Dynamical systems and infinite sequences of coprime integers

Max van Spengler
3935892

Supervisor: Damaris Schindler

Universiteit Utrecht

Departement Wiskunde
Universiteit Utrecht
Nederland
31-05-2018

Contents

1 Introduction

Since the Hellenistic period, prime numbers and their properties have been a fundamental object of interest in mathematics [MB11]. The defining property of such a number is that it is only divisible by 1 and itself. Their counterparts are the composite numbers. These are numbers defined as being divisible by at least one number other than 1 or themselves. One of the earliest results obtained from research into these numbers is now known as the fundamental theorem of arithmetic.

Fundamental theorem of arithmetic. *Every natural number > 1 is either prime or can be written, up to the order of factors, as a unique product of primes.*

Proof. We will give a proof by induction. First, note that 2 and 3 are prime. Now assume the theorem to be true for all numbers between 1 and $n+1$ for some $n \in \mathbb{N}$, so each number in between can be written as a unique product of primes. Either $n+1$ is prime, in which case the proof is finished or $n+1$ is composite. In that case $n+1$ can be written as ab, where $1 < a \leq b < n+1$, so the theorem is true for the numbers a and b. Let $\prod_{i=1}^{k} p_i^{c_i}$ and $\prod_{j=1}^{l} q_j^{d_j}$ be the prime representations of a and b, respectively. Then $n+1 = \prod_{i=1}^{k} p_i^{c_i} * \prod_{j=1}^{l} q_j^{d_j}$, proving that $n+1$ has a prime representation as well. Thus, it follows by induction that every natural number is either prime or can be written as a product of primes.

It remains to show that this representation is unique. Suppose an integer m has the prime representations $\prod_{i=1}^{k} p_i$ and $\prod_{j=1}^{l} q_j$ where p_i and q_j are not neccesarily unique for every i and j. Using the properties of divisibility, $p_1 | \prod_{j=1}^{l} q_j$ and therefore $p_1 | q_j$ for some j. The prime representations can be ordered such that $p_1 | q_1$. Note that q_1 is prime and therefore $p_1 = q_1$. Dividing both prime representations by p_1 gives $\prod_{i=2}^{k} p_i$ and $\prod_{j=2}^{l} q_j$. Repeating this process until both representations are exhausted reveals they are made up of the same primes. If one of the representations is exhausted before the other, then that representation is smaller than the other, which would imply that $m \neq m$. Therefore the representations must be equal and, hence, a prime representation is unique up to the order of the factors. □

The fundamental theorem of arithmetic can be used to define the greatest common divisor (gcd) and the least common multiple (lcm).

Definition 1.1 (Greatest common divisor and least common multiple)**.** *Let $a, b \in \mathbb{Z}$ with prime representations $\prod_{i=1}^{n} p_i^{k_i}$ and $\prod_{i=1}^{n} p_i^{l_i}$, where the p_i are unique primes and where $k_i, l_i \geq 0$ for every i. Then* $\gcd(a,b) := \prod_{i=1}^{n} p_i^{min(k_i,l_i)}$ *and* $\operatorname{lcm}(a,b) := \prod_{i=1}^{n} p_i^{max(k_i,l_i)}$.

One of the first questions that arose from the research on prime numbers, was on the cardinality of the set of these numbers, which led to the following theorem.

The infinitude of primes. *There are infinitely many prime numbers.*

The proof given below is the oldest surviving proof of this theorem, found in Euclid's Elements [Beu15].

Proof. Assume there is a finite number of primes. Then we can define a set $P = \{p_1, p_2, ..., p_n\}$, where n is the number of primes, containing every prime number. Let $p_{n+1} = \prod_{i=1}^{n} p_i + 1$, then $\gcd(p_{n+1}, p_i)|1$ for every $1 \leq i \leq n$ and therefore $\gcd(p_{n+1}, p_i) = 1$. This implies that none of the elements of P is a part of the prime representation of p_{n+1}. Thus p_{n+1} is prime itself or it has a prime representation containing numbers outside of P. This contradicts our assumption that P was the set of all prime numbers, which proves the infinitude of primes. □

This is however not the only known proof of the infinitude of primes. In fact, mathematicians have come up with a large number of proofs of this theorem using many different techniques. A few well known proofs are Goldbach's proof [AZ10], Erdős's proof [AZ10] and Furstenberg's proof [Fu55]. These are shown in the subsections below.

Chapter 2 will provide some background for Chapter 3 and Chapter 4. In Chapter 3, a number of results obtained by Andrew Granville [Gr17] will be presented. These results provide methods for finding infinite sequences of coprimes using dynamical systems and polynomials with integer coefficients. When the sequence of integers, obtained by repeatedly applying such a polynomial to 0, contains an infinite number of distinct elements, Granville's method fails. However, with his last result, he shows that in these cases, the existence of infinite sequences of distinct coprimes can still be proven. This last result depends on the validity of the abc-conjecture.

In Chapter 4 we will expand upon this last result, giving a proof using weaker assumptions. Moreover, a minimal assumption regarding the weak abc-conjecture will be determined and interpreted. The strongest bound proven at the time of writing, related to the abc-conjecture, will be applied in order to determine whether it is sufficient for proving the result as well. We shall see that this bound is sufficiently strong for proving the result for certain polynomials.

1.1 Goldbach's proof

In 1730, Christian Goldbach gave a proof of the infinitude of primes in a letter written to Leonhard Euler. He used the properties of the Fermat numbers in a fashion slightly similar to Euclid's proof. These numbers are defined as follows.

$$F_n := 2^{2^n} + 1,$$

Where n is a non-negative integer. We can use this definition to derive two properties of the Fermat numbers. First, note that

$$F_{n+1} = 2^{2^{n+1}} + 1 = (2^{2^n})^2 + 1 = (F_n - 1)^2 + 1. \tag{1}$$

We can use this identity to show that $F_n = F_0 \cdots F_{n-1} + 2$ with a proof by induction. Note that $F_1 = F_0 + 2 = 5$. Now, assume that $F_n = F_0 \cdots F_{n-1} + 2$ holds for some $n \geq 1$. Then, using equation 1, $F_{n+1} = (F_n - 1)^2 + 1$. Applying our assumption yields

$$\begin{aligned} F_{n+1} &= (F_0 \cdots F_{n-1} + 1)^2 + 1 \\ &= (F_0 \cdots F_{n-1})^2 + 2F_0 \cdots F_{n-1} + 2 \\ &= F_0 \cdots F_{n-1}(F_0 \cdots F_{n-1} + 2) + 2 \\ &= F_0 \cdots F_n + 2, \end{aligned}$$

which proves the property. This is the important property which Goldbach used in his proof of the infinitude of primes as shown below.

Goldbach's proof. Note that the Fermat numbers form an infinite sequence of distinct integers. It follows from the identity $F_n = F_0 \cdots F_{n-1} + 2$ that $\gcd(F_n, F_m) \leq 2$ for every $0 \leq m < n$. Furthermore, the definition of the Fermat numbers implies that they are all odd and, therefore, $\gcd(F_n, F_m) = 1$. From the definition of the greatest common divisor as given above, it follows that the prime representations of the Fermat numbers never share a prime factor. This in combination with the fact that the Fermat numbers are an infinite sequence of distinct integers and with the fundamental theorem of arithmetic proves that there are infinitely many prime numbers. □

1.2 Erdős' proof

Before giving Erdős' proof, the following definitions and a simple lemma should be introduced. The function $\pi(N)$ is defined as the cardinality of the set of prime numbers smaller than or equal to $N \in \mathbb{N}$.

Definition 1.2 (Square-free number)**.** *Let $r \in \mathbb{Z}$ with prime representation $\prod_{i=1}^{n} p_i^{k_i}$, where $k_i \geq 1$. If $k_i = 1$ for every $i \in \{1, \ldots, n\}$, then r is called square-free.*

Lemma 1.3. *Every integer n can be written as a product rs^2, where r is a square-free number and s is an integer.*

Proof. Given an integer n, let s be the largest integer, such that s^2 is contained in the prime representation of n. If $r = n/s^2$ is not square-free and if the prime representation of r is $\prod_{i=1}^{k} p_i^{a_i}$, then there is at least one $j \in \{1, \ldots, k\}$ such that a_j is greater than 1. However, in that case $(sp_j)^2$ is also contained in n, contradicting our assumption that s is the largest integer such that its square is contained in n. Therefore, r has to be square-free, proving the lemma. □

Erdős' proof. Suppose N is an integer greater than 1. Using Lemma 1.3, we can represent the set of integers from 1 to N as $\{r_1 s_1^2, \ldots, r_N s_N^2\}$ where r_i is a square-free number for every i. In this representation, r_i could be any square-free number smaller than or equal to N. Using the definition of square-free

numbers, we can determine an upper-bound for the number of possible square-free numbers smaller than N. Any such number must be a product of primes smaller than N. The number of possible products of such primes is given by $2^{\pi(N)}$. Any square s_i^2 contained in the set above, must be smaller than N as well, therefore $1 \leq s_i \leq \lfloor\sqrt{N}\rfloor$. Now the total amount of possible combinations r_i and s_i, such that $r_i s_i^2 \leq N$, is

$$2^{\pi(N)}\lfloor\sqrt{N}\rfloor \geq |\{r_1 s_1^2, \ldots, r_N s_N^2\}| = N,$$

where $|.|$ is the number of elements in the set. By noting that $\sqrt{N} \geq \lfloor\sqrt{N}\rfloor$ and dividing by $\sqrt{N}$, we get

$$2^{\pi(N)} \geq \sqrt{N}.$$

Taking the logarithm yields

$$\pi(N) \geq \frac{\log(N)}{\log 4}.$$

The right hand side of this inequality goes to infinity as N tends to infinity. Therefore the number of primes must be infinite as well. □

What is remarkable about this proof, besides being an elegant proof of the infinitude of primes, is that it provides a lower bound for the function $\pi(N)$, namely $\log(N)/\log(4)$. Therefore, it reveals something about the density of the primes within the collection of positive integers up to some positive integer N. However, the prime number theorem, proven independently by Jacques Hadamard [Ha96] and Charles Jean de la Vallée Poussin [Va96] in 1896, shows that the asymptotic distribution of $\pi(N)$ is $N/\log(N)$. This term grows considerably faster than the aforementioned lower bound. Therefore, for large N, this lower bound will generally be very weak.

1.3 Furstenberg's proof

Furstenberg gave a topological proof of the infinitude of primes. In order to present this proof, some topological definitions and notation should be introduced.

Definition 1.4 (Arithmetic progression)**.** *A collection $S(a, b) = \{an+b \,|\, n \in \mathbb{Z}\}$ where a, $b \in \mathbb{Z}$ and $a \neq 0$ is called an arithmetic progression.*

Definition 1.5 (Union and intersection)**.** *Given two sets V, W, their union is defined as*

$$V \cup W := \{x \,|\, x \in V \vee x \in W\},$$

and their intersection as

$$V \cap W := \{x \,|\, x \in V \wedge x \in W\}.$$

Definition 1.6 (Complement)**.** *Given a set X and a set $U \subset X$, the complement of U in X is defined as*

$$X \backslash U := \{x \in X \mid x \notin U\}.$$

Definition 1.7 (Topology)**.** *Given an arbitrary set X, a topology τ is a collection of subsets of X satisfying the following axioms.*

1. *The set containing no elements, called the empty set $\emptyset$, and the entire set X are elements of τ.*
2. *Any finite or infinite union of elements in τ belongs to τ as well.*
3. *The intersection of any finite number of elements of τ belongs to τ as well.*

Definition 1.8 (Topological space)**.** *A space X endowed with a topology τ is called a topological space (X, τ).*

Definition 1.9 (Open and closed sets)**.** *Given a topological space (X, τ), a subset $U \subset X$ is called an open set if $U \in \tau$. The complement of an open set in X is called closed.*

Besides these definitions, Furstenberg used a well known lemma regarding the union of closed sets.

Lemma 1.10. *Given a topological space (X, τ), the union of finitely many closed sets of (X, τ) is closed as well.*

Proof. Let $\bigcup_{i=1}^{n} U_i$ be a union of $n \in \mathbb{N}_{>0}$ closed sets in a topological space (X, τ). Let x be an arbitrary element of the complement of this union, then $x \notin U_i$ for every U_i. This implies $x \in X \backslash U_i$ for every U_i and thus that $x \in \bigcap_{i=1}^{n} (X \backslash U_i)$. On the other hand, if x is an arbitrary element of $\bigcap_{i=1}^{n} (X \backslash U_i)$, then $x \in X \backslash U_i$ for every U_i. Therefore $x \notin U_i$ for every U_i from which it follows that $x \notin \bigcup_{i=1}^{n} U_i$ and thus $x \in X \backslash \bigcup_{i=1}^{n} U_i$. So $X \backslash \bigcup_{i=1}^{n} U_i = \bigcap_{i=1}^{n} (X \backslash U_i)$. Since every U_i is closed, $X \backslash U_i$ is open, so the right hand side of this equation is a finite intersection of open sets, which is itself open because of property 3 of topologies as defined above. Therefore the complement of $\bigcup_{i=1}^{n} U_i$ is an open set, which implies that $\bigcup_{i=1}^{n} U_i$ is closed.

□

Furstenberg's proof. Let τ be the collection of the empty set $\emptyset$ and unions of arithmetic progressions. We can show that τ defines a topology on $\mathbb{Z}$.

First note that $S(1, 0) = \mathbb{Z}$ and thus that $\emptyset, \mathbb{Z} \in \tau$. So τ satisfies the first property of topologies. Next, take a union of, not necessarily finitely many, elements U of τ. If x is an element of this union, then there exists an arithmetic progression $S(a, x) \subset U$ for some a and for some U. Therefore $S(a, x) \subset \bigcup U$, which shows that any element of the union is contained in an arithmetic progression contained in the union as well. This proofs that this union is an element of τ and thus that τ satisfies the second property of topologies. Lastly,

take an intersection of two sets $U, V \in \tau$. If x is an element of this intersection, then there exist a_U and a_V such that $S(a_U, x) \in U$ and $S(a_V, x) \in V$. Note that for every $n \in \mathbb{Z}$, $n \operatorname{lcm}(a_U, a_V) + x = nba_U + x = nca_V + x$ for some $b, c \in \mathbb{Z}$. Therefore $S(\operatorname{lcm}(a_U, a_V), x)$ is contained in the intersection. This proves that for every x in the intersection, there exists an arithmetic progression, containing x, which is itself contained in the intersection. So τ also satisfies the third property of topologies and $(\mathbb{Z}, \tau)$ is a topological space.

The following two properties of this topological space can be used to prove the infinitude of primes.

1. Any non-empty finite subset of $\mathbb{Z}$ cannot be open, because arithmetic progressions are infinite. Therefore the complement of a finite set cannot be closed.

2. Arithmetic progressions are open and closed sets, because the complement of an arithmetic progression is $\bigcup_{i=1}^{a-1} S(a, b+i)$, which is an open set.

The fundamental theorem of arithmetic tells us that any number greater than 1 or smaller than -1 can be written as a product of primes. Therefore, the union $\bigcup_{p\,prime} S(p, 0)$ contains every number except for the numbers -1 and 1, so we can write

$$\mathbb{Z}\backslash\{-1, 1\} = \bigcup_{p\,prime} S(p, 0).$$

Note that the left-hand side of this equation is the complement of a finite set. Property one of this topological space implies that this set cannot be closed. Because of property two, the right-hand side is a union of closed sets. If this were a finite union, than it would be closed as a result of Lemma 1.10, which would contradict property one. Therefore the number of primes must be infinite. □

2 Theoretical background

This chapter will provide the theory required for proving the results provided in Chapters 3 and 4. The theory consists of number theory, dynamical systems theory and some additional theorems from various research areas.

2.1 Number theory

Besides the definitions provided in the previous chapter, some additional definitions and results from the field of number theory will be used in the next chapters. These definitions and results will be provided here. The first important definition is that of coprime integers.

Definition 2.1 (Coprime integers)**.** *Two integers $a, b \in \mathbb{Z}$ are coprime if* $\gcd(a, b) = 1$.

Note that this implies that two integers are coprime exactly when their prime representations share no prime factors. When sequences of integers are not pairwise coprime, we can use the following two definitions to recognize some important differences in their prime representations.

Definition 2.2 (Private prime factors)**.** *Given a sequence of integers $a_0, a_1, \ldots$, a prime factor p_i of a_i is called a private prime factor of a_i if $p_i \nmid a_j$ whenever $i \neq j$.*

Definition 2.3 (Primitive prime factors)**.** *Given a sequence of integers $a_0, a_1, \ldots$, a prime factor p_n of a_n is called a primitive prime factor of a_n if $p_n \nmid a_m$ for all $0 \leq m \leq n-1$*

Given an infinite sequence of integers, where every element contains a private or primitive prime factor. The sequence of these prime factors forms an infinite sequence of distinct primes. Therefore, these definitions can be used to construct infinite sequences of distinct primes as shown in the following lemma regarding coprime sequences presented by Granville [Gr17].

Lemma 2.4. *Suppose that $a_0, a_1, \ldots$ is an infinite sequence of distinct, pairwise coprime integers. Let $p_0, p_1, \ldots$ be an infinite sequence such that p_i is a prime divisor of a_i for every i, then this sequence is an infinite sequence of distinct primes.*

Proof. Let $a_0, a_1, \ldots$ be an infinite sequence of distinct, pairwise coprime integers. Then the greatest common divisor between any two elements of this sequence is 1. Suppose we take a sequence $p_0, p_1, \ldots$ where p_i is a prime factor of a_i for every i. Then if $p_i | a_j$ for $i \neq j$, then $p_i | \gcd(a_i, a_j) = 1$ and thus $p_i = 1$, contradicting our assumption that p_i is prime. Therefore $p_i \nmid a_j$ whenever $i \neq j$, which implies that p_i is a private prime factor of a_i for every i. So $p_0, p_1, \ldots$ is an infinite sequence of distinct primes.

□

The following lemma is provided by Granville, but without a proof [Gr17]. It will be used extensively in Chapter 3 and Chapter 4.

Lemma 2.5. *Let $f(x)$ be a polynomial with integer coefficients $a_0, ..., a_k \in \mathbb{Z}$, such that $f(x) = a_k x^k + ... + a_0$. For any $b, c \in \mathbb{Z}$, $b - c$ divides $f(b) - f(c)$ and if $b \equiv c \pmod{m}$ for an integer m, then $f(b) \equiv f(c) \pmod{m}$.*

Proof. In order to proof that $(b-c) | (f(b) - f(c))$, we have to show that $f(b) - f(c) = d(b-c)$ for some integer d. Note that

$$f(b) - f(c) = \sum_{i=1}^{k} a_i (b^i - c^i).$$

We can write

$$b^n - c^n = (b-c) \sum_{i=1}^{n} b^{n-i} c^{i-1}$$

thereby showing that $(b-c)|(b^n-c^n)$ for every $n \geq 1$. Let d_i be the integer such that $d_i(b-c) = b^i - c^i$, then

$$f(b) - f(c) = \sum_{i=1}^{k} a_i d_i (b-c) = (b-c) \sum_{i=1}^{k} a_i d_i,$$

which proves that $(b-c)|(f(b)-f(c))$.

Now suppose that $b \equiv c \pmod{m}$ for some integer m. Then we can write $b = dm+c$ for some integer d. Substituting this into $f(b)$ gives $a_k(dm+c)^k + ... + a_0$. The only term in $(dm+c)^k$ not explicitly containing m is c^k, so

$$f(b) \equiv a_k c^k + ... + a_0 \pmod{m}$$

which proves that $f(b) \equiv f(c) \pmod{m}$. □

The next definition will be used in one of the most famous conjectures of number theory.

Definition 2.6 (Radical of an integer)**.** *Let a be an integer with prime representation $\prod_{i=1}^{n} p_i^{k_i}$ where $k_i \geq 1$ for every i and $p_i \neq p_j$ when $i \neq j$. The radical of a is defined as the product of each distinct prime in the prime representation of a, i.e.*

$$\mathrm{Rad}(a) = \prod_{i=1}^{n} p_i.$$

Note that the radical of an integer is always the largest square-free number contained in that integer. The next conjecture was proposed by David Masser and Joseph Oesterlé [Oe88] in 1985 and in 1988, respectively, and has not yet been proven.

The abc-conjecture. *For every $\epsilon > 0$, there exists a constant k_ϵ, such that for every pair of positive coprime integers a and b with $a+b=c$,*

$$c \leq k_\epsilon \, \mathrm{Rad}(abc)^{1+\epsilon}.$$

A related conjecture, which requires a weaker assumption is the weak abc-conjecture.

The weak abc-conjecture. *There exists $\gamma > 0$ such that, for every pair of positive coprime integers a and b with $a+b=c$, the following inequality holds:*

$$c < \mathrm{Rad}(abc)^{1+\gamma}.$$

Neither the abc-conjecture, nor the weak abc-conjecture has been proven. However, an exponential version of the abc-conjecture has been proven by Stewart and Yu in 2001 [SY01].

Theorem 2.7 (Stewart, Yu, 2001)**.** *There exists an effectively computable positive number k, such that, for all positive integers a, b, and c with $a+b=c$ and* $\gcd(a,b,c) = 1$,

$$c < \exp(k \, \mathrm{Rad}(abc)^{\frac{1}{3}} \log(\mathrm{Rad}(abc))^3).$$

2.2 Dynamical systems

This subsection will provide two definitions from dynamical systems theory. These will be used in Chapter 3 for the simplification of the theorems and proofs presented there.

Definition 2.8 (orbit)**.** *Given a map $f(x) \in \mathbb{Z}[x]$ and an integer x_0. The sequence $(x_n)_{n\geq 0}$, where $x_{n+1} = f(x_n)$ is called to orbit of x_0 under the map f.*

Consider the Fermat numbers for instance. If we let $f(x) = (x-1)^2+1$, then equation (1) from Subsection 1.1 can be written as $F_{n+1} = f(F_n)$. Let $x_0 = F_1 = 3$, then the orbit of x_0 under f is exactly the sequence of Fermat numbers. This example shows how orbits can be used to give a clear representation of integer sequences.

Definition 2.9 (periodicity of orbits)**.** *The orbit of x_0 under the map f is called periodic if there exists $n \geq 1$ such that $f^n(x_0) = x_0$, preperiodic if there exists $m \geq 0$ such that x_m is periodic under f and strictly preperiodic if $m \geq 1$. The n and m are called the period and the preperiod of x_0, respectively. If an orbit is not preperiodic, then it is wandering.*

Note that only wandering orbits are infinite sequences of distinct elements. Therefore, only wandering orbits can be used for the construction of infinite sequences of primes, as will be shown in Chapter 3.

2.3 Additional theory

This subsection contains a number of definitions, lemma's and theorems from multiple fields, often connected to algebraic geometry and number theory. They lead to a consequence of the abc-conjecture and a somewhat equivalent consequence of the weak abc-conjecture. These consequences will be used in Chapters 3 and 4. The first theorem is the Riemann-Hurwitz formula, presented without a proof. The definition of $mult_p(F)$ can be found in [Ba07].

The Riemann-Hurwitz formula. *Let $F : X \to Y$ be a nonconstant holomorphic map between compact Riemann surfaces. Then*

$$2g(X) - 2 = deg(F)(2g(Y) - 2) + \sum_{p\in X}[mult_p(F) - 1],$$

where g is the genus of the surface.

A proof of this theorem is provided in the original article by Hurwitz [Hu92] (for an English variant, see [Mi95] for instance). As an example, consider $\phi(z) \in \mathbb{C}[z]$ with $\phi(z) = z^2$ over the set $\mathbb{C} \cup \{\infty\}$. This function is ramified only at 0 and ∞, with $mult_0(\phi) = mult_\infty(\phi) = 2$ and the function has degree 2. This set is the Riemann sphere, which has genus zero. Suppose we did not know the genus of this set, then we could apply the Riemann-Hurwitz formula as follows:

$$2g(\mathbb{C} \cup \{\infty\}) - 2 = 2(2g(\mathbb{C} \cup \{\infty\}) - 2) + (2 - 1) + (2 - 1).$$

Through solving this equation, we obtain

$$g(\mathbb{C} \cup \{\infty\}) = 0.$$

The following lemma is a special case of the Riemann-Hurwitz formula. When dealing with the complex projective space $\mathbb{P}^1(\mathbb{C})$, we will think of it as the Riemann sphere $\mathbb{C} \cup \{\infty\}$ instead, as these sets are homeomorphic.

Lemma 2.10. *Let $\varphi \in \mathbb{C}(z)$ be a rational function, then*

$$2deg(\varphi) - 2 = \sum_{z_0 \in \mathbb{P}^1(\mathbb{C})} (mult_{z_0}(\varphi) - 1).$$

Proof. If $\varphi : \mathbb{C} \to \mathbb{C}$, then we can define φ over the complex projective space $\mathbb{P}^1(\mathbb{C})$ as well, such that $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$. For a complete definition of this φ, see [Ba07] page 7. The genus of $\mathbb{P}^1(\mathbb{C})$ is zero. Applying the Riemann-Hurwitz formula gives the desired result. □

Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. The following theorem was postulated and proved by Belyĭ in 1979. For a proof see [Bel79].

Belyĭ's theorem. *For any finite subset S of $\mathbb{P}^1(\overline{\mathbb{Q}})$, there exists a rational function $\phi(x) \in \mathbb{Q}(x)$, only ramified over $\{0, 1, \infty\}$, such that $\phi(S) \subset \{0, 1, \infty\}$.*

The Riemann-Hurwitz formula and Belyĭ's theorem lead to the following lemma, presented by Granville [Gr98].

Lemma 2.11. *Given any homogeneous polynomial $f(x, y) \in \overline{\mathbb{Q}}[x, y]$. We can determine homogeneous polynomials $a(x, y)$, $b(x, y)$, $c(x, y) \in \mathbb{Z}[x, y]$ all of degree $D \geq 1$, without common factors, where $a(x, y)b(x, y)c(x, y)$ has exactly $D + 2$ non-proportional linear factors, including the factors of $f(x, y)$, and $a(x, y) + b(x, y) = c(x, y)$.*

Proof. Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be the rational function from Belyĭ's theorem such that $\phi(\{(\alpha, \beta) \in \mathbb{P}^1 : f(\alpha, \beta) = 0\}) \subset \{0, 1, \infty\}$, which is only ramified over $\{0, 1, \infty\}$. Let D be the degree of ϕ. We can write $\phi(x/y) = a(x, y)/c(x, y)$, where $a(x, y), c(x, y) \in \mathbb{Z}[x, y]$ are homogeneous polynomials, with degree D. Let $b(x, y) = c(x, y) - a(x, y)$. Note that

$$\phi(x/y) = 0 \iff a(x, y) = 0,$$

$$\phi(x/y) = 1 \iff b(x, y) = 0,$$

$$\phi(x/y) = \infty \iff c(x, y) = 0.$$

Therefore, whenever $f(x, y) = 0$, either $a(x, y) = 0$, $b(x, y) = 0$ or $c(x, y) = 0$ and thus all the linear factors of $f(x, y)$ are contained in $a(x, y)b(x, y)c(x, y)$. Let $\#\phi^{-1}(u) = |\{t \in \mathbb{P}^1(\mathbb{Q}) : \phi(t) = u\}|$, where $|.|$ denotes the cardinality of the set. Then, because of the three relations above, $\#\phi^{-1}(0)$, $\#\phi^{-1}(1)$ and $\#\phi^{-1}(\infty)$ are the number of distinct linear factors of $a(x, y)$, $b(x, y)$ and $c(x, y)$, respectively.

Because these polynomials share no common factors, $\#\phi^{-1}(0) + \#\phi^{-1}(1) + \#\phi^{-1}(\infty)$ is the number of distinct linear factors in $a(x,y)b(x,y)c(x,y)$.

We can apply Lemma 2.10 to ϕ, as it is a rational function and since it is only ramified over $\{0,1,\infty\}$.

$$2D-2 = \sum_{u\in\phi^{-1}(\{0,1,\infty\})} (mult_u(\phi)-1).$$

The right-hand side of this equation can be written as

$$\sum_{v\in\{0,1,\infty\}} \sum_{u\in\phi^{-1}(v)} (mult_u(\phi)-1)$$

$$= \sum_{u\in a^{-1}(0)} (mult_u(a)-1) + \sum_{u\in b^{-1}(0)} (mult_u(b)-1) + \sum_{u\in c^{-1}(0)} (mult_u(c)-1)$$

$$= deg(a) - \#a^{-1}(0) + deg(b) - \#b^{-1}(0) + deg(c) - \#c^{-1}(0)$$

$$= 3D - \#\phi^{-1}(0) - \#\phi^{-1}(1) - \#\phi^{-1}(\infty).$$

Therefore, $\#\phi^{-1}(0)+\#\phi^{-1}(1)+\#\phi^{-1}(\infty) = D+2$ which proves the lemma. □

Before presenting and proving the consequences of the abc-conjecture, a few more definitions and lemma's regarding the resultant of polynomials, presented by Barry, must be introduced [Ba07].

Definition 2.12 (Resultant)**.** *The resultant of two non-zero polynomials*

$$f(x) = b\prod_{i=1}^{s}(x-\beta_i),\ g(x) = c\prod_{j=1}^{r}(x-\gamma_j) \in \mathbb{Q}[x]$$

is defined by

$$R(f,g) = b^r c^s \prod_{i=1}^{s}\prod_{j=1}^{r}(\beta_i - \gamma_j).$$

For example, the resultant of $f(x) = 2(x-2)(x+3)$ and $g(x) = (x+1)(x-1)$ is $R(f,g) = 2(2+1)(2-1)(-3+1)(-3-1) = 48$. The following lemma is a property of the resultant. For a proof see [La02].

Lemma 2.13. *Given polynomials $f(x), g(x) \in \mathbb{Z}[x]$, there exist polynomials $a(x), b(x) \in \mathbb{Z}[x]$ with $deg(a) \leq deg(g) - 1$ and $deg(b) \leq deg(f) - 1$ such that $a(x)f(x) + b(x)g(x) = R(f,g)$.*

Definition 2.14 (Resultant of homogeneous forms)**.** *Let*

$$F(x,y) = \sum_{i=0}^{s} a_i x^{s-i}y^i,\ G(x,y) = \sum_{j=1}^{r} b_j x^{r-j}y^j,$$

be two binary homogeneous polynomials in $\mathbb{Z}[x,y]$ such that $a_0 \neq 0$, $b_0 \neq 0$. Then the resultant of f and g is $R(F,G) = R(f,g)$, where $f(x) = F(x,1)$ and $g(x) = G(x,1)$.

For example, the resultant of $F(x,y) = (x-2y)(x+5y)$ and $G(x,y) = (x+y)(x-3y)$ is $R(F,G) = (2+1)(2-3)(-5+1)(-5-3) = -96$

Lemma 2.15. *Let $F, G \in \mathbb{Z}[x,y]$ be two homogeneous polynomials without common factors, written as in definition 2.14. Let $m, n \in \mathbb{Z}$ with $\gcd(m,n) = 1$, then*

$$gcd(F(m,n), G(m,n))|R(F,G).$$

Proof. Let $F(x,y) = y^s f(\frac{x}{y})$ and $G(x,y) = y^r g(\frac{x}{y})$, such that $F(x,1) = f(x)$ and $G(x,1) = g(x)$. Let $a(x), b(x) \in \mathbb{Z}[x]$ be the polynomials from Lemma 2.13, such that $a(x)f(x) + b(x)g(x) = R(f,g)$. Now let $A(x,y) = y^{r-1}a(\frac{x}{y})$ and $B(x,y) = y^{s-1}b(\frac{x}{y})$. Then

$$\begin{aligned} A(x,y)F(x,y) + B(x,y)G(x,y) &= y^{r+s-1}(a(x,y)f(x,y) + b(x,y)f(x,y)) \\ &= y^{r+s-1}R(f,g) = y^{r+s-1}R(F,G). \end{aligned}$$

Therefore,

$$\gcd(F(m,n), G(m,n))|n^{r+s-1}R(F,G).$$

F and G are both homogeneous polynomials which means that the m and n can be interchanged. This yields

$$\gcd(F(m,n), G(m,n))|m^{r+s-1}R(F,G).$$

Since $\gcd(m,n) = 1$, this implies that

$$\gcd(F(m,n), G(m,n))|R(F,G).$$

□

The following theorem, with a proof by Granville [Gr98], is the key result in this subsection. From this point onward, $a \ll_A b$ denotes $a \leq k_A b$, where k_A is a constant dependent on the variables in the collection A (i.e. $a \ll_{\epsilon,f} b$ denotes $a \leq k_{\epsilon,f} b$, where $k_{\epsilon,f}$ is a constant dependent on ϵ and f).

Theorem 2.16. *Assume the abc-conjecture. Let $f(x,y) \in \mathbb{Z}[x,y]$ be a homogeneous polynomial of degree $d \geq 3$, without any repeated linear factors. Fix $\epsilon > 0$. Then, for any coprime integers m and n,*

$$\max\{|m|, |n|\}^{d-2-\epsilon} \ll_{\epsilon,f} \mathrm{Rad}(f(m,n)).$$

Proof. Let $a(x,y), b(x,y), c(x,y) \in \mathbb{Z}[x,y]$ be the homogeneous polynomials of degree D obtained by applying Lemma 2.11 to $f(x,y)$. Then the product of the distinct irreducible factors of $a(m,n)b(m,n)c(m,n)$ yields a polynomial $f(x,y)g(x,y)$ of degree $D+2$.

Now let $m, n \in \mathbb{Z}$ be two coprime integers and let $r = \gcd(a(m,n), b(m,n))$. It follows from Lemma 2.15 that r divides the resultant $R(a,b)$, which is a nonzero integer. Therefore, r is bounded. We can apply the abc-conjecture to the equation $\frac{a(m,n)}{r} + \frac{b(m,n)}{r} + \frac{c(m,n)}{r}$, which results in

$$\max\{|a(m,n)|, |b(m,n)|\} \ll_{\epsilon,f} \mathrm{Rad}(abc)^{1+\epsilon/D},$$

which implies

$$\max\{|a(m,n)|,|b(m,n)|\}^{1-\epsilon/D} \ll_{\epsilon,f} \operatorname{Rad}(abc)^{1-(\epsilon/D)^2} \ll_{\epsilon,f} \operatorname{Rad}(abc)$$

$$= \operatorname{Rad}(fg) \leq g(m,n)\operatorname{Rad}(f(m,n)).$$

We proceed by finding a lower bound for the left-hand side and an upper bound for the right-hand side of this equation. Let $H = \max\{|m|,|n|\}$. Note that we can write $g(x,y) = \sum_{i=0}^{D+2-d} g_i x^i y^{D+2-d-i}$ as the degree of $f(x,y)$ is d and the degree of $f(x,y)g(x,y)$ is $D+2$. Therefore, we can write

$$|g(m,n)| = \Big|\sum_{i=0}^{D+2-d} g_i m^i n^{D+2-d-i}\Big| \leq H^{D+2-d}\sum_{i=0}^{D+2-d}|g_i| \ll_f H^{D+2-d},$$

which provides an upper bound for the right-hand side.

Fix $\alpha,\beta \in \mathbb{R}$ such that $\alpha \neq \beta$. Note that

$$|\alpha-\beta|H = \max\{|m-\alpha n-(m-\beta n)|, |\alpha(m-\beta n)-\beta(m-\alpha n)|\}$$

$$\leq \max\{2,|\alpha|+|\beta|\}\max\{|m-\alpha n|,|m-\beta n|\},$$

hence we can write

$$H \leq \frac{\max\{2,|\alpha|+|\beta|\}}{|\alpha-\beta|}\max\{|m-\alpha n|,|m-\beta n|\}.$$

We can use this inequality to find the aforementioned lower bound. Note that we can write $a(x,y) = k_a\prod_{i=0}^{D}(x-\alpha_i y)$ and $b(x,y) = k_b\prod_{j=0}^{D}(x-\beta_j y)$ with $\alpha_i \neq \beta_j$ for any i and j, such that they are written as a product of their factors. This is a result of the fact that $a(x,y)$ and $b(x,y)$ share no factors. Now we can write

$$\max\{|a(m,n)|,|b(m,n)|\} = \max\Big\{\Big|k_a\prod_{i=0}^{D}(m-\alpha_i n)\Big|, \Big|k_b\prod_{j=0}^{D}(m-\beta_j n)\Big|\Big\}.$$

By noting that k_a and k_b depend on f, we can reduce this to

$$\max\{|a(m,n)|,|b(m,n)|\} \gg_f \max\Big\{\Big|\prod_{i=0}^{D}(m-\alpha_i n)\Big|, \Big|\prod_{i=0}^{D}(m-\beta_i n)\Big|\Big\}.$$

Let (α,β) be the pair of α_i and β_j which minimizes

$$\frac{\max\{2,|\alpha_i|+|\beta_j|\}}{|\alpha_i-\beta_j|},$$

then

$$\max\{|a(m,n)|,|b(m,n)|\} \gg_f \Big(\frac{\max\{2,|\alpha|+|\beta|\}}{|\alpha-\beta|}\Big)^D H^D \gg_f H^D,$$

since this α and β depend on the linear factors of a and b which depend on f and because $\alpha_i \neq \beta_j$ for all i and j.

Applying the lower and upper bound yields

$$\max\{|m|,|n|\}^{D-\epsilon} \ll_{\epsilon,f} g(m,n)\,\mathrm{Rad}(f) \leq \max\{|m|,|n|\}^{D+2-d}\,\mathrm{Rad}(f)$$

and thus

$$\max\{|m|,|n|\}^{d-2-\epsilon} \ll_{\epsilon,f} \mathrm{Rad}(f(m,n)),$$

which proves the theorem. □

Corollary 2.16.1. *Assume the abc-conjecture. Suppose $f(x) \in \mathbb{Z}[x]$ has no repeated roots. Fix $\epsilon > 0$. Then*

$$|x|^{\deg(f)-1-\epsilon} \ll_{\epsilon,f} \mathrm{Rad}(f(x)).$$

Proof. Let $F(x,y) = y^{\deg(f)+1} f(x/y)$. Then $F(x,1) = f(x)$ and $\deg(F) = \deg(f)+1$. Applying Theorem 2.16 gives

$$\mathrm{Rad}(f(m)) \gg_{\epsilon,f} \max\{|m|,|1|\}^{\deg(F)-2-\epsilon} = |m|^{\deg(f)-1-\epsilon},$$

since $\mathrm{Rad}(F(m,1)) = \mathrm{Rad}(f(m))$. □

Theorem 2.16 can be proven as well by assuming the weak abc-conjecture instead of the abc-conjecture, as will be shown below.

Theorem 2.17. *Assume the weak abc-conjecture. Let $f(x,y) \in \mathbb{Z}[x,y]$ be a homogeneous polynomial of degree $d \geq 3$, without any repeated linear factor such that $f(m,n) \in \mathbb{Z}$ for all $m,n \in \mathbb{Z}$. Let $\gamma > 0$ such that the weak abc-conjecture holds. Then, for any coprime integers m and n,*

$$max(|m|,|n|)^{d-2-\gamma_*} \ll_f \mathrm{Rad}(f(m,n)),$$

where $\gamma_* = D\gamma$ and D is the degree of the polynomials from Lemma 2.11.

Proof. The proof of this theorem is essentially the same as the proof of Theorem 2.16, except for the application of the abc-conjecture. In the proof of Theorem 2.16, the abc-conjecture is applied using $\frac{\epsilon}{D}$, where D is the degree of the polynomials derived from Lemma 2.11. This is possible because the abc-conjecture holds for any $\epsilon > 0$. If the weak abc-conjecture is true for γ then it is not necessarily true for $\frac{\gamma}{D}$. However, if the weak abc-conjecture is true for γ, then it is also true for $D\gamma > \gamma$. Therefore, we can use $\gamma_* = D\gamma$ in the same way as ϵ in the previous proof to obtain the desired result. □

Corollary 2.17.1. *Assume the weak abc-conjecture. Let $\gamma > 0$ such that the weak abc-conjecture holds. For any $f(x) \in \mathbb{Z}[x]$ with no repeated roots*

$$|x|^{deg(f)-1-\gamma_*} \ll_f \mathrm{Rad}(f(x)),$$

where $\gamma_* = D\gamma$ and D is the degree of the polynomials from Lemma 2.11 applied to the polynomial $F(x,y) = y^{\deg(f)+1} f(x/y)$.

Proof. This proof is essentially the same as the proof of Corollary 2.16.1. □

The following theorem is similar to Theorems 2.16 and 2.17, but requires the bound found by Stewart and Yu, presented in Theorem 2.7. As this bound has been proven, the following theorem and its corollary hold without any further assumptions.

Theorem 2.18. *Let $f(x,y) \in \mathbb{Z}[x,y]$ be a homogeneous polynomial of degree $d \geq 3$, without any repeated linear factor such that $f(m,n) \in \mathbb{Z}$ for all $m,n \in \mathbb{Z}$. Then, for any coprime integers m and n,*

$$H \ll_f \exp\Big(\frac{k}{D} H^{\frac{D+2-d}{3}} \operatorname{Rad}(f(m,n))^{\frac{1}{3}} \log(H^{D+2-d} \operatorname{Rad}(f(m,n)))^3\Big),$$

where $H = \max\{|m|,|n|\}$, D is the degree of the polynomials obtained by applying Lemma 2.11 to $f(x,y)$ and k is the constant from Theorem 2.7.

Proof. The desired result is obtained by applying Lemma 2.11 to $f(x,y)$ and applying Theorem 2.7 in the same fashion as the abc-conjecture was applied in the proof of Theorem 2.16. By using the lower bound for $\max\{|a(m,n)|,|b(m,n)|\}$ and the upper bound for $\operatorname{Rad}(abc)$, we find the inequality presented in the theorem. □

Corollary 2.18.1. *For any $f(x) \in \mathbb{Z}[x]$ with no repeated roots*

$$|x| \ll_f \exp\Big(\frac{k}{D} |x|^{\frac{D+1-\deg(f)}{3}} \operatorname{Rad}(f(x))^{\frac{1}{3}} \log(|x|^{D+1-\deg(f)} \operatorname{Rad}(f(x)))^3\Big),$$

where D is the degree of the polynomials obtained by applying Lemma 2.11 to $F(x,y) = y^{deg(f)+1} f(x/y)$ and k is the constant from Theorem 2.7.

Proof. The desired result is obtained by applying Theorem 2.18 on $F(x,y)$ and by realizing that $\deg(F) = \deg(f) + 1$. □

3 Constructing infinitely many primes

Since sequences of distinct, pairwise coprime integers such as those described in section 1 are clearly defined by a recurrence relation, they can be simplified using a recursive formula. The recurrence relation, which defines the sequence used in Euclid's proof for instance, can be described by the map $x_{n+1} = f(x_n) = (x_n - 1)x_n + 1$ by noting that any element in the sequence is equal to the product of all previous elements, minus 1. Similarly, the recurrence relation of the Fermat numbers can be described by the map $x_{n+1} = g(x_n) = (x_n - 2)x_n + 2$ as noted previously in Subsection 2.2.

In order to prove the infinitude of primes through Euclid's proof, one has to show that the greatest common divisor between any two elements in the aforementioned sequence is 1. To show that the sequence of Fermat numbers is an infinite sequence of distinct, pairwise coprime integers, one has to show

that the greatest common divisor between any two Fermat numbers is at most 2, as can be seen in Subsection 1.1. Using the recurrence relations introduced above, this corresponds to proving $x_n \equiv 1 \pmod{x_m}$ and $x_n \equiv 2 \pmod{x_m}$ for the sequence from Euclid's proof and for the Fermat numbers, respectively. This can be achieved by noting that $x_{n+1} = f(x_n) = f^n(x_0)$ and by applying Lemma 2.5 and the notation introduced in Subsection 2.2.

It follows from Lemma 2.5 that $x_n = f^{n-m}(x_m) \equiv f^{n-m}(0) \pmod{x_m}$ for any polynomial with integer coefficients and $0 < m < n$. The orbit of 0 under $f(x) = (x-1)x + 1$ is $0 \to 1 \to 1 \to \ldots$, and the orbit of 0 under $g(x) = (x-2)x + 2$ is $0 \to 2 \to 2 \to \ldots$. Therefore, $x_n \equiv 1 \pmod{x_m}$ for the map f and $x_n \equiv 2 \pmod{x_m}$ for the map g, which shows that the sequences introduced above are indeed infinite, distinct and pairwise coprime. In these examples, the orbits of 0 under their respective maps could be used to simplify the problem, as they are both preperiodic. The cases where the orbit of 0 is wandering are slightly more complicated as will be shown at the end of this section.

If a different orbit under the map $g(x) = (x-2)x + 2$ were to be taken, say the orbit of $x_0 = 4$, then the resulting sequence would be $4 \to 10 \to 82 \to ...$ which is obviously not a sequence of coprime integers. This is the case since the equivalency shown above holds for this orbit as well, so $x_n \equiv 2 \pmod{x_m}$ for all $0 < m < n$ and all the elements of the orbit are even. A way to turn this sequence into an infinite sequence of distinct, pairwise coprime integers would be to divide every element by 2, giving the equivalency $x_n \equiv 1 \pmod{x_m}$. This example shows that the orbit of 0 being preperiodic under a map does not always imply that wandering orbits under the same map are infinite sequences of distinct, pairwise coprime integers, but that they could perhaps be modified to find such sequences. The possible equivalencies between any two elements of an orbit depend on the distinct elements in the orbit of 0. When the number of distinct elements in the orbit of 0 is finite, then we can remove the finitely many distinct factors in the orbit of 0 from a wandering orbit to obtain an infinite sequence of distinct coprime integers. However, when the orbit of 0 contains infinitely many factors, the construction becomes more complicated.

Subsections 3.1 and 3.2 will provide general methods for constructing such sequences when the orbit of 0 is stricly preperiodic or periodic. In Subsection 3.3, maps under which the orbit of 0 is wandering will be considered, concluding with a proof to show that the orbits of those maps contain infinitely many primitive prime factors.

3.1 A general method when 0 is strictly periodic

Before giving a general method for performing a modification similar to the one used in the previous section, we should prove the following lemma's. The first lemma is presented by Granville with a complete proof and the second is presented with a sketch of a proof [Gr17].

Lemma 3.1. *Let $f(x) \in \mathbb{Z}[x]$. If the orbit of x_0 is periodic, then its exact period*

length is either one or two.

Proof. Suppose the exact period length is $n \geq 3$. Then $x_n = x_0$ and $x_n - x_0 = \sum_{i=1}^{n}(x_i - x_{i-1}) = 0$. It follows from Lemma 2.5 that

$$(x_i - x_{i-1})|(f(x_i) - f(x_{i-1})) = x_{i+1} - x_i$$

for every $i \geq 1$, but this implies that

$$|x_1 - x_0| \leq |x_2 - x_1| \leq ... \leq |x_{n+1} - x_n| = |x_1 - x_0|$$

and thus that all of these are in fact equal. If none of these differences differ in sign, then $x_n - x_0 \neq 0$, so there must be some $j \geq 1$ for which $x_{j+1} - x_j = -(x_j - x_{j-1})$ and thus for which $x_{j+1} = x_{j-1}$. However, this implies

$$x_2 = x_{n+2} = f^{n+1-j}(x_{j+1}) = f^{n+1-j}(x_{j-1}) = f^n(x_0) = x_n.$$

This is a contradiction, since we assumed the exact period length to be at least three, which proves that the exact period length has to be either one or two. □

Lemma 3.2. *Let $f(x) \in \mathbb{Z}[x]$. If the orbit of 0 is strictly preperiodic under f, then the exact length of the preperiod is either one or two.*

Proof. As a consequence of Lemma 3.1, we can split this proof into two cases: (i) The period length is one. (ii) The period length is two.

(i) In this case, the orbit of 0 is given by

$$0 \to x_1 \to ... \to x_m \to x_m \to ...$$

It follows from Lemma 2.5 that

$$(x_1 - 0)|(f(x_1) - f(0)) = (x_2 - x_1)$$

which implies that $x_1|x_2$. By combining this with the fact that $x_2|(x_3 - x_1)$, we see that $x_1|x_3$. Now assume $x_1|x_k$ for all $k \geq 1$, then $x_1|x_{k+1}$, because $x_k|(x_{k+1} - x_1)$. It remains to show that $x_m|x_1$, which can be shown by noting that

$$x_m|(f(x_m) - f(0)) = x_m - x_1.$$

Now we know that $x_1|x_2$, $x_2|x_3$, ..., $x_m|x_1$ and thus that $|x_1| = |x_2| = ... = |x_m|$. Therefore either $x_1 = x_2$ in which case x_1 is periodic or $x_1 = -x_2 = -x_3$ in which case x_2 is periodic If $x_1 = -x_2 = x_3$, then x_1 is periodic with period length 2, which contradicts our assumptions, so this cannot be the case.

(ii) In this case, the orbit of 0 is given by

$$0 \to x_1 \to ... \to x_m \to x_{m+1} \to x_m \to ...$$

This case can be split again into two more cases. One where the preperiod m is even and one where m is odd. We will only deal with the first case, since the second case follows a similar proof.

Assume m is even. It follows from Lemma 2.5 and the fact that the period length is 2 that

$$x_m|(x_{m+1} - x_1)|(x_m - x_2)| \ ... \ |(x_m - x_{m-2}),$$

so x_m divides every element in the sequence with an even index number. Now take the sequence of even indices $\{2, 4, ..., m\}$. Let i be an arbitrary element of this sequence. It follows from Lemma 2.5 that $x_i|(x_{2i} - x_i)$ if $2i < m$ and $x_i|(x_m - x_i)$ if $2i > m$, so either $x_i|x_{2i}$ or $x_i|x_m$. Note that if $2i < m$, then $2i$ is again an element of the sequence of even indices. Therefore $x_{2i}|x_{4i}$ or $x_{2i}|x_m$. Since m is finite, we can continue this process to show that $x_i|x_m$ for every $i \in \{2, 4, ..., m\}$. Therefore $x_2|x_4|...|x_m|x_2$, from which it follows that

$$|x_2|= |x_4|= ... = |x_m|$$

. We assumed $m > 2$ to be even, but $m < 6$, otherwise $x_2 \neq x_4 \neq x_6$, which is impossible if their absolute values are identical. Therefore m must be 4 and $x_2 = -x_4$.

Because we know that x_1 divides all the other elements in the sequence and because $x_2 = -x_4$, we can rewrite the elements as

$$x_2 = ax_1, \ x_3 = bx_1, \ x_4 = -ax_1.$$

It follows from Lemma 2.5 that $x_2|(x_3 - x_1)$ and thus that $a|(b - 1)$. We can use this to write $x_3 = (ac + 1)x_1$ for some $c \in \mathbb{Z}$. Using the same reasoning, $(x_2-x_1)|(x_3-x_2)$ implies that $c = d(a-1)$, which we can use to write $x_3 = (a(a-1)d + 1)x_1$. We can now use Lemma 2.5 again to arrive at an inequality which we can use to prove that m cannot be 4. Namely, it follows from $x_3|(x_4 - x_1)$ that

$$|a(a - 1)d + 1|\leq |a + 1|.$$

Note that $a = 0$ would imply that 0 itself is periodic and $a = \pm 1$ would imply that x_1 is periodic, so $|a|\geq 2$. If $d = 0$, then x_1 is periodic, so $|d|\geq 1$. We first consider the cases where both a and d are positive, so where $a \geq 2$ and $d \geq 1$. The inequality given above reduces to

$$(a - 1)d \leq 1.$$

Note that this equality only holds if $d = 1$ and $a = 2$, but from Lemma 2.5, as shown above, we know that $x_3|x_m = x_4$, which would imply that $3x_1|2x_1$. This can only be true if $x_1 = 0$, which we have assumed not to be true.

Now we consider the case where $a \leq -2$ and $d \leq -1$. Using these restrictions, we can reduce the inequality to

$$(a - 1)d \leq 1,$$

which has no solutions for $a \leq -2$.

The next restrictions we consider are $a \geq 2$ and $d \leq -1$. This reduces the inequality to

$$a^2|d|-a(|d|+1) - 2 \leq 0,$$

from which it follows that

$$\frac{|d|+1-\sqrt{|d|^2+10|d|+1}}{2|d|} \leq a \leq \frac{|d|+1+\sqrt{|d|^2+10|d|+1}}{2|d|}.$$

The left-hand side is always a negative number and we assumed a to be greater than or equal to 2, so only the right-hand side gives us a new restriction. Since a has to be greater than or equal to 2, we can use the right-hand side to find a restriction for d. Equating it to 2 gives us $|d|= 2$ and thus $d = -2$. For all d smaller than -2, $a < 2$, which contradicts our assumptions, so d has to be -1 or -2. If $d = -1$, then $1 - \sqrt{3} \leq a \leq 1 + \sqrt{3} < 2$, which contradicts our assumptions. So $d \neq -1$. If $d = -2$, then $-\frac{1}{2} \leq a \leq 2$, so a has to be 2. Therefore x_3 has to be $-3x_1$ which implies $-3x_1|2x_1$, which is not possible, since $x_1 \neq 0$.

Lastly, we consider the restriction $a \leq -2$ and $d \geq 1$. This reduces the inequality to

$$a^2d + a(1-d) + 2 \leq 0,$$

which in turn gives the following restriction on d:

$$d \leq \frac{-a-2}{a(a-1)}.$$

The right-hand side of this inequality has a maximum for negative a, which is $5 - 2\sqrt{6} < 1$, which implies that $d < 1$, which contradicts our assumption that $d \geq 1$. Therefore, there are no solutions to the inequality.

This proves that if 0 is preperiodic with an even preperiod length m, than m can not be greater than 2, and therefore has to be exactly 2. A similar proof can be given when m is odd. □

Now we can give a method for creating infinite sequences of pairwise coprime integers, presented with the same proof by Granville [Gr17].

Theorem 3.3. *Suppose that $f(x) \in \mathbb{Z}[x]$ and that 0 is strictly preperiodic under f. Let $\ell(f) = lcm(f(0), f^2(0))$. For any wandering orbit $(x_n)_{n\geq 0}$, the sequence $(a_n)_{n\geq 0}$, where*

$$a_n = \frac{x_n}{gcd(x_n, \ell(f))},$$

is an infinite sequence of pairwise coprime integers. If $n \geq 3$, then a_n has a private prime factor.

Proof. Suppose $k = n - m > 0$. Then, using Lemma 2.5, we can write

$$x_n = f^k(x_m) \equiv f^k(0) \pmod{x_m},$$

from which it follows that $x_n = ax_m + f^k(0)$ for some $a \in \mathbb{Z}$. We can also write $x_n = k(x_m, x_n)$ and $x_m = l(x_m, x_n)$ for some $k, l \in \mathbb{Z}$. Combining these equalities yields $(x_m, x_n)(k - al) = f^k(0)$ and therefore $(x_m, x_n)|f^k(0)$.

Now let

$$L(f) := lcm[f^k(0)|k \geq 1],$$

then $(x_m, x_n)|L(f)$ and therefore $(x_m, x_n)|(x_m, L(f))$ and $(x_m, x_n)|(x_n, L(f))$.

Let $(A_n)_{n\geq 0}$ be a sequence where

$$A_n = \frac{x_n}{gcd(x_n, L(f))},$$

then $A_n|(x_n/(x_m, x_n))$ and $A_m|(x_m/(x_m, x_n))$, but

$$\left(\frac{x_m}{(x_m, x_n)}, \frac{x_n}{(x_m, x_n)}\right) = 1,$$

so $(A_m, A_n) = 1$. It remains to show that $L(f) = \ell(f)$.

If the preperiod is 1, then $f^2(0) = f(0)$ or $f^3(0) = f(0)$, so the unique elements in the orbit of 0 are $\{0, f(0)\}$ or $\{0, f(0), f^2(0)\}$ and thus $L(f) = \ell(f)$. If the preperiod is 2 and the period is 1, then the unique elements in the orbit of 0 are $\{0, f(0), f^2(0)\}$. If the preperiod is 2 and the period is 1, then it follows from Lemma 2.5 that $x_3|(x_3 - x_1)$ and thus $x_3|x_1$. This means that $x_3|\ell(f)$ and therefore $L(f) = \ell(f)$. □

With this theorem, we can create infinite sequences of pairwise coprime integers using maps under which the orbit of 0 is strictly preperiodic. An example of such a polynomial map is $f(x) = x^2 - 4x + 4$. Note that the orbit of 0 under this map is $0 \to 4 \to 4 \to \ldots$, so this orbit is indeed preperiodic. If we apply Theorem 3.3 to the orbit of $x_0 = 6$, then we obtain the coprime sequence

$$3 \to 4 \to 49 \to 9409 \to 354079489 \to 501489136705686529 \to \ldots$$

Using prime factorization, we can extract a sequence of distinct primes from this sequence.

$$3 \to 2 \to 7 \to 97 \to 31 \to 708158977 \to \ldots$$

Prime factorization with our current techniques is quite slow and the growth of the a_n is at least quadratic (larger for higher order polynomials) for large n. Therefore, it becomes difficult to extract actual prime factors from $(a_n)_{n\geq 0}$ for large n. In this thesis, examples of prime factors were found using Pollard's rho method for factorization, described in [Po75]. The complexity of this algorithm is $\mathcal{O}(\sqrt{p}) \leq \mathcal{O}(N^{1/4})$, where p is the smallest prime factor contained in the integer N, which we try to factor.

3.2 General methods when 0 is periodic

Theorem 3.3 gives a method for finding infinite sequences of pairwise coprime integers which is valid when 0 is strictly preperiodic. In this section, appropriate methods for when 0 is periodic will be explored. It follows directly from Lemma

3.1 that, when 0 is periodic under a certain map, the period length is either 1 or 2.

If we assume the period length of 0 under the map $f(x) \in \mathbb{Z}[x]$ to be 1, then $f(0) = 0$. Since f is a polynomial with integer coefficients, it can be written as $f(x) = a_k x^k + ... + a_0$ and therefore $f(0) = a_0 = 0$. It follows that f can be written as the product of an arbitrary polynomial $g(x) \in \mathbb{Z}[x]$ and a polynomial of the form $h(x) = x^p$, with $p \geq 1$ chosen such that $g(0) \neq 0$, so $f(x) = h(x)g(x) = x^p g(x)$. Note that if $g(x) = c$ with $c \in \mathbb{Z}$ for all x, then all the elements of any orbit of x_0 under f are products of powers of c and powers of x_0, so we can not create an infinite sequence of distinct, pairwise coprime integers from such orbits. Therefore, we will assume the order of g to be at least 1. The following theorem and its proof are found by Granville [Gr17].

Theorem 3.4. *Suppose that $f(x) = x^p g(x)$ for some $g(x) \in \mathbb{Z}[x]$, with $\deg(g) \geq 1$, and where $p \geq 1$ is chosen such that $g(0) \neq 0$. For any given wandering orbit $(x_n)_{n\geq 0}$ under the map f, the sequence $(a_n)_{n\geq 1}$, where*

$$a_{n+1} := \frac{g(x_n)}{gcd(g(x_n), g(0))},$$

is an infinite sequence of distinct, pairwise coprime integers and, once n is sufficiently large, each a_n has a private prime factor.

Proof. Assume that $m < n$. Given a wandering orbit of x_0 under the map f, $x_{n+1} = x_n^p g(x_n)$. Therefore, $x_m | x_n$ for all m. Note that

$$a_{n+1} x_n^p (g(x_n), g(0)) = x_{n+1},$$

so $a_{n+1} | x_{n+1}$. Furthermore,

$$(g(x_m), g(x_n)) | (x_{m+1}, g(x_n)),$$

because $g(x_m) | x_{m+1}$. We have seen above that $x_m | x_n$ for every m, but since $m < n$, $m + 1 \leq n$ and therefore $x_{m+1} | x_n$ as well. Therefore,

$$(x_{m+1}, g(x_n)) | (x_n, g(x_n)).$$

We can write $g(x_n) = ax_n + g(0)$ for some $a \in \mathbb{Z}$ and use the Euclidean algorithm to show that

$$(x_n, g(x_n)) = (x_n, g(0)),$$

which implies that

$$(g(x_m), g(x_n)) | (g(x_n), g(0)),$$
$$(g(x_m), g(x_n)) | (g(x_m), g(0)).$$

This shows that

$$a_{m+1} \Big| \frac{x_m}{(g(x_m), g(x_n))},$$
$$a_{n+1} \Big| \frac{x_n}{(g(x_m), g(x_n))}.$$

Therefore, we deduce that $(a_{n+1}, a_{m+1}) = 1$.

It remains to prove that each a_n has a private prime factor for large enough n. Note that this is the case if $|a_n| > 1$. If $a_{n+1} = 0$, then $g(x_n) = 0$, which contradicts our assumptions. If $|a_{n+1}| = 1$, then $g(x_n) = (g(x_n), g(0))$, which implies that $g(x_n)$ is a divisor of $g(0)$. Since $g(0)$ is finite, it has only a finite number of divisors and because x_0 is wandering and $g(x)$ is non-constant, there is a finite number of n such that $g(x_n)$ is a divisor of $g(0)$. Therefore, if n is large enough $|a_n| > 1$ as desired.

□

An example of a polynomial to which we can apply this theorem, is $f(x) = 4x + 5x^2 = x(4 + 5x) = xg(x)$. Note that the orbit of 0 under this map is $0 \to 0 \to \ldots$, so this orbit is indeed periodic with period length 1. If we apply Theorem 3.4 to the orbit of $x_0 = 6$, then we obtain

$$17 \to 256 \to 261121 \to 272735662081 \to 297538965481954742353921 \to \ldots,$$

from which we can extract the prime factors

$$17 \to 2 \to 7 \to 367 \to 97 \to \ldots$$

The other polynomial maps, for which zero is periodic, are the maps where $f^2(0) = f(x_1) = 0$, where $x_1 \neq 0$. In order to obtain infinite sequences of distinct integers, polynomial maps must have some wandering orbits. As the map $f(x) = a - x$, where $a \in \mathbb{Z}$ is an arbitrary constant, is always periodic, we will not consider such maps. The following theorem and its proof can be found in [Gr17].

Theorem 3.5. *Suppose $f(x) \in \mathbb{Z}[x]$ with $f(x) + x$ nonconstant, such that 0 is periodic under the map $x \to f(x)$, with period length 2. Write $f^2(x) = x^r G(x)$ with $G(0) \neq 0$ and $r \geq 1$. For any given wandering orbit $(x_n)_{n\geq 0}$ with $x_0 \in \mathbb{Z}$, define*

$$a_{n+2} := \frac{G(x_n)}{\gcd(G(x_n), G(0)f(0))} \text{ for all } n \geq 0.$$

The $(a_n)_{n\geq 2}$ are an infinite sequence of pairwise coprime integers and, once n is sufficiently large, each a_n has a private prime factor.

Proof. Firstly, we show that $G(x)$ is not some constant $c \in \mathbb{Z}$. If $G(x) = c$, then $f^2(x) = cx^r$, which implies that $f^2(x)$ has exactly one distinct root, which is 0. We can show that $f^2(x)$ has at least as many roots as $f(x)$. For every root r of $f(x)$ there exists $q \in \mathbb{C}$ such that $f(q) = r$. Therefore, there are at least as many distinct q's as distinct r's. Note that $f^2(q) = f(r) = 0$, so each q is a root of $f^2(x)$. Therefore, $f^2(x)$ has at least as many roots as $f(x)$. Since $f^2(x) = f(f(x)) = 0$ for some x and as the number of distinct roots of $f(x)$ is at most one, $f(x)$ has exactly one distinct root. Let $a \neq 0$ be this root. Then we can write $f(x) = c(x - a)^d$ and $f^2(x) = c(c(x - a)^d - a)^d$, which is 0 when $c(x - a)^d = a$. This has distinct solutions if $d > 1$, while $f^2(x)$ has

only one distinct root. Therefore, $d = 1$ and $f^2(x) = c^2x - c^2a - ca$. Since the root of $f^2(x)$ is 0, $c^2a = -ca$ and thus $c = -1$. Inserting this into $f(x)$ yields $f(x) = a - x$, which means $f(x) + x$ is constant, contradicting our assumptions. Thus, $G(x)$ is not a constant.

We know that $a_{n+2}|G(x_n)|x_{n+2}$ for every $n \geq 0$. Let $n > m \geq 0$. If $n - m$ is even, then

$$(G(x_m), G(x_n))|(x_{m+2}, G(x_n))|\ldots|(x_n, G(x_n)) = (x_n, G(0))|G(0).$$

Therefore,

$$(G(x_m), G(x_n))|(G(x_m), G(0)f(0)) \; and \; (G(x_m), G(x_n))|(G(x_n), G(0)f(0)).$$

This implies that

$$\frac{G(x_m)}{(G(x_m), G(0)f(0))}\Big|\frac{G(x_m)}{(G(x_m), G(x_n))} \; and \; \frac{G(x_n)}{(G(x_n), G(0)f(0))}\Big|\frac{G(x_n)}{(G(x_m), G(x_n))}.$$

The left-hand sides are a_{m+2} and a_{n+2} and the right-hand sides of these equations are clearly coprime, so $\gcd(a_{m+2}, a_{n+2}) = 1$.

If $n - m$ is odd, then

$$G(x_m)|x_{m+2}|\ldots|x_{n-1}|x_{n+1},$$

and

$$G(x_n)|x_{n+2} = f(x_{n+1}).$$

Therefore,

$$(G(x_m), G(x_n))|(x_{n+1}, f(x_{n+1})) = (x_{n+1}, f(0))|f(0).$$

This implies that

$$(G(x_m), G(x_n))|(G(x_m), G(0)f(0)) \; and \; (G(x_m), G(x_n))|(G(x_n), G(0)f(0)),$$

from which it follows that

$$\frac{G(x_m)}{(G(x_m), G(0)f(0))}\Big|\frac{G(x_m)}{(G(x_m), G(x_n))} \; and \; \frac{G(x_n)}{(G(x_n), G(0)f(0))}\Big|\frac{G(x_n)}{(G(x_m), G(x_n))}.$$

So in this case, $(a_{m+2}, a_{n+2}) = 1$ as well.

This shows that the $(a_n)_{n\geq 2}$ are an infinite sequence of pairwise coprime integers. The proof for showing that the a_n contain a private prime factor for sufficiently large n is equivalent to that of the proof below Theorem 3.4. □

An example of a polynomial map to which we can apply this theorem is $f(x) = x^2 - 6x + 5$. Note that $f^2(x) = x(x^3 - 12x^2 + 40x - 24) = xG(x)$ and the orbit of 0 is $0 \to 5 \to 0 \to \ldots$, which is indeed periodic with period length 2. Applying Theorem 3.5 to the orbit of $x_0 = 8$ yields

$$1 \to 319 \to 3943997 \to 338166506260267 \to \ldots,$$

from which we can extract the prime factors

$$11 \to 157 \to 19 \to \dots$$

As noted by Granville, Theorems 3.3, 3.4 and 3.5 together result in the following corollary [Gr17].

Corollary 3.5.1. *Suppose $f(x) \in \mathbb{Z}[x]$ is not of the form cx^d or $a - x$ for any $a, c \in \mathbb{Z}$, and that 0 is preperiodic under the map $x \to f(x)$. Then, for any given wandering orbit $(x_n)_{n\geq 0}$ with $x_0 \in \mathbb{Z}$, each x_n has a private prime factor for all sufficiently large n.*

3.3 The case where 0 has a wandering orbit

In this subsection, we will consider a method for finding infinite sequences of primes when the orbit of 0 under a polynomial map is wandering. We shall see that, while such sequences can certainly be constructed in these cases, the construction relies on prime factorization algorithms. Currently, these algorithms are incredibly computationally expensive. Therefore, such constructions are currently quite difficult.

Before being able to prove that the aforementioned constructions are possible, the following lemma and its corollary must be introduced. Granville provides the lemma with a sketch of a proof and the corollary with a complete proof [Gr17]. The proof of the lemma provided here is derived from Granville's sketch of a proof.

Lemma 3.6. *If $f(x) \in \mathbb{Z}[x]$ has degree $d > 1$ and if x_0 is an integer whose orbit is wandering, then there exist real numbers $1 \geq \alpha > 0$ and β, which depend only on f, for which $|x_n|$ is the integer nearest to $\alpha\tau^{d^n} + \beta$, when n is sufficiently large and where $\tau > 1$ is a constant that depends on both f and x_0.*

Proof. Without loss of generality, suppose $f(x) = ax^d + bx^{d-1} + \dots$ with $a > 0$. Let $(x_n)_{n\geq 0}$ be the orbit of x_0 under the map f and let $y_n = \alpha^{-1}(x_n - \beta)$, where $\alpha = a^{-\frac{1}{d-1}}$ and $\beta = -\frac{b}{ad}$. We will show that the polynomial $y_{n+1} - y_n^d$ is of degree $\leq d - 2$.

$$y_{n+1} - y_n^d = \alpha^{-1}(ax_n^d + bx_n^{d-1} + \dots - \beta) - (\alpha^{-1}(x_n - \beta))^d.$$

If the order of this polynomial is at most $d - 2$, then the terms involving x_n^d and x_n^{d-1} must disappear. These terms are

$$\alpha^{-1}ax_n^d - \alpha^{-d}x_n^d = (a^{\frac{d}{d-1}} - a^{\frac{d}{d-1}})x_n^d = 0,$$

and

$$\alpha^{-1}bx_n^{d-1} + \alpha^{-d}d\beta x_n^{d-1} = a^{\frac{1}{d-1}}bx_n^{d-1} - a^{\frac{d}{d-1}}d\frac{b}{da}x_n^{d-1} = 0,$$

so the degree of this polynomial is at most $d - 2$. We can prove that

$$(y_n - \epsilon)^d + \epsilon < y_{n+1} < (y_n + \epsilon)^d - \epsilon \tag{2}$$

for any $\epsilon > 0$, for sufficiently large n by showing that $y_{n+1} - (y_n - \epsilon)^d - \epsilon$ and $y_{n+1} - (y_n + \epsilon)^d + \epsilon$ are polynomials of degree $d-1$ with a positive and a negative coefficient on their $d-1$ exponential terms, respectively. The first polynomial can be written in terms of x_n as

$$y_{n+1} - (y_n - \epsilon)^d + \epsilon = \alpha^{-1}(ax_n^d + bx_n^{d-1} + \ldots) - \alpha^{-1}\beta - (\alpha^{-1}(x_n - \beta) - \epsilon)^d + \epsilon.$$

Note that the coefficient on the d exponential term is the exact same as in the $y_{n+1} - y_n^d$ polynomial and therefore 0. The $d-1$ exponential term is

$$\alpha^{-1}bx_n^{d-1} - \alpha^{1-d}x_n^{d-1}d(\alpha^{-1}\beta + \epsilon) = a\epsilon d x_n^{d-1}.$$

a, ϵ and d are all positive numbers and therefore, the coefficient of this term is a positive number as well. So this polynomial has degree $d-1$ and a positive coefficient on the $d-1$ exponential term. Therefore, as n tends to infinity, this polynomial will tend to infinity, which proves that $(y_n - \epsilon)^d + \epsilon < y_{n+1}$ for sufficiently large n. By applying the same reasoning to the polynomial $y_{n+1} - (y_n + \epsilon)^d + \epsilon$, we find that it has degree $d-1$ as well and that the coefficient on the $d-1$ exponential term is $-a\epsilon d$, which is obviously a negative number. Therefore, this polynomial tends to negative infinity as n tends to infinity, which proves that $y_{n+1} < (y_n + \epsilon)^d - \epsilon$ for sufficiently large n.

Now let $\ell_n = (y_n - \epsilon)^{1/d^n}$ and $u_n = (y_n + \epsilon)^{1/d^n}$. It follows from (2) that

$$\ell_n = (y_n - \epsilon)^{1/d^n} = ((y_n - \epsilon)^d)^{1/d^{n+1}} < (y_{n+1} - \epsilon)^{1/d^{n+1}} = \ell_{n+1},$$

$$\ell_n = (y_n - \epsilon)^{1/d^n} < (y_n + \epsilon)^{1/d^n} = u_n,$$

$$u_{n+1} = (y_{n+1} + \epsilon)^{1/d^{n+1}} < ((y_n + \epsilon)^d)^{1/d^{n+1}} = (y_n + \epsilon)^{1/d^n} = u_n,$$

for sufficiently large n. Therefore, $\ell_n < \ell_{n+1} < \ldots < u_{n+1} < u_n$ which implies that the ℓ_n form an increasing bounded sequence, which must tend to some limit, which we will denote as τ. Thus,

$$(y_n - \epsilon)^{1/d^n} < \tau < (y_n + \epsilon)^{1/d^n}$$

which implies

$$\tau^{d^n} - \epsilon < y_n < \tau^{d^n} + \epsilon.$$

In terms of x_n, this inequality is

$$\alpha\tau^{d^n} - \alpha\epsilon + \beta < x_n < \alpha\tau^{d^n} + \alpha\epsilon + \beta.$$

By taking $\epsilon = \frac{\alpha}{2}$, this reduces to

$$\alpha\tau^{d^n} + \beta - \frac{1}{2} < x_n < \alpha\tau^{d^n} + \beta + \frac{1}{2},$$

which proves the lemma. □

As $d \geq 2$ and $\tau > 1$, we can easily see that the elements of these orbits grow exponentially. This is why factorization of these orbits proves rather difficult in practice. Moreover, this lemma only holds for large n. We shall see below that if n is not sufficiently large, we cannot guarantee the factorization to succesfully find a primitive prime factor. Therefore, this lemma shows that finding actual primes from these orbits is not feasible with our current factorization techniques.

In the case $x_0 = 0$, we will write $\tau = \tau_0$. The proof of the following corollary is provided by Granville [Gr17].

Corollary 3.6.1. *If $f(x) \in \mathbb{Z}[x]$ has degree $d > 1$, x_0 is an integer whose orbit is wandering and if $0 \leq m \leq n-1$, then*

$$\gcd(x_m, x_n) \leq \min\{|x_m|, f^{n-m}(0)\} \leq 2\tau_*^{d^{n/2}},$$

if n is sufficiently large and where $\tau_* = \max\{\tau, \tau_0\}$.

Proof. We have seen before that $x_n \equiv f^{n-m}(0) \pmod{x_m}$. Therefore we know that $\gcd(x_m, x_n)$ divides x_m and $f^{n-m}(0)$, and thus

$$\gcd(x_m, x_n) \leq \min\{|x_m|, f^{n-m}(0)\}. \tag{3}$$

Furthermore, it follows from Lemma 3.6 that $|x_m| \leq 2\tau^{d^m}$ if m is sufficiently large and $f^{n-m}(0) \leq 2\tau_0^{d^{n-m}}$ if $n-m$ is sufficiently large, because $\alpha \leq 1$. We can take n sufficiently large such that either m or $n-m$ is sufficiently large. This gives the following inequality:

$$\min\{|x_m|, f^{n-m}(0)\} \leq \min\{2\tau_*^{d^m}, 2\tau_*^{d^{n-m}}\} \leq 2\tau_*^{d^{n/2}}, \tag{4}$$

where $\tau_* = \max\{\tau_0, \tau\}$. Combining (3) and (4) yields the desired result. □

Now we can prove that wandering orbits under polynomial maps, for which the orbit of 0 is wandering, contain infinitely many primitive prime factors. The key to this proof is showing that the orbits grow too fast to contain finitely many primitive prime powers. This is where the abc-conjecture and its consequences are applied. Therefore, the validity of the following depends on the validity of the abc-conjecture.

The following theorem and a slightly more concise proof are provided by Granville [Gr17].

Theorem 3.7. *Assume the abc-conjecture. Suppose $f(x) \in \mathbb{Z}[x]$ has no repeated roots and is of degree $d \geq 2$, and 0 and x_0 both have wandering orbits under the map $x \to f(x)$. Then x_n contains a primitive prime factor for all sufficiently large n.*

Proof. Fix $0 < \epsilon < d-1$. It follows from Corollary 2.16.1 that

$$|x| \ll_{\epsilon, f} \operatorname{Rad}(f(x))^{\frac{1}{d-1-\epsilon}}.$$

If $(x_n)_{n\geq 0}$ is an orbit under the map f, then

$$|x_{n-1}| \ll_{\epsilon,f} \operatorname{Rad}(f(x_{n-1}))^{\frac{1}{d-1-\epsilon}} = \operatorname{Rad}(x_n)^{\frac{1}{d-1-\epsilon}}. \tag{5}$$

Now assume x_n has no primitive prime factor, then, for every distinct prime factor p_i of x_n, there exists $0 \leq m \leq n-1$ such that $p_i | gcd(x_m, x_n)$. Therefore,

$$\operatorname{Rad}(x_n) | \prod_{m=0}^{n-1} \gcd(x_m, x_n).$$

Using Corollary 3.6.1, we get

$$\operatorname{Rad}(x_n) \leq \prod_{m=0}^{n-1} \gcd(x_m, x_n) \leq 2^n \tau_*^{nd^{n/2}}. \tag{6}$$

Finally substituting (6) into (5) gives

$$|x_{n-1}| \ll_{\epsilon,f} (2^n \tau_*^{nd^{n/2}})^{\frac{1}{d-1-\epsilon}} = 2^{n/(d-1-\epsilon)} \tau_*^{nd^{n/2}/(d-1-\epsilon)}. \tag{7}$$

The following inequality follows directly from Lemma 3.6:

$$|x_{n-1}| \geq \lfloor \alpha \tau^{d^{n-1}} + \beta \rfloor, \tag{8}$$

where α and β depend only on f, and τ on f and x_0. Let $\delta_n = 1 + \frac{\beta - 1}{\alpha \tau^{d^{n-1}}}$ such that for sufficiently large n, $\delta_n > 0$, then combining (7), (8) and the inequality $\tau \leq \tau_*$ yields

$$\delta_n \alpha \tau^{d^{n-1}} < \lfloor \alpha \tau^{d^{n-1}} + \beta \rfloor \ll_{\epsilon,f} 2^{n/(d-1-\epsilon)} \tau_*^{nd^{n/2}/(d-1-\epsilon)}.$$

By taking logarithms we can reduce this to

$$\frac{\log(\delta_n)}{\log(\tau)} + \frac{\log(\alpha)}{\log(\tau)} + d^{n-1} \ll_{\epsilon,f} \frac{n}{d-1-\epsilon} \frac{\log(2)}{\log(\tau)} + \frac{nd^{n/2}}{d-1-\epsilon} \frac{\log(\tau_*)}{\log(\tau)}.$$

This inequality must hold for any sufficiently large n, therefore it must hold as n tends to infinity. Therefore, the following inequality must hold as well.

$$\lim_{n\to\infty} d^{n-1} \ll_{\epsilon,f} \lim_{n\to\infty} \left(\frac{n}{d-1-\epsilon} \frac{\log(2)}{\log(\tau)} + \frac{nd^{n/2}}{d-1-\epsilon} \frac{\log(\tau_*)}{\log(\tau)} - \frac{\log(\delta_n)}{\log(\tau)} - \frac{\log(\alpha)}{\log(\tau)} \right),$$

and therefore

$$1 \ll_{\epsilon,f} \lim_{n\to\infty} \left(\frac{\frac{n}{d-1-\epsilon} \frac{\log(2)}{\log(\tau)} + \frac{nd^{n/2}}{d-1-\epsilon} \frac{\log(\tau_*)}{\log(\tau)} - \frac{\log(\delta_n)}{\log(\tau)} - \frac{\log(\alpha)}{\log(\tau)}}{d^{n-1}} \right). \tag{9}$$

We can split the right-hand side into four different limits of which the last term is obviously 0. The term involving δ_n is 0 as well, since $\lim_{n\to\infty} \delta_n = 1$. The other two limits can be determined using L'Hôpital's rule.

$$\lim_{n\to\infty} \left(\frac{\frac{n}{d-1-\epsilon} \frac{\log(2)}{\log(\tau)}}{d^{n-1}} \right) = \lim_{n\to\infty} \left(\frac{\frac{1}{d-1-\epsilon} \frac{\log(2)}{\log(\tau)}}{(n-1)d^{n-2}} \right) = 0,$$

$$\lim_{n\to\infty}\left(\frac{\frac{nd^{n/2}}{d-1-\epsilon}\frac{\log(\tau_*)}{\log(\tau)}}{d^{n-1}}\right)=\lim_{n\to\infty}\left(\frac{\frac{1}{d-1-\epsilon}\frac{\log(\tau_*)}{\log(\tau)}}{(n/2-1)d^{n/2-2}}\right)=0.$$

This shows that every term on the right-hand side of equation (9) is equal to 0 and therefore, equation (9) does not hold. So our assumption that x_n has no primitive prime factor does not hold for sufficiently large n, which proves the theorem. □

4 New results

The results in this section are based on Theorem 3.7 and its proof. They were obtained through attempting to prove Theorem 3.7 with the assumption of weaker versions of the abc-conjecture. Furthermore, we unexpectedly uncover a relation between the presence of infinitely many primitive prime factors in the orbits of some polynomial and the number of linear factors in the polynomials obtained by applying Lemma 2.11 to said polynomial.

4.1 A restriction on the weak abc-conjecture

Theorem 3.7 from the previous subsection can be proven using the weak abc-conjecture with an additional restriction as shown below.

Theorem 4.1. *Suppose $f(x) \in \mathbb{Z}[x]$ has no repeated roots and is of degree $d \geq 2$, and 0 and x_0 both have wandering orbits under the map $x \to f(x)$. Let D be the degree of the polynomials obtained by applying Lemma 2.11 to the polynomial $F(x,y) = y^{d+1}f(x/y)$. Assume the weak-abc conjecture holds for some $0 < \gamma < \frac{d-1}{D}$. Then x_n has a primitive prime factor for every sufficiently large n.*

Proof. The proof of this theorem is essentially the same as the proof of Theorem 3.7, with $\gamma_* = D\gamma$ substituted for ϵ. This results in the following inequality, similar to (9),

$$1 \ll_f \lim_{n\to\infty}\left(\frac{\frac{n}{d-1-\gamma_*}\frac{\log(2)}{\log(\tau)}+\frac{nd^{n/2}}{d-1-\gamma_*}\frac{\log(\tau_*)}{\log(\tau)}-\frac{\log(\delta_n)}{\log(\tau)}-\frac{\log(\alpha)}{\log(\tau)}}{d^{n-1}}\right).$$

We can show that this inequality does not hold for large n in the same way as in the proof of Theorem 3.7, thereby proving the result. □

Note that a rather strong constraint on γ is necessary for the theorem to hold. Namely, it follows from Corollary 2.16.1 that, if $\gamma_* > d-1$,

$$|x| \gg_f \mathrm{Rad}(f(x))^{\frac{1}{d-1-\gamma_*}}.$$

For every $x \in \mathbb{Z}\backslash\{-1,0,1\}$, the right-hand side is less than or equal to 1, while the left-hand side is greater than 1 and, as a result, the inequality holds for

all sufficiently large n. Thus, the assumption that the orbit does not contain infinitely many primitive prime powers would not lead to a contradiction.

In the case where $\gamma_* = d - 1$, the inequality resulting from Corollary 2.16.1 is

$$1 \ll_f \mathrm{Rad}(f(x)).$$

This is a trivial statement providing no useful information, since $\mathrm{Rad}(x) \geq 1$ for every $x \in \mathbb{Z}\backslash\{0\}$. Introducing $|x_n|$ into this inequality would imply introducing it into the left-hand side and into the right-hand side. Therefore, the application of Lemma 3.6 would no longer result in finding a contradiction. Thus, this theorem requires the additional constraint, introduced above, on the weak abc-conjecture.

In Subsection 3.3, it was stated that the key to proving Theorem 3.7 is to show that the orbits grow too fast to contain finitely many primitive prime factors. This is what leads to this additional assumption on the weak abc-conjecture. The magnitude of the powers of the prime factors present in the orbit must be bound in order for the theorem to hold. The required strength of the bound is correlated to the rate of growth of the orbit (order of the polynomial when n is large). This bound is obtained through the application of the weak abc-conjecture. Therefore, the additional restriction on the weak abc-conjecture is dependent on the order of the polynomial. The larger the order of the polynomial, the weaker the required assumption becomes.

4.2 Applying the exponential bound

Theorem 3.7 cannot be proven by applying the currently best known bound, which was introduced in Theorem 2.7. Applying Corollary 2.18.1 in the same fashion as we applied Corollary 2.16.1 in the proof of Theorem 3.7, yields

$$|x_{n-1}| \ll_f \exp\Big(\frac{k}{D}|x_{n-1}|^{\frac{D+1-\deg(f)}{3}}\mathrm{Rad}(x_n)^{\frac{1}{3}} \cdot \log(|x_{n-1}|^{D+1-\deg(f)}\mathrm{Rad}(x_n))^3\Big). \quad (10)$$

Note that in inequality (10),

$$\frac{k}{D}\,\mathrm{Rad}(x_n)^{\frac{1}{3}}\log(|x_{n-1}|^{D+1-\deg(f)}\mathrm{Rad}(x_n))^3 > \frac{k}{D}\log(2|x_{n-1}|^{D+1-\deg(f)})^3 > 0$$

for large enough n (such that $|x_n| \geq 2$) and this term is monotonically increasing for increasing $|x_n|$. Moreover $D+1-\deg(f) \geq 0$. Therefore, (10) can be written as

$$|x_{n-1}| \ll_f \exp(\ell_n |x_{n-1}|^{\frac{D+1-\deg(f)}{3}}),$$

for some increasing sequence of $\ell_n > 0$ which depends on f, n and k. This inequality obviously holds for large n whenever $\deg(f) < D + 1$, as $e^{|x_n|}$ grows much faster than $|x_n|$.

When $\deg(f) = D + 1$, the inequality becomes

$$|x_{n-1}| \ll_f \exp(k \operatorname{Rad}(x_n)^{\frac{1}{3}} \log(\operatorname{Rad}(x_n))^3/D). \tag{11}$$

If the x_n contain no primitive prime factors for every $n > N \in \mathbb{N}$, then $\operatorname{Rad}(x_n) \leq \operatorname{Rad}(\prod_{i=1}^{N} x_i)$. Therefore, the right-hand side is bounded, while the left-hand side is not. So, if $\deg(f) = D + 1$, we can prove that the orbits contain infinitely many primitive prime factors, but not that every element contains a primitive prime factor. Thus we have shown the following result to be true.

Theorem 4.2. *Suppose $f(x) \in \mathbb{Z}[x]$ has no repeated roots and is of degree $d = D + 1 \geq 2$, where D is the degree of the polynomials obtained by applying Lemma 2.11 to the polynomial $F(x, y) = y^{d+1} f(x/y)$. Let 0 and x_0 both have wandering orbits under the map $x \to f(x)$. The orbit of x_0 contains infinitely many primitive prime factors.*

Applying Lemma 3.6 and Corollary 3.6.1 to (11) would not increase the strength of this theorem, as this would lead to

$$\delta_n \alpha \tau^{d^{n-1}} \ll_f \exp(\frac{k}{D}(2^n \tau_*^{nd^{n/2}})^{1/3} \log(2^n \tau_*^{nd^{n/2}})^3).$$

The right-hand side of this inequality contains n in a triple exponential, while the left-hand side only contains a double exponential. Therefore, this inequality holds for large n.

We can find the intuitive reason for Theorem 4.2 by looking at the proof of Theorem 2.16. In that proof, we used that

$$a(m, n)b(m, n)c(m, n) = F(m, n)G(m, n).$$

However, because $\deg(abc) = D + 2 = deg(F)$, $G(m, n) = 1$, which means that $\operatorname{Rad}(abc) = \operatorname{Rad}(F)$. Substituting this into the bound from Theorem 2.7 and applying the lower bound

$$H^D \ll_f \max\{|a(m, n)|, |b(m, n)|\},$$

where $H = \max\{|m|, |n|\}$, gives the desired result.

In order to find examples of polynomials $f(x)$ with the properties mentioned in Theorem 4.2, we can search for homogeneous polynomials $a(x, y), b(x, y), c(x, y) \in \mathbb{Z}[x, y]$ with degree D and a total of $D+2$ distinct linear factors, one of which must be y. If none of them contain y as a linear factor, then there does not exist a polynomial $f(x) \in \mathbb{Z}[x]$ such that $F(x, y) = y^{d+1} f(x/y)$, where $F(x, y)$ is the product of the distinct linear factors. To see this, note that in this case, every monomial in $y^{d+1} f(x/y)$ contains y, while $F(x, y)$ would contain a monomial without y. If we have found an example of polynomials with these properties, then

$$a(x, y)b(x, y)c(x, y) = k\Big(y \prod_{i=1}^{D+1} (x - \beta_i y)\Big)\Big(\prod_{j=1}^{n} p_j(x, y)\Big),$$

where $k, \beta_i \in \mathbb{Z}$ and where p_j are irreducible nonlinear polynomials with $\sum_{j=1}^{n} \deg(p_j) = 3D - D + 2 = 2D + 2$. Now

$$y^{d+1} f(x/y) = F(x, y) = ky \prod_{i=1}^{D+1} (x - \beta_i y),$$

provides an example of an f to which Theorem 4.2 applies. Note that f can be multiplied by a scalar to obtain a polynomial with strictly integer coefficients if necessary. The above implies that we can find a polynomial to which Theorem 4.2 applies whenever we find homogeneous polynomials $a(x, y)$, $b(x, y)$ and $c(x, y)$ as described above. If there are infinitely many of these triplets, than there are likely infinitely many polynomials to which Theorem 4.2 applies.

For example, the polynomials $a(x, y) = 2y(4x - 5y)$ and $b(x, y) = (3y - 4x)(2x + 3y)$ both contain two linear factors, but $c(x, y) = a(x, y) + b(x, y) = -8x^2 + 2xy - y^2$ contains no real linear factors. If we take the product of the distinct linear factors in a, b, c, then we obtain

$$F(x, y) = -64x^3y + 32x^2y^2 + 132xy^3 - 90y^4,$$

and then

$$f(x) = F(x, 1) = -64x^3 + 32x^2 + 132x - 90.$$

Note that $\deg(a) = \deg(b) = \deg(c) = 2 = \deg(f) - 1$ and the orbit of 0 is wandering, so this is indeed an example of a polynomial to which we can apply Theorem 4.2. Therefore, a wandering orbit under $f(x)$ contains infinitely many primitive prime factors.

The method, applied to find this example, involved generating random homogeneous polynomials $a(x, y)$ and $b(x, y)$ of degree $D \geq 2$ and the subsequent construction of $c(x, y) = a(x, y) + b(x, y)$. Afterwards, a root finding algorithm was used on the three polynomials to check for the existence of linear factors. If the number of distinct linear factors is $D + 2$, then the product of these linear factors is a polynomial to which Theorem 4.2 applies. If an infinite number of pairs $a(x, y)$ and $b(x, y)$ exists, such that the product of $a(x, y)$, $b(x, y)$ and $c(x, y) = a(x, y) + b(x, y)$ contains $D + 2$ linear factors, then this method can be used for constructing infitely many examples.

5 Summary

In this thesis, we have examined the orbits of integers under polynomials with integer coefficients. The objective was to obtain an understanding of the methods for constructing infinite sequences of distinct coprimes, presented by Granville [Gr17]. It follows from Granville's results that we know methods for constructing such sequences when the orbit of 0 under a polynomial map is preperiodic. However, if the orbit of 0 is wandering, we do not yet know for certain whether the wandering orbits of a polynomial contain infinitely many primitive primes.

The validity of Granville's result on such polynomials depends on the validity of the abc-conjecture.

After obtaining a thorough understanding of Granville's results, we attempted to expand upon his result regarding polynomials under which 0 is wandering. By applying the weak abc-conjecture, we determined an upper bound for γ, which is dependent on the order of the polynomial. This upper bound tells us how strong the bound in the weak abc-conjecture must be for wandering orbits to contain infinitely many primitive prime factors. Moreover, we applied the exponential bound, proven by Stewart and Yu [SY01]. This revealed the existence of polynomials under which 0 has a wandering orbit, for which we can already prove that the wandering orbits contain infinitely many primitive prime factors.

References

[MB11] U.C. Merzbach, C.B. Boyer, *A History of Mathematics*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2011.

[Beu15] F. Beukers, *Getaltheorie - Een inleiding*. Epsilon Uitgaven, Amsterdam, 2015.

[AZ10] M. Aigner, G.M. Ziegler, *Proofs from THE BOOK*. Springer-Verlag, Berlin, Heidelberg, 2010.

[Fu55] H. Furstenberg, *On the infinitude of primes*, Amer. Math. Monthly. **62** no. 5 (1955), 353.

[Gr17] A. Granville, *Using Dynamical Systems to Construct Infinitely Many Primes* (2017), arXiv:1708.06953.

[Ha96] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques.* (French) Bull. Soc. Math. France 24 (1896), 199-220.

[Va96] C.J. de la Vallée Poussin, *Recherches analytiques la théorie des nombres premiers*. Ann. Soc. scient. Bruxelles 20, 183-256, 1896.

[Oe88] J. Oesterlé. *Nouvelles approches du "théorème" de Fermat.* (French) Séminaire Bourbaki, Vol. 1987/88. Astérisque No. 161-162 (1988), Exp. No. 694, 4, 165–186 (1989).

[SY01] C.L. Stewart, K. Yu, *On the abc-conjecture, II*. Duke Math. J. **108** (2001), no. 1, 169–181.

[Ba07] A.D. Barry, *The abc conjecture and k-free numbers* (Master's thesis, Mathematisch instituut, Universiteit Leiden, Leiden, Nederland)

[Hu92] A. Hurwitz, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich.* (German) Math. Ann. **41** no. 3 (1892), 403–442.

[Mi95] R. Miranda, *Algebraic Curves and Riemann Surfaces*, Amer. Math. Soc., Providence, Rhode Island, 1995.

[Bel79] G.V. Belyĭ, *Galois extensions of a maximal cyclotomic field*. (Russian) Izv. Akad. Nauk. SSSR Ser. Mat. **43** no. 2 (1979), 267-276.

[Gr98] A. Granville, *ABC allows us to count squarefrees*. Internat. Math. Res. Notices. no. 19 (1998), 991-1009.

[La02] S. Lang. *Algebra*. Springer-Verlag, New-York, 2002.

[Po75] J.M. Pollard, *A Monte Carlo method for factorization.* Nordisk Tidskr. Informationsbehandling (BIT) 15 (1975), no. 3, 331-334.