^{\infty}\frac{\log\left(a^n-1\right)}{n^s} = \sum_p \frac{\alpha_p \log p}{f(p)^s} + D(s).$$

On one hand,

$$\begin{aligned}
\frac{1}{\zeta(s)}\sum_{n=1}^{\infty}\frac{\log\left(a^n-1\right)}{n^s} &= \left(\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}\right)\left(\sum_{n=1}^{\infty}\frac{\log\left(a^n-1\right)}{n^s}\right) \\
&= \sum_{n=1}^{\infty}\frac{1}{n^s}\left(\sum_{d|n}\mu(d)\log(a^{n/d}-1)\right) \\
&= \sum_{n=1}^{\infty}\frac{1}{n^s}\left(\log\prod_{d|n}(a^{n/d}-1)^{\mu(d)}\right) \\
&= \sum_{n=1}^{\infty}\frac{\log\Phi_n(a)}{n^s}.
\end{aligned}$$

On the other hand, we can write

$$\sum_p \frac{\alpha_p \log p}{f(p)^s} = \sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

as a Dirichlet series where

$$a_n = \sum_{p:f(p)=n}\alpha_p \log p.$$

However, by Proposition 5.5, this is

$$\begin{aligned} &= \sum_{\substack{p|\Phi_n(a) \\ p\neq P_n}} \alpha_p \log p \\ &= \log \prod_{p|\Phi_n(a)} p^{\alpha_p} - \delta_n \log P_n \\ &= \log \Phi_n(a) - \delta_n \log P_n. \end{aligned}$$

Putting the two above statements together, we obtain the following expression for $D(s)$.

$$D(s) = \sum_{n=1}^{\infty} \frac{\delta_n \log P_n}{n^s}.$$

Call $b_n = \delta_n \log P_n$ and notice that b_n are all non-negative. Recall that $D(s)$ converges absolutely strictly to the left of 1. Therefore, for some $\theta < 1$, we have

$$\sum_{n\leq x} b_n \leq \sum_{n\leq x} b_n \left(\frac{x}{n}\right)^{\theta} \leq x^{\theta} \sum_{n=1}^{\infty} \frac{b_n}{n^{\theta}} = Cx^{\theta}$$

and we conclude that

$$\sum_{n\leq x} \delta_n \log P_n = O\left(x^{\theta}\right).$$

□

Corollary 5.4 follows since $\log P_n \geq \log 2$.

5.6 Connection to Wieferich primes

Here, we take a closer look at what it means to be a Wieferich prime in light of Proposition 5.9, and in doing so we prove the following result.

Theorem 5.18. *Suppose that there are only finitely many super-Wieferich primes. Then, there are infinitely many non-Wieferich primes.*

It is not known unconditionally at the moment whether there are infinitely many non-Wieferich primes. From the heuristics presented at the beginning of this chapter, along with the numerical computation, we suspect that this is the case. Also, in [49], Silverman shows, subject to the *abc*-conjecture, that the number of non-Wieferich primes up to x is at least $\gg \log x$. We believe our argument can be modified to yield a lower bound of $\log\log x$, which is more modest but depends on an assumption much weaker than the *abc*-conjecture.

We start by proving the following lemma about the characterization of Wieferich primes.

Lemma 5.19. *The prime p is a Wieferich prime (for a) if and only if*

$$p^2 | \Phi_n(a)$$

for some n.

Moreover, if p^2 divides $\Phi_n(a)$ for some n, then $n = f(p)$.

Finally, p does not divide $\Phi_n(a)$ for n other than $f(p)$ and multiples of p.

Proof. We start by proving the last two statements. Suppose that p divides $\Phi_n(a)$ for some n. Then, by Proposition 5.5, either $n = f(p)$ or p divides n.

Now suppose that $p^2|\Phi_n(a)$ for some n. Since the only prime dividing both n and $\Phi_n(a)$ does so with order at most one, we know that p does not divide n. Therefore, by Proposition 5.5, $n = f(p)$.

For the first part of the lemma, suppose first that p^2 divides $\Phi_n(a)$ for some n. By the above, $n = f(p)$. By (5.1.2), p^2 also divides $a^{f(p)} - 1$. Finally, by (5.1.1), p^2 divides $a^{p-1} - 1$.

To show the other implication, suppose that p is a Wieferich prime. Then,

$$p^2|a^{p-1} - 1 = \prod_{d|p-1} \Phi_d(a).$$

Following exactly the proof of Proposition 5.9, we obtain that p^2 divides $\Phi_{f(p)}(a)$. □

Remark 5.20. Call a prime p a *k-super-Wieferich prime* if $a^{p-1} \equiv 1 \bmod p^k$. The same proof can be used to show the following more general lemma.

Lemma 5.21. *The prime p is a k-super-Wieferich prime ($k \geq 2$) if and only if*

$$p^k|\Phi_n(a)$$

for some n.

Also, if p^k divides $\Phi_n(a)$ for some n, then $n = f(p)$.

Moreover, p does not divide $\Phi_n(a)$ for n other than $f(p)$ and multiples of p.

We now prove Theorem 5.18.

Proof. We start by assuming that there are finitely many super-Wieferich primes. Suppose that p is a super-Wieferich prime. Clearly p is also a Wieferich prime. From Lemma 5.19, p only divides $\Phi_n(a)$ for $n = f(p)$ or when n is a multiple of p. Consider the set

$$\mathcal{W} := \left\{ q \text{ prime} : \begin{array}{c} q \text{ is not a super-Wieferich prime, and} \\ f(p) \neq q \text{ for any super-Wieferich prime } p \end{array} \right\}.$$

Then, for every $q \in \mathcal{W}$, $\Phi_q(a)$ is not divisible by any super-Wieferich prime. Also, since we assume that there are only finitely many super-Wieferich primes, we only remove a finite number of primes from the set of all primes, and so the set $\mathcal{W}$ is infinite.

Let q be any prime number. Then,

$$\begin{aligned} q|\Phi_q(a) &\Rightarrow q|a^q - 1 \\ &\Rightarrow a^q - 1 \equiv 0 \bmod q \\ &\Rightarrow a - 1 \equiv 0 \bmod q \end{aligned}$$

since $a^q \equiv a \bmod q$ by Fermat's little Theorem. Therefore, the only primes q for which q can divide $\Phi_q(a)$ are the divisors of $a - 1$.

Now consider the set

$$\mathcal{P} = \mathcal{W} \cap \{p \text{ prime} : p \text{ does not divide } a - 1\}.$$

For this set, we also have that q does not divide $\Phi_q(a)$ for all $q \in \mathcal{P}$. Since we again only remove finitely many primes from $\mathcal{W}$, we still have that $\mathcal{P}$ is infinite.

We prove the statement of the theorem by the method of contradiction. In particular, we suppose that there are only finitely many non-Wieferich primes. Suppose that there are N of them, and call them $p_1, \ldots, p_N$. Let $q \in \mathcal{P}$, and consider $\Phi_q(a)$. We ask which primes can divide $\Phi_q(a)$, and with what power.

Of course, any non-Wieferich primes can potentially divide $\Phi_q(a)$, but they must do so to at most the first power, as otherwise they would be Wieferich primes by Lemma 5.19. Also, as we remarked above, since $q \in \mathcal{P}$, no super-Wieferich prime can divide $\Phi_q(a)$. As for the Wieferich primes, they can certainly divide $\Phi_q(a)$, but if they do, they must do so with order exactly 2. Indeed, if p is such a Wieferich prime dividing $\Phi_q(a)$, then p^3 dividing $\Phi_q(a)$ would imply that p is a super-Wieferich prime. Also, if p were to divide $\Phi_q(a)$ with order 1, by Lemma 5.19, q would be a multiple of p, that is $p = q$. However, since $q \in \mathcal{P}$, this cannot happen.

We therefore have the general form of $\Phi_q(a)$ as

$$\Phi_q(a) = p_1^{\epsilon_1} \cdots p_N^{\epsilon_N} W^2$$

where each ϵ_i is either 0 or 1, and W is a product of distinct Wieferich primes. Since q is prime, we can write

$$\Phi_q(a) = \frac{a^q - 1}{a - 1}$$

and so

$$a^q - 1 = (a - 1) p_1^{\epsilon_1} \cdots p_N^{\epsilon_N} W^2.$$

We then mimic the argument of Section 2.4. Writing q as $3j + \delta$ for some integer j and $\delta \in \{0, 1, 2\}$, we get

$$a^\delta \left(a^j\right)^3 - 1 = (a-1)p_1^{\epsilon_1} \cdots p_N^{\epsilon_N} W^2.$$

The curves

$$a^\delta X^3 - 1 = (a-1)p_1^{\epsilon_1} \cdots p_N^{\epsilon_N} Y^2$$

are elliptic curves. Moreover, there are 3×2^N of them. By Siegel's Theorem [48, IX.3], there is a finite number of integral points (X, Y) on each of them. However, the above construction gives a distinct integral point on one of the curves for every $q \in \mathcal{P}$. This gives a contradiction, and we conclude that there are infinitely many non-Wieferich primes. □

Remark 5.22. We believe it is possible to get a quantitative lower bound on the number of non-Wieferich primes using this method. We can simply follow Section 2.4 in this thesis to get a lower bound of $\log \log x$ non-Wieferich primes up to x. This should be compared with [49], where Silverman shows that the *abc*-conjecture implies that there are at least $\gg \log x$ non-Wieferich primes up to x.

5.7 Generalizations

In [9], Erdős proved estimates of the form

$$\sum_{d | a^n - 1} \frac{1}{d} \leq C(a) \log \log n. \tag{5.7.1}$$

In Section 5.5, we were considering a very similar sum, namely

$$\sum_{d|a^n-1} \Lambda(d).$$

It would be interesting to see the extent with which we can generalize the above discussion and if we can obtain a result similar to that of Erdős. We exploited the fact that we can write $\log n$ as a sum of $\Lambda(d)$ where d ranges over divisors of n. This is also true for $\sigma(n)/n$ because

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}.$$

In general, let $G(n)$ be an arithmetic function, and $F(n)$ be defined as

$$F(n) = \sum_{d|n} G(d).$$

Then, consider the Dirichlet series given by

$$\sum_{n=1}^{\infty} \frac{F(a^n-1)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|a^n-1} G(d).$$

Under suitable convergence conditions, we can interchange the order of summation to get

$$= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} G(d) \sum_{n:d|a^n-1} \frac{1}{n^s}.$$

Notice once again that the integers n for which d divides $a^n - 1$ are specifically the multiples of $f_a(d)$. We get

$$= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} G(d) \sum_{r=1}^{\infty} \frac{1}{(rf(d))^s}$$

$$= \zeta(s) \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{G(d)}{f(d)^s}.$$

In Section 5.5, we used Theorem 5.17 to show the convergence of the series on the right. Suppose that the Dirichlet series

$$\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{G(d)}{f(d)^s}$$

converges absolutely for $\Re(s) \geq 1$ and the function $F(a^n - 1) \geq 0$ for every n. Then, we could apply the Tauberian Theorem, which we recall here. See [37, Thm 3.3.1] for the proof.

Theorem 5.23. *Let $H(s) = \sum_{n=1}^{\infty} b_n/n^s$ be a Dirichlet series with non-negative coefficients and absolutely convergent for $\Re(s) > 1$. Suppose that $H(s)$ can be extended to a meromorphic function in the region $\Re(s) \geq 1$ having no poles except for a simple pole at $s = 1$ with residue $r \geq 0$. Then,*

$$\sum_{n \leq x} b_n = Rx + o(x)$$

as $x \to \infty$.

We therefore have

$$\sum_{n \leq x} F(a^n - 1) = \sum_{n \leq x} \sum_{d | a^n - 1} G(d) = Cx + o(x)$$

where

$$C = \sum_{d=1}^{\infty} \frac{G(d)}{f(d)}.$$

The above discussion essentially proves the following theorem:

Theorem 5.24. *Let $G(n)$ be an arithmetic function, and $F(n)$ be defined as*

$$F(n) = \sum_{d|n} G(d).$$

Suppose that $F(a^n - 1) \geq 0$ for every n,

$$\sum_{n=1}^{\infty} \frac{F(a^n - 1)}{n^s}$$

converges for $\Re(s) > 1$, and

$$\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{G(d)}{f(d)^s}$$

converges absolutely for $\Re(s) \geq 1$, then

$$\sum_{n \leq x} \sum_{d|a^n-1} G(d) = Cx + o(x)$$

where

$$C = \sum_{d=1}^{\infty} \frac{G(d)}{f(d)}.$$

Applying this to $F(n) = \sigma(n)/n$ and $G(d) = 1/d$, we get that

$$\sum_{n=1}^{\infty} \frac{\sigma(a^n - 1)}{(a^n - 1)n^s} = \zeta(s) \sum_{\substack{d=1 \\ (d,a)=1}} \frac{1}{d\, f(d)^s}.$$

From Theorem 5.16, we know that the series

$$\sum_{\substack{d=1 \\ (d,a)=1}} \frac{1}{d\, f(d)^s}$$

converges absolutely everywhere to the right of 0 (that is for every s with $\Re(s) > 0$). Therefore, Theorem 5.24 above can be applied to obtain the following result.

Corollary 5.25.

$$\sum_{n\le x}\sum_{d\mid a^n-1}\frac{1}{d} = Rx + o(x)$$

where R is the "Romanoff" constant

$$R := \sum_{\substack{d\ge 1\\(d,a)=1}}\frac{1}{d\, f_a(d)}.$$

It is interesting to see that Corollary 5.25 actually gives an improvement of (5.7.1) on average.

Chapter 6

Problems for future research

6.1 Elliptic analogues of conditional positive density

One possible avenue of research is to prove the analogue of the Stephens and Moree-Stevenhagen Theorem (Theorem 1.5) in the context of elliptic curves. We tried to do so as part of this thesis, but unfortunately ran into complications and couldn't find a definitive result. We are convinced, however, that an adaptation of the Stephens and Moree-Stevenhagen argument is possible in this context, and we would like to revisit this problem in future research. We record here the basic approach as well as the obstructions we encountered.

Original Artin Argument

The first thing we need in Artin's original argument is a criterion for the divisibility of $[\mathbb{F}_p^\times : \langle a \rangle]$ by an integer j. We will use $i_a(p)$ as a shorthand for the index of a in $\mathbb{F}_p^\times$. In this classical setting, we have the following criterion.

Proposition 6.1. *For any $a \in \mathbb{Z}^\times$, p any prime not dividing a, the index $i_a(p)$ is divisible by j is and only if p splits completely in the splitting field $F_j = \mathbb{Q}(\zeta_j, a^{1/j})$ of $X^j - a$ over $\mathbb{Q}$.*

Note that this proposition holds for any integer j. Then, if we want to find all primes p for which $\langle a \pmod p \rangle = \mathbb{F}_p^\times$, we find those primes p that do not split completely in any F_j. In particular, it is sufficient to require they do not split in any F_j with j prime.

From the Chebotarev density theorem, we know that the density of primes splitting completely in some F_j is $1/[F_j : \mathbb{Q}]$.

An inclusion-exclusion argument yields the heuristic density of primes not splitting completely in *any* F_j for any j as

$$\sum_{j=1}^{\infty} \frac{\mu(j)}{[F_j : \mathbb{Q}]}.$$

Stephens and Moree-Stevenhagen modified argument

Suppose now that we have two non-zero integers a and b, and that we want to find the primes p for which $b \pmod p \in \langle a \pmod p \rangle$. Since $\mathbb{F}_p^\times$ is cyclic,

there is exactly one subgroup for each divisor of $p-1$. Therefore, this condition is equivalent to requiring that the order of b modulo p divides the order of a modulo p, that is $f_b(p)|f_a(p)$. Equivalently, since the index $i_a(p) = (p-1)/f_a(p)$, this is saying that $i_a(p)$ should divide $i_b(p)$.

Since we now have two integers a and b, we rewrite the proposition above to take that in consideration. Define $F_{j,k} = \mathbb{Q}(\zeta_{jk}, a^{1/jk}, b^{1/j})$. From the criterion above, both indices $i_a(p)$ and $i_b(p)$ are divisible by j if and only if p splits completely in $F_{j,1}$.

We now fix an integer $j \geq 1$, and we consider the set of primes for which $i_a(p) = j$ and $i_b(p)$ is divisible by j. For distinct j, those sets are disjoint, and their union is specifically the set of all primes for which $b \pmod p \in \langle a \pmod p \rangle$.

For $i_a(p)$ to be equal to j and $i_b(p)$ to be divisible by j, we need that

1. p splits completely in $F_{j,1}$ (i.e. both $i_a(p)$ and $i_b(p)$ are divisible by j),

2. but p does not split completely in any $F_{j,k}$ for any integer $k > 1$ (i.e. $i_a(p)$ is not divisible by any multiple of j).

Using Chebotarev and an inclusion-exclusion argument, we get that for this fixed j, the density of primes is

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[F_{j,k}, \mathbb{Q}]}$$

and therefore summing over all possible j, we get the final density as

$$\sum_{j=1}^{\infty}\sum_{k=1}^{\infty}\frac{\mu(k)}{[F_{j,k},\mathbb{Q}]}.$$

Primitive points on elliptic curves

We can also look at a different generalization of Artin's primitive root conjecture, this time in the context of elliptic curves. Given a point A of infinite order of an elliptic curve $E/\mathbb{Q}$, we can ask what is the density of primes p for which $\langle\overline{A}\rangle = \overline{E}(\mathbb{F}_p)$. This was done by Gupta and Murty [15]. As before, we start by finding a criterion for the divisibility of the index $[\langle\overline{A}\rangle : \overline{E}(\mathbb{F}_p)]$ which we call here $i_A(p)$. In particular, we will look at CM elliptic curves $E/\mathbb{Q}$, with complex multiplication by the ring of integer $\mathcal{O}_k$ of some quadratic number field k. For a prime q, call $K_q = k(E[q])$ the q-division field over k. Also, let $\mathfrak{q}$ be a prime ideal above q in k. For the point A, let $\mathfrak{q}^{-1}A$ denote a point Q of $E(\mathbb{C})$ such that $\gamma Q = A$ where $\mathfrak{q} = (\gamma)$ (as $\mathcal{O}_k$ is a PID). Finally, let $L_{\mathfrak{q}} = k(E[\mathfrak{q}], \mathfrak{q}^{-1}A)$.

We have the following two equivalent criteria.

Lemma 6.2. *Suppose that $p \not| q\Delta$. Then, $q|i_A(p)$ if and only if either*

(a) p splits completely in $\mathbb{Q}(E[q])$ or

(b) the q-primary part of $\overline{E}(\mathbb{F}_p)$ is a non-trivial cyclic group and p has a first-degree prime factor in $\mathbb{Q}(q^{-1}A)$.

Note that if some prime p splits completely in $\mathbb{Q}(E[q])$, this means that $q|i_P(p)$ for any point P.

Lemma 6.3. *Let p and q be primes such that p splits in k as $p = \pi_p\overline{\pi_p}$ and such that p does not divide $q\Delta$.*

(a) If q is inert in k, then $q|i_A(p)$ if and only if p splits completely in K_q.

(b) If q ramifies or splits in k, let $q = \mathfrak{q}_1\mathfrak{q}_2$ be its prime ideals factorization in k. Then, $q|i_A(p)$ if and only if (π_p) splits completely in $L_{\mathfrak{q}_1}$ or $L_{\mathfrak{q}_2}$ or K_p.

Implication for the elliptic analogue of the two-variable Artin conjecture

To be able to apply the same argument as in the Moree and Stevenhagen case, we first need to suppose that $E(\mathbb{F}_p)$ is cyclic, as then being a subgroup is equivalent to index divisibility. Suppose that we now have two points of infinite order A and B on the CM elliptic curve $E/\mathbb{Q}$. Then, trying to follow the approach of Moree and Stevenhagen, we would first fix some integer j, and then ask for which primes p does $i_A(p) = j$ and $i_B(p)$ be divisible by j.

Unfortunately, the criteria that we have are only formulated in terms of the primes dividing the index.

For example, if p is a prime that splits completely in $\mathbb{Q}(E[q])$ for some q prime, then we know that q divides both $i_A(p)$ and $i_B(p)$. However, we have no information about the power of p dividing those two indices.

For this reason, we were unable to devise a heuristical argument for the elliptic analogue of the two-variable conjecture. We are hopeful, however, that a careful analysis of the criterion and the Stephens, Moree-Stevenhagen argument could provide a conjectural density.

6.2 Yet another approach to the two-variable Artin conjecture

Here we record a different approach to the two variable conjecture. We try to use information about the original Artin conjecture to tackle the two-variable version. We start by observing that Artin's conjecture implies the two-variable version. As such, we can then suppose that Artin's conjecture is false and see what information we get from that. We record here an incomplete attempt to do so. We then add a few remarks about possible weakening to GRH as the assumption in Theorem 1.5.

Recall the following notations.

$$\begin{aligned}
N_a(x) &= \#\left\{p \leq x \text{ prime } : a \text{ is a primitive root } \bmod p\right\} \\
N_{a,b}(x) &= \#\left\{p \leq x \text{ prime } : b \bmod p \in \langle a \bmod p\rangle\right\} \\
i_a(p) &= \left[\mathbb{F}_p^{\times} : \langle a\rangle\right] \\
K_d &= \mathbb{Q}\left(\zeta_d, a^{1/d}\right) \\
F_{j,k} &= \mathbb{Q}\left(\zeta_{jk}, a^{1/jk}, b^{1/j}\right) \\
\pi(x,K) &= \#\left\{p \leq x \text{ prime } : p \text{ splits completely in } K\right\}.
\end{aligned}$$

Also, we will say an integer N is *z-free* if the only prime factors of N are larger than z.

Recall that the conditional proof of Artin's conjecture start with the inclusion-exclusion argument yielding

$$N_a(x) = \sum_d \mu(d)\pi(x, K_d).$$

Suppose that we take z to be some parameter to be chosen later, and define

$$P_z = \prod_{p \leq z} p,$$

then the sum

$$\sum_{d|P_z} \mu(d)\pi(x, K_d)$$

would specifically sieve out the primes p for which $i_a(p)$ is divisible by a prime less than z. As such,

$$N_a(x) = \sum_{d|P_z} \mu(d)\pi(x, K_d) - \#\{p \leq x : i_a(p) \neq 1 \text{ is } z\text{-free}\}.$$

As we will see in the next section, we can apply an unconditional version of the Chebotarev density theorem to evaluate this sum when the parameter z is chosen small enough. As such, for some density $A(a)$, we can get

$$N_a(x) = A(a)\pi(x) - \#\{p \leq x : i_a(p) \neq 1 \text{ is } z\text{-free}\} + o\left(\frac{x}{\log x}\right).$$

Here is how we can relate this to the two-variable problem. If the original Artin conjecture is true, then a is a primitive root for a positive density of primes, and in particular, b is in the subgroup generated by a for those prime. We would therefore get positive density.

We can therefore suppose that Artin's original conjecture is not true. Suppose that it fails badly, i.e. $N_a(x) = o\left(\frac{x}{\log x}\right)$. Then, we would have

$$M_a(x,z) \coloneqq \#\{p \leq x : i_a(p) \neq 1 \text{ is } z\text{-free}\} = A(a)\pi(x) + o\left(\frac{x}{\log x}\right).$$

Now, we need a way to relate this new piece of information to the two-variable problem somehow. Recall that we have the following description for $N_{a,b}(x)$.

$$N_{a,b}(x) = \sum_{j=1}^{\infty} S_j$$

where S_j is the set of primes p for which $i_a(p) = j$ and $i_b(p)$ is divisible by j, and by an inclusion-exclusion argument again, can be written as

$$S_j = \sum_{d=1}^{\infty} \mu(d)\pi(x, F_{j,d}).$$

Similarly to what we did before, let us look instead at the truncated sum

$$T_j = \sum_{d|P_z} \mu(d)\pi(x, F_{j,d}).$$

Again here, we are sieving out primes p for which $i_a(p) = jm$ with m divisible by some prime less than z, and $i_b(p)$ is divisible by j. Therefore,

$$T_j = \#\{p \leq x : j | i_b(p) \text{ and } i_a(p) = jm \text{ for some } z\text{-free } m\}.$$

Also, summing over all j up to z, we obtain

$$\sum_{j \leq z} T_j = \#\{p \leq x : \text{ the } z\text{-smooth part of } i_a(p) \text{ divides } i_b(p)\}.$$

and so

$$\begin{aligned} N_{a,b}(x) &= \sum_{j \leq z} T_j - \# \left\{ p \leq x : \begin{array}{c} \text{the } z\text{-smooth part of } i_a(p) \text{ divides } i_b(p) \\ \text{and there exists a prime } q > z \text{ dividing } i_a(p) \end{array} \right\} \\ &\geq \sum_{j \leq z} T_j - \# \left\{ p \leq x : q | i_a(p) \text{ for some } q > z \right\}. \end{aligned} \tag{6.2.1}$$

It is unclear at the moment how to relate either of the above quantities to $M_a(x, z)$, and as such this avenue falls short of our expectations.

Additional remarks

We would however like to make a few remarks concerning the hypothesis used in the proof of Theorem 1.5. In his proof, Stephens follows closely Hooley's proof and as such simply uses the Riemann hypothesis generalized to every field extension used in the proof, namely $F_{j,k}$ for every j and k. We want to remark here that since

$$F_{j,k} = \mathbb{Q}\left(\zeta_{jk}, a^{1/jk}, b^{1/j}\right) \supseteq \mathbb{Q}\left(\zeta_{jk}, a^{1/jk}\right) = K_{jk},$$

it might be sufficient to assume the Riemann hypothesis only for those number fields. Indeed, from the above discussion, we can see in equation (6.2.1) that we get a lower bound for $N_{a,b}(x)$, where the part requiring GRH is independent of b. As such, GRH on F_d might be enough to estimate (6.2.1).

Also, by partitioning the set on the right hand side of (6.2.1) between those primes for which $z < q < x^{1/4}$ and those for which $q > x^{1/4}$, it might be possible to only require a weaker hypothesis to estimate these quantities, namely a $\frac{3}{4}$-GRH, i.e. assuming that the related zeta functions have no zeros to the right of $\Re(s) = 3/4$. In the interest of brevity, we will not provide any details and will relegate this analysis to future research.

6.3 The complementary two-variable problem

We remark here that we can get an unconditional result for the "complementary" two-variable problem. This was also remarked by Moree and Stevenhagen in [30] without much explanation, which we provide here.

Statement of the problem

The original two-variable Artin conjecture that was considered throughout this thesis concerns the set

$$S_{a,b} = \{p \text{ prime } : b \bmod p \in \langle a \bmod p \rangle\},$$

that is, those primes p for which $\langle b \bmod p \rangle$ is a subgroup of $\langle a \bmod p \rangle$. Instead here, we will look at the set of primes for which this does not happen. We will show the following theorem, which is unconditional.

Theorem 6.4. *Let a, b be integers for which there is a prime q dividing b with odd order and not dividing a. Then, the set*

$$\tilde{S}_{a,b} = \{p \text{ prime } : b \notin \langle a \bmod p \rangle\}$$

has positive density in the set of all primes. In other words,

$$\#\tilde{S}_{a,b}(x) = \#\{p \leq x \text{ prime } : b \notin \langle a \bmod p \rangle\} \gtrsim \tilde{A}(a,b)\pi(x)$$

for some $\tilde{A}(a,b) > 0$, that is the quantity on the left is asymptotically greater than $\tilde{A}(a,b)\pi(x)$ as x goes to infinity.

Moree and Stevenhagen comment in [30] that this is true without giving a proof. They remark that this was already known to Schinzel [44] through the following result.

Theorem 6.5 (Schinzel)**.** *Given a, b integers, $a > 0$ and $b \neq a^k$ for any k, there exists infinitely many primes p for which the equation*

$$a^x \equiv b \bmod p$$

has no solutions in $x \in \mathbb{Z}$.

By looking at the proof of Schinzel, we see that it is possible to show positive density for these primes, although this remark is not made by Moree and Stevenhagen. We present here a simplified version of Schinzel's argument, obtained by assuming a slightly stronger hypothesis on a and b.

Proof of Theorem 6.4

Let p be a prime for which a is a square $\bmod p$ and b is not a square $\bmod p$. Then, we claim $b \bmod p \notin \langle a \bmod p \rangle$. Indeed, suppose that b was in the subgroup generated by $a \bmod p$, that is $b \equiv a^n \bmod p$ for some $n \geq 1$. Since a is a square modulo p, there is a c for which $a \equiv c^2 \bmod p$. Hence, $b \equiv (c^n)^2 \bmod p$ and would therefore be a square.

Therefore, any prime p for which a is a square modulo p and b is *not* a square modulo p is in $\tilde{S}_{a,b}$. Recall the following notation for the Legendre symbol: Let p be an odd prime and n any integer, define

$$\left(\frac{n}{p}\right) \coloneqq \begin{cases} 1 & \text{if } n \text{ is a square mod } p \text{ and } n \not\equiv 0 \bmod p \\ -1 & \text{if } n \text{ is not a square } \bmod p \\ 0 & \text{if } n \equiv 0 \bmod p. \end{cases}$$

We then show the following lemma which directly yields Theorem 6.4.

Lemma 6.6. *Let a, b be integers for which there is a prime q dividing b with odd order and not dividing a. Then,*

$$\#\left\{p \le x \text{ prime} : \left(\frac{a}{p}\right) = 1 \text{ and } \left(\frac{b}{p}\right) = -1\right\} \gtrsim \frac{\pi(x)}{2^{\omega(ab)}}.$$

Proof. Let q be a prime dividing b with order t (odd) but not dividing a. Let r be the product of the primes dividing a and b except for q, i.e. $r := ab/(b, q)$. Let p be a prime for which q is a non-quadratic residue (mod p), and all the primes ℓ dividing r are a quadratic residues (mod p), that is,

$$\left(\frac{q}{p}\right) = -1 \qquad \text{and} \qquad \left(\frac{\ell}{p}\right) = 1 \text{ for all } \ell | r. \tag{6.3.1}$$

Since the Legendre symbol is completely multiplicative in its top argument, we get

$$\left(\frac{a}{p}\right) = \prod_{\ell | a} \left(\frac{\ell}{p}\right)^{\mathrm{ord}_\ell(a)} = 1$$

and

$$\left(\frac{b}{p}\right) = \left(\frac{q}{p}\right)^t \prod_{\substack{\ell | b \\ \ell \neq q}} \left(\frac{\ell}{p}\right)^{\mathrm{ord}_\ell(b)} = -1.$$

Therefore, any such prime would be in our set of interest. We will count those primes.

For any prime p, define

$$D(p) = \frac{1}{2^{\omega(ab)}} \left[1 - \left(\frac{q}{p}\right)\right] \prod_{\ell | r} \left[1 + \left(\frac{\ell}{p}\right)\right].$$

The factor $1-\left(\frac{q}{p}\right)$ will take value 2 when q is a non-residue modulo p, and 0 otherwise. Each factor $1+\left(\frac{\ell}{p}\right)$ will take value 2 when ℓ is a quadratic residue modulo p, and 0 otherwise. Therefore, for primes p coprime to ab, $D(p)$ will be 1 if and only if condition (6.3.1) is satisfied, and 0 otherwise. We then consider

$$M(x) = \sum_{\substack{p\leq x \\ (p,ab)=1}} D(p).$$

$M(x)$ will count exactly the number of primes up to x satisfying condition (6.3.1). Expanding the product in $D(p)$ and using multiplicativity of the Legendre symbol, we get

$$\begin{aligned} D(p) &= \frac{1}{2^{\omega(ab)}}\left[1-\left(\frac{q}{p}\right)\right]\left[1+\sum_{d|\operatorname{rad}(r)}\left(\frac{d}{p}\right)\right] \\ &= \frac{1}{2^{\omega(ab)}}\left[1+\sum_{d|\operatorname{rad}(r)}\left(\frac{d}{p}\right)-\sum_{d|\operatorname{rad}(r)}\left(\frac{qd}{p}\right)-\left(\frac{q}{p}\right)\right] \\ &= \frac{1}{2^{\omega(ab)}}\left[1+\sum_{\substack{d|\operatorname{rad}(ab) \\ d\neq 1}}\epsilon_d\left(\frac{d}{p}\right)\right] \end{aligned}$$

where

$$\epsilon_d := \begin{cases} -1 & \text{if } q|d \\ 1 & \text{otherwise.} \end{cases}$$

Therefore, $M(x)$ becomes

$$M(x) = \frac{\pi(x)}{2^{\omega(ab)}} + \sum_{\substack{d|\operatorname{rad}(ab) \\ d\neq 1}}\epsilon_d \sum_{\substack{p\leq x \\ (p,ab)=1}}\left(\frac{d}{p}\right).$$

By the Prime Number Theorem for arithmetic progressions (See [37]), we know that

$$\sum_{\substack{p\leq x\\(p,ab)=1}} \left(\frac{d}{p}\right) = o\left(\pi(x)\right)$$

whenever $\left(\frac{d}{p}\right)$ is not a trivial character. Since every divisor d is square-free, and since we sum over a finite number of divisors d, we obtain

$$M(x) = \frac{\pi(x)}{2^{\omega(ab)}} + o\left(\pi(x)\right).$$

This conclude the proof of the lemma. □

The uncomparable two-variable problem

We considered the set of primes p for which $\langle b \bmod p\rangle \subseteq \langle a \bmod p\rangle$ as well as the set of prime for which this does not happen. Note that there are three possibilities of inclusions of those two subgroups. Either $\langle b \bmod p\rangle \subseteq \langle a \bmod p\rangle$, $\langle b \bmod p\rangle \supset \langle a \bmod p\rangle$ or neither is a subgroup of the other, in which case we will call a and b uncomparable modulo p. We can ask the question: does the set

$$\hat{S}_{a,b} = \{p \text{ prime } : a \text{ and } b \text{ are uncomparable}\rangle\}$$

have positive density in the set of all primes?

To adopt a method similar to what we have above, we first need to study the related set

$$\check{S}_{a,b} = \{p \text{ prime } : \langle b \bmod p\rangle = \langle a \bmod p\rangle\rangle\}.$$

Then, if the above set has density $\check{A}(a,b)$, the density $\hat{A}(a,b)$ of $\hat{S}_{a,b}$ becomes

$$\hat{A}(a,b) = 1 - A(a,b) - A(b,a) + \check{A}(a,b).$$

The problem of finding a density for $\check{S}_{a,b}$ unconditionally appears somewhat harder than for $\tilde{S}_{a,b}$, and as such we relegate this problem to future research.

6.4 Concluding remarks

There are still many unanswered questions about the two-variable Artin conjecture. In particular, since this problem seems easier than the original conjecture in some respect, it might be possible to show positive density unconditionally. If this is still not accessible, we can ask if a weakened version of the generalized Riemann hypothesis is sufficient.

Alternatively, Theorem 2.9 suggests that it might be possible to get positive density unconditionally for sets of this nature.

In the case of the elliptic two-variable Artin conjecture, even a conjectural density is yet to be determined. Our unconditional lower bound in Theorem 4.2 needs also to be extended to elliptic curves of higher rank.

It is possible that some generalized theory of binary recurrence sequences might help understand the elliptic setting for this problem. This is an approach that will require careful analysis, and that we intend to do in future research.

Bibliography

[1] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)*, 181(1):191–242, 2015.

[2] E. Bombieri, J. B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli. *Acta Math.*, 156(3-4):203–251, 1986.

[3] E. Bombieri, J.B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli II. *Math. Ann.*, 277:361–393, 1987.

[4] E. Bombieri and W.M. Schmidt. On Thue's equation. *Invent. Math.*, 88:69–81, 1987.

[5] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Annals of Math.*, 15(2):30–70, 1913.

[6] David A. Clark and M. Ram Murty. The Euclidean algorithm for Galois extensions of $\mathbb{Q}$. *J. Reine Angew. Math.*, 459:151–162, 1995.

[7] N. D. Elkies. $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, etc. NMBRTHRY Listserv, May 2006. `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;99f4e7cd.0605`; accessed 13-June-2018.

[8] Paul Erdős. Some recent advances and current problems in number theory. In *Lectures on Modern Mathematics*, volume III, pages 196–244. Wiley, New York, 1965.

[9] Paul Erdős. On the sum $\sum_{d|2^n-1} d^{-1}$. *Israel J. Math.*, 9:43–48, 1971.

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

[11] E. Fouvry and H. and Iwaniec. Primes in arithmetic progressions. *Acta Arith.*, 42(2):197–218, 1983.

[12] Étienne Fouvry. Autour du théorème de Bombieri-Vinogradov. *Acta Math.*, 152(3-4):219–244, 1984.

[13] A. O. Gelfond. *Selected Works*. Nauka, 1973. [in Russian].

[14] R. Gupta and M. Ram Murty. A remark on Artin's conjecture. *Invent. Math.*, 78:127–130, 1984.

[15] R. Gupta and M. Ram Murty. Primitive points on elliptic curves. *Compositio Mathematica*, 58(1):13–44, 1986.

[16] R. Gupta and M. Ram Murty. Cyclicity and generation of points mod p on elliptic curves. *Invent. Math.*, 101:225–235, 1990.

[17] Rajiv Gupta, M. Ram Murty, and V. Kumar Murty. The Euclidean algorithm for S-integers. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 189–201. Amer. Math. Soc., Providence, RI, 1987.

[18] G. H. Hardy and S. Ramanujan. The normal number of prime factors of a number n [Quart. J. Math. **48** (1917), 76–92]. In *Collected papers of Srinivasa Ramanujan*, pages 262–275. AMS Chelsea Publ., Providence, RI, 2000.

[19] Malcolm Harper. $\mathbb{Z}[\sqrt{14}]$ is Euclidean. *Canad. J. Math.*, 56(1):55–70, 2004.

[20] Malcolm Harper and M. Ram Murty. Euclidean rings of algebraic integers. *Canad. J. Math.*, 56(1):71–76, 2004.

[21] H. Hasse. *Vorlesungen über Zahlentheorie*. Akademie-Verlag, 1964.

[22] D. R. Heath-Brown. Artin's conjecture for primitive roots. *The Quarterly Journal of Mathematics*, 37(1):27–38, 1986.

[23] M. Hindry and J. H. Silverman. *Diophantine Geometry: An introduction*. Number 201 in GTM. Springer-Verlag, 2000.

[24] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[25] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Am. Math. Soc.*, 83:289–292, 1977.

[26] J. Lee and M. Ram Murty. An application of Mumford's gap principle. *Journal of Number Theory*, 105:333–343, 2004.

[27] D.H. Lehmer and E. Lehmer. Heuristics, anyone? In *Studies in Mathematical Analysis and Related Topics*, pages 385–416. Standford Univ. Press, Standford, California, 1962.

[28] K. Mahler. Eine arithmetische eigenschaft der rekurrierenden reihen. *Mathematica(Leiden)*, 3:153–156, 1934–1935.

[29] P. Moree. Artin's primitive root conjecture - a survey. *Integers*, 12(6):1305–1416, 2012.

[30] P. Moree and P. Stevenhagen. A two-variable Artin conjecture. *Journal of Number Theory*, 85:291–304, 2000.

[31] D. Mumford. A remark on Mordell's conjecture. *American Journal of Mathematics*, 87(4):1007–1016, 1965.

[32] Leo Murata and Carl Pomerance. On the largest prime factor of a Mersenne number. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 209–218. Amer. Math. Soc., Providence, RI, 2004.

[33] M. R. Murty and Kathleen L. Petersen. The Euclidean algorithm for number fields and primitive roots. *Proc. Amer. Math. Soc.*, 141(1):181–190, 2013.

[34] M. Ram Murty. On Artin's conjecture. *Journal of Number Theory*, 16:147–168, 1983.

[35] M. Ram Murty. On the supersingular reduction of elliptic curves. *Proc. Indian Acad. Sci. (Math. Sci.)*, 97(1–3):247–250, 1987.

[36] M. Ram Murty. Artin's conjecture for primitive roots. *Math. Intelligencer*, 10(4):59–67, 1988.

[37] M. Ram Murty. *Problems in Analytic Number Theory*. Springer, second edition edition, 2008.

[38] M. Ram Murty, Michael Rosen, and Joseph H. Silverman. Variations on a theme of Romanoff. *International Journal of Mathematics*, 7(3):373–391, 1996.

[39] Ram Murty, François Séguin, and Cameron L. Stewart. A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences. *Submitted*, 2017.

[40] Ram Murty and Siman Wong. The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences. In *Number theory for the millennium, III (Urbana, IL, 2000)*, pages 43–54. A K Peters, Natick, MA, 2002.

[41] G. Pólya. Arithmetische eigenschaften der reihenentwicklungen rationaler funktionen. *J. Reine Angew. Math.*, 151:1–31, 1921.

[42] S. Ramanujan. Highly composite numbers. *Proc. London Math. Soc.*, 2(XIV):347–409, 1915.

[43] Karl Rubin and Alice Silverberg. Ranks of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 39(4):455–474, 2002.

[44] A. Schinzel. On the congruence $a^x \equiv b \pmod{p}$. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, 8:307–309, 1960.

[45] J.-P. Serre. Résumé des cours de 1977–1978. *Annuaire du Collège de France*, pages 67–70, 1978.

[46] I. E. Shparlinski. Prime divisors of recurrence sequences. *Izv. Vyssh. Uchebn. Zaved.*, 4:100–103, 1980.

[47] I. E. Shparlinski. Number of different prime divisors of recurrence sequences. *Mat. Zametki*, 42:494–507, 1987.

[48] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 2nd ed. edition, 1986.

[49] J. H. Silverman. Wieferich's criterion and the abc-conjecture. *Journal of Number Theory*, 30:226–237, 1988.

[50] J. H. Silverman and J. Tate. *Rational points on elliptic curves*. UTM. Springer, New York, 1992.

[51] P.J. Stephens. Prime divisors of second order linear recurrences. *Journal of Number Theory*, 8:313–332, 1976.

[52] Cameron L. Stewart. On divisors of Lucas and Lehmer numbers. *Acta Math.*, 211(2):291–314, 2013.

[53] C.L. Stewart. The greatest prime factor of $a^n - b^n$. *Acta Arith.*, 26:427–433, 1975.

[54] C.L. Stewart. On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. *Proc. London Math. Soc.*, 35:425–447, 1977.

[55] C.L. Stewart. On divisors of terms of linear recurrence sequences. *J. Reine Angew. Math.*, 333:12–31, 1982.

[56] C.L. Stewart. On prime factors of terms of linear recurrence sequences. In J.M.Borwein et al., editor, *Number Theory and Related Fields: In memory of Alf van der Poorten*, volume 43 of *Springer Proceedings in Mathematics and Statistics*, pages 341–359. Springer, 2013.

[57] R. Thangadurai and A. Vatwani. The least prime congruent of one modulo n. *The American Mathematical Monthly*, 118(8):737–742, 2011.

[58] M. Ward. Prime divisors of second-order recurring sequences. *Duke Math. J.*, 21:607–614, 1954.

[59] Peter J. Weinberger. On Euclidean rings of algebraic integers. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St.*

Louis Univ., St. Louis, Mo., 1972), pages 321–332. Amer. Math. Soc., Providence, R. I., 1973.

[60] A. E. Western and J. C. P. Miller. *Tables of indices and primitive roots*. Royal Society Mathematical Tables, Vol. 9. Published for the Royal Society at the Cambridge University Press, London, 1968.

[61] Horst G. Zimmer. A limit formula for the canonical height of an elliptic curve and its application to height computations. In *Number theory (Banff, AB, 1988)*, pages 641–659. de Gruyter, Berlin, 1990.