How many primes are there in a Polinomial sequences?

Javier San Martín Martinez

Seminario Diagonal

Lisboa, 1 October 2025

Motivation

Dirichlet Theorem on Arithmetic progressions

Let $a, d \in \mathbb{Z}_{>0}$ coprimes then the sequences, $x_n = a + dn$ contains infinitely many primes.

For example for $a = 1, d = 2$ we recover the fact that there are infinitely many primes. For $a = 1$ and $d = 4$ we recover the fact that there are infinitely many primes of the form $p \equiv 1 \bmod 4$. Reciprocally there are infinitely many $p \equiv 3 \bmod 4$. Later we will see much more can be said...

Talk Goal

We want to study primes in sequences of the form:
$x_0 = x, x_n = f(x_{n-1})$. f will be in general a cubic polynomial.

Example 1

$x_0 = 2, f = x^3$. Then $x_1 = 8, x_2 = 512, ..., x_n = 2^{3^n}$. Clearly in this case just 2 divides an element of the sequences, so is a rather boring example, in fact for any x_0 this is the case, this is nonetheless insightful since in general very "few" will divide elements for this sequences for f cubic.

Example 2

Let $x_0 = 3, f = -2z^3 + 3z^2, x_1 = -27, x_2 = 41553, ..., x_n =$???.
This already hints that even with small initial values and easy polynomials this method dose not allow a elemental study.

Recall Galois Theory

Motivation: Galois theory studies the symmetries of solutions to polynomial equations.

Example

In the complex number we can consider conjugation that send $a + bi \to a + b(-i)$.

Definition

We define a field extension $K/\mathbb{Q}$ as $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$ this is the smallest field containing the complex numbers $\alpha_1, ..., \alpha_n$.

Example

$\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$

Recall Galois Theory

Definition

We define the Galois group $Gal(K/\mathbb{Q})$ as the automorphism of K, this is the bijection from K to K. This elements are the symetries we were talking about before.

Remark

Any automorphism restricted to $\mathbb{Q}$ is the identity.
If τ is an automorphism then $\tau(f(\alpha)) = f(\tau(\alpha))$

Notice that If K is constructed adding the roots of a polynomial f then the automorphism is given by the image of the roots and by remark those are also roots so it defines an element of the symmetric group in n letters being n the degree of the polynomial.

Recall Galois Theory

We give some examples:

Example 1

We come back to $\mathbb{Q}(i)$ which can be understand by taking the roots of x^2+1. Hence the Galois groups sits inside S_2 and indeed conjugating defines an automorphism then we have discover is S_2.

Its far from being true that all elements of the symmetric group defines an automorphism.

Example 2

We consider x^n-1 which is a field generated by a $n-$th root of unity(if you prefer $e^{\frac{2\pi i}{n}}$). The fact is that $Gal(\mathbb{Q}(e^{\frac{2\pi i}{n}})) = (\mathbb{Z}/n\mathbb{Z})^\times$. Which is much smaller than S_n.

Reinterpretation of Chebotarev Density Theorem

Cycle data of elements in S_n

We define the cycle data of an element $\sigma \in S_n$. We decompose $\sigma = \prod \sigma_i$ with σ_i disjoint cycles. Then we define the cycle data of σ as a tuple of the length of σ_i in decreasing order, i.e. $(l(\sigma_{i_1}, l(\sigma_{i_2}), ..., l(\sigma_{i_j}))$, and $l(\sigma_{i_k}) \geq l(\sigma_{i_{k+1}})$.

Cycle data of a polynomial

Given $f \in K[x]$, we can factor f into irreducible polynomials $f = \prod f_i$. The cycle data of f is the degree of the irreducible factors in decreasing order.

Reinterpretation of Chebotarev Density Theorem

Example

(1,2)(3)	*Cycle data 2,1*
(1,2,3)	*Cycle data 3*
(1)(2)(3)	*Cycle data 1,1,1*
(x)(x-1)(x-2)	*Cycle data 1,1,1*
$(x^2 + 1)(x - 2)$	*Cycle data 2,1*
$(x^3 - 2)$	*Cycle data 3.*

Reinterpretation of Chebotarev Density Theorem

Chebotarev density theorem

Let $\mathbb{Q} \subset K = \mathbb{Q}[x]/(f)$ a Galois extension. Then, the frequencies of the cycle data of the elements in $G = Gal(K/\mathbb{Q})$ coincide with the frequencies of primes in $\mathbb{Z}$ for which f splits with that cycle data in $\mathbb{F}_p$.

Example

Given the polynomial $f = x^3 + x + 1$, then $\Delta(f) = -31$ as it is not a square $\mathrm{Gal}(f) = S_3$ and hence we know that:

1. For $\frac{1}{6}$ of the primes f splits in $\mathbb{F}_p$.
2. For $\frac{1}{3}$ of the primes f remains irreducible.
3. For $\frac{1}{2}$ of the primes $f = f_1 f_2$.

Primes congruent to 1 mod 4

Theorem

There are infinite primes p such that $p \equiv 1$ mod 4 and $p \equiv 3$ mod 4. Moreover, the densities of both sets of primes equal $\frac{1}{2}$.

Proof.

Blackboard □

Surprising fact

Dirichlet theorem on primes in arithmetic progression can be proven with Chebotarev Density theorem using slightly more involved techniques.

Automorphism of regular rooted trees

Definition: Regular rooted tree

A $d-$regular rooted tree $\mathcal{T}$ is a tree where all vertices but the root have $d+1$ neighbours. The root has d neighbours.

We can define a distance between two vertices v, u as the minimum edges needed to go from v to u. This allows us to define the levels of the tree. We say a vertex is in the nth level if it is a distance n from the root.

Automorphism of regular rooted trees

Definition: Regular rooted tree

A $d-$regular rooted tree $\mathcal{T}$ is a tree where all vertices but the root have $d+1$ neighbours. The root has d neighbours.

We can define a distance between two vertices v, u as the minimum edges needed to go from v to u. This allows us to define the levels of the tree. We say a vertex is in the nth level if it is a distance n from the root.
Another point of view:
Let X the alphabet $X = \{0, 1, ..., d-1\}$. Then we consider the monoid with juxtaposition X^*. Then a vertex in $\mathcal{T}_n$ can be interpret as a word in X^n.

Recall tree automorphism

Definition group automorphism of a regular rooted tree

We define the group $(\mathrm{Aut}(\mathcal{T}), \cdot)$ as the underlying set the automorphism (automorphism in the set-theoretical sense preserving incidence and the root) with the operation $\cdot$ which is composition, i.e. $(f \cdot g)(u) = g(f(u))$.

$$\varprojlim \mathrm{Aut}(\mathcal{T}_n) \cong \mathrm{Aut}(\mathcal{T});$$
$$\{\sigma_n\} \to \sigma$$

Arboreal representations

Aim

For $f \in K[x]$ we study the Galois group of $f \circ \ldots \circ f := f^n$ for different n, i.e. determine $\varprojlim \mathrm{Gal}(f^n)$.

Arboreal representations

Aim

For $f \in K[x]$ we study the Galois group of $f \circ \ldots \circ f := f^n$ for different n, i.e. determine $\varprojlim \mathrm{Gal}(f^n)$.

This could serve for various purposes, among others:

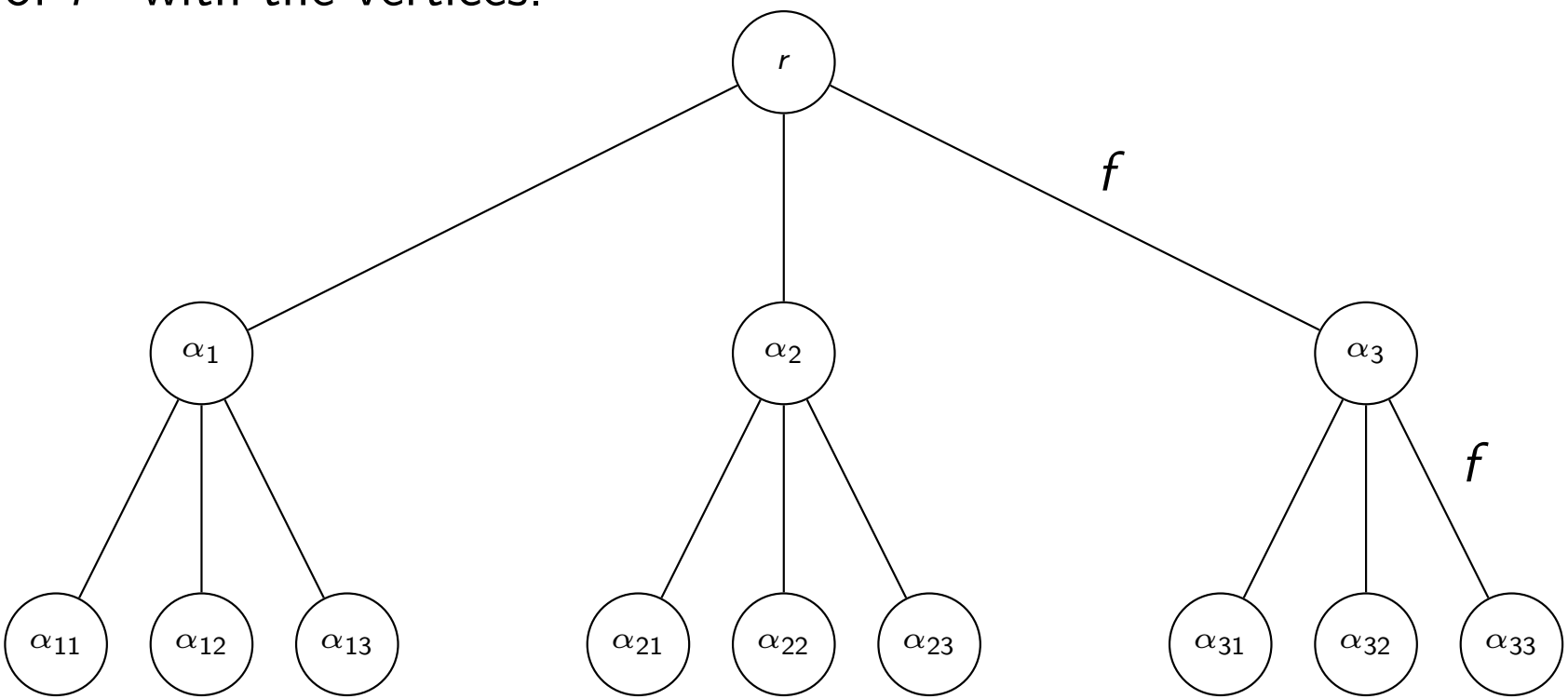
1. Deduce density of primes appearing in sequences of the form $x_n = f(x_{n-1})$.
2. Better knowledge of absolute Galois group $G_{\mathbb{Q}}$ over rationals.

Arboreal representation

We consider a regular $d-$regular rooted tree and identify the roots of f^n with the vertices.

Arboreal representation

We consider a regular $d-$regular rooted tree and identify the roots of f^n with the vertices.



Arboreal representations

$$\mathrm{Gal}_{\mathbb{Q}}(f^n) \leq \mathrm{Aut}(\mathcal{T}_n) \leq S_{d^n}$$

Applying inverse limits we get:

$$\varprojlim \mathrm{Gal}_{\mathbb{Q}}(f^n) \leq \mathrm{Aut}(\mathcal{T}).$$

Arboreal representations

$\mathrm{Gal}_{\mathbb{Q}}(f^n) \leq \mathrm{Aut}(\mathcal{T}_n) \leq S_{d^n}$

Applying inverse limits we get:

$$\varprojlim \mathrm{Gal}_{\mathbb{Q}}(f^n) \leq \mathrm{Aut}(\mathcal{T}).$$

This is an incredible improvement in the size of the groups we work with since $|\mathrm{Aut}(\mathcal{T}_n)| = (d!)^{\frac{d^n-1}{d-1}}, |S_{d^n}| = d^n! \sim \sqrt{2\pi d^n}(\frac{d^n}{e})^{d^n}$.

Arithmetic Interlude

We are going to hint how information on the Galois group of f^n can help us deducing the density of primes in sequences.

Definition

We define $G_{fix,n}$ as the elements of G that fix a leave in T_n.

We claim that if we can prove that the limit of $|G_{fix,n}|/|G_n| \to 0$ as $n \to \infty$. Then we can prove that in the sequences $x_n = f(x_{n-1})$ there are a zero density set of primes.

Markov model for cubics: Initial point

Markov model

Boston and Jones proposed a Markov model for factorization of quadratic polynomials which Goksel used to construct groups for those polynomials. We give an analogue of the construction for cubics.

Boston, Jones and Goksel's idea

We can study factorization over $\mathbb{F}_q$ and, with that, construct a group.

Markov Model for cubics

Critical points

Let $f \in K[x]$, we call γ a critical point of f if $f'(\gamma) = 0$.

Orbit of a point

Let $f \in K[x], \alpha \in \overline{K}$. We define the orbit of α as the set of points $\{f^n(\alpha)\}$.

We then say f is post-critical Finite(PCF) if the orbit of all critical points is finite.

Combined critical orbit for cubics

Let $f \in K[x]$ a cubic polynomial. We defined the combined critical orbit of f as $\{\{f(\gamma_1), f(\gamma_2)\}, ..., \{f^j(\gamma_1), f^j(\gamma_1)\}\}$

Markov model for cubics

Theorem on factorization cubics

Let $f \in \mathbb{F}_q[z]$ a cubic and g a generic polynomial. Let γ_1, γ_2 the critical points of f.Suppose further that g is irreducible. Then:

- If $(-3)^{\deg(g)} g(f(\gamma_1))g(f(\gamma_2))$ is a square then $g \circ f$ may remain irreducible or split in three factors of the same degree.
- If $(-3)^{\deg(g)} g(f(\gamma_1))g(f(\gamma_2))$ is not square then $g \circ f$ factors into an irreducible polynomial of degree $2\deg(g)$ and another factor of degree $\deg(g)$.

Markov model for cubics

Small technical remark

We are going to "ignore" the term $(-3)^{\deg(g)}$. This makes the model easier as then we just care about $g(f^n(\gamma_1))g(f^n(\gamma_2))$.

Markov model for cubics

Small technical remark

We are going to "ignore" the term $(-3)^{\deg(g)}$. This makes the model easier as then we just care about $g(f^n(\gamma_1))g(f^n(\gamma_2))$.

Example

Consider the polynomial $f = -2(z+3)^3 + 3(z+3)^2 - 3$. We compute the critical point and obtain $-3, -2$. We have $f(-3) = -3$ and $f(-2) = -2$. Moreover, $f^n(-2) = -2, f^n(-3) = -3$.

Markov Model for cubics

Strategy

We want to predict the factorization of f^n. We want to given the factorization of f^{n-1} deduce the factorization of f^n using our theorem. If:

$$f^{n-1} = h_1 h_2 \cdot \ldots \cdot h_m$$

Then:

$$f^n = h_1(f)h_2(f) \cdot \ldots \cdot h_m(f).$$

Where the factorization of $h_i(f)$ depends by the theorem on $h_i(-2)h_i(-3)$ being a square or not. So we are going to save the factors and for each factor if $h_i(-2)h_i(-3)$ is a square or not.

Markov Model for cubics

Attaching types

Now, given g a polynomial, we attach a "type". We attach s if $g(-3)g(-2)$ is a square and n if not. If $\deg(g) = m$. Then we write:

$$[s, m] \textit{ if } g(-3)g(-2) \textit{ is a square or } [n, m] \textit{otherwise.}$$

We moreover can juxtapose types if our polynomial $g = g_1 g_2 g_3$ then we have the type:

$$[s, m_1][s, m_2][n, m_3].$$

That means $g_1(-3)g_1(-2)$ and $g_2(-3)g_2(-2)$ are squares, but $g_3(-3)g(-2)$ is not a square.

Markov Model for cubics

Remark

Given our polynomial $f = -2(z+3)^3 + 3(x+3)^2 - 3$, we have $z \circ f = f$. This would read as following:

$$z \circ f = z(f) = f.$$

We recall that given g if $g(-2)g(-3)$ is a square, then $g \circ f$ splits or is irreducible and if it is not a square, $g \circ f = g_1 g_2$.

Initial setting

Our $g = z$. Then $g(-2)g(-3) = 6$. For the primes such that 6 is a square in $\mathbb{F}_p$ we have the type $[s, 1]$ and $[n, 1]$ for those which are not squares.Moreover, both happen for half of the primes, and we write:

$$[[s, 1], \frac{1}{2}], [[n, 1], \frac{1}{2}].$$

Markov Model for cubics

We want to obtain factorization of f given the data of $f^0 = z$ or, in general, factorization of f^n given the data of f^{n-1}. We proposed that:

$$[n, k] \xrightarrow{\circ f} [[n, 2k][s, k], \frac{1}{2}], [[n, k][s, 2k], \frac{1}{2}]$$

$$[s, k] \xrightarrow{\circ f} [[s, 3k], \frac{2}{3}], [[s, k][s, k][s, k]\frac{1}{12}], [[s, k][n, k][n, k], \frac{1}{4}]$$

Markov Model for cubics

With this, we can give the following data for f :

$$[[s,3],\frac{1}{3}],[[s,1]^3,\frac{1}{24}],[[s,1][n,1]^2,\frac{1}{8}],[[n,2][s,1],\frac{1}{4}],[[s,2][n,1],\frac{1}{4}].$$

In this case we have $\frac{1}{3}$ of $3-$cycles $\frac{1}{2}$ of $2,1-$cycles and $\frac{1}{6}$ of $1,1,1-$cycles. This group coincide with S_3.

Markov Model for cubics

With this, we can give the following data for f :

$$[[s,3],\frac{1}{3}],[[s,1]^3,\frac{1}{24}],[[s,1][n,1]^2,\frac{1}{8}],[[n,2][s,1],\frac{1}{4}],[[s,2][n,1],\frac{1}{4}].$$

In this case we have $\frac{1}{3}$ of $3-$cycles $\frac{1}{2}$ of $2,1-$cycles and $\frac{1}{6}$ of $1,1,1-$cycles. This group coincide with S_3.
We can do this iteratively.

Fact

We can construct a family of groups satisfying the cycle data on each level. We conjecture that our groups M_n contain the Galois group of f^n as subgroups and in some cases coincide.

Markov Model for cubics

In fact, these groups also work for the polynomials:

$$-(z+a)^3+\frac{3}{2}(z+a)^2+1-a, -4(z+a)^3+6(z+a)^2-\frac{1}{2},$$
$$2(z+a)^3-3(z+a)^2+1-a, 4(z+a)^3-6(z+a)^2+\frac{3}{2}-a,$$
$$(z+a)^3-3(z+a)^2-a.$$

Markov Model for cubics

In fact, these groups also work for the polynomials:

$$-(z+a)^3+\frac{3}{2}(z+a)^2+1-a, -4(z+a)^3+6(z+a)^2-\frac{1}{2},$$
$$2(z+a)^3-3(z+a)^2+1-a, 4(z+a)^3-6(z+a)^2+\frac{3}{2}-a,$$
$$(z+a)^3-3(z+a)^2-a.$$

We can also do something similar for polynomials with critical orbit of length 2. For example, the following:

$$-2(z+a)^3+3(z+a)^2+\frac{1}{2}-a, -\frac{1}{28}(z+a)^3-\frac{3}{4}(z+a)+7/2-a.$$

Arithmetic application

Theorem

For the polynomials satisfying the model mentioned, we have that the density of primes appearing in the sequence is zero for the sequences:

$$a_n = f(a_{n-1}), a_0 \neq \gamma_1, \gamma_2.$$

The end

Thanks for your attention
Questions?