Rose-Hulman Undergraduate Mathematics Journal

Volume 22
Issue 1

Article 10

Irreducibility and Galois Groups of Random Polynomials

Hanson Hao
Stanford University, hhao@stanford.edu

Eli Navarro
Stanford University

Henri Stern
Stanford University

Irreducibility and Galois Groups of Random Polynomials

Cover Page Footnote

We would like to thank our project mentor, Max Xu, for introducing us to this problem and providing us with the necessary background material. We are grateful for his encouragement throughout the project and for his many valuable insights. We would like to thank both him and Pawel Grzegrzolka for his helpful comments on our paper. The first author would like to thank Keith Conrad for his proof of Theorem 4.7 and other assistance on the results of Section 4. Finally, we would like to thank Pawel Grzegrzolka and the rest of the Stanford Undergraduate Research Institute in Mathematics (SURIM) staff for setting up this program, as well as for their flexibility and support during a very unusual summer.

Rose-Hulman Undergraduate Mathematics Journal

Volume 22, Issue 1, 2021

Irreducibility and Galois Groups of Random Polynomials

By *Hanson Hao*, *Eli Navarro*, and *Henri Stern*

Abstract. In 2015, I. Rivin introduced an effective method to bound the number of irreducible integral polynomials with fixed degree d and height at most N. In this paper, we give a brief summary of this result and discuss the precision of Rivin's arguments for special classes of polynomials. We also give elementary proofs of classic results on Galois groups of cubic trinomials.

1 Introduction

Suppose $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ is a polynomial with integral coefficients a_i chosen uniformly and independently at random from $[-\mathrm{N}, \mathrm{N}]$. It is natural to ask for the probability that $f(x)$ is reducible over $\mathbb{Z}$ and the probability that the Galois group of $f(x)$ is the full symmetric group S_d. The first question was resolved by R. Chela in 1963 [1]:

Theorem 1.1. Fix a degree $d \geq 3$. Suppose $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ is a polynomial with integral coefficients a_i chosen uniformly and independently at random from $[-\mathrm{N}, \mathrm{N}]$. Then as N tends to infinity, the probability that $f(x)$ is irreducible is $\frac{(1+o(1))c_d}{\mathrm{N}}$, where c_d is a constant depending only on d.

The second question, in particular the following 1936 conjecture by van der Waerden [8], is still unresolved.

Conjecture 1.2. For a random polynomial $f(x)$ as in Theorem 1.1, as N tends to infinity,

$$\Pr(\mathrm{Gal}(f(x)) = \mathrm{S}_d) \geq 1 - \mathrm{O}(\mathrm{N}^{-1+\epsilon})$$

for any $\epsilon > 0$.

Mathematics Subject Classification. 11C08, 11R32

Keywords. Number Theory, Probability, Random Polynomials, Galois Theory

S. Chow and R. Dietmann [2] proved van der Waerden's conjecture for random polynomials of degrees 3 and 4 in 2018, but the general case is still open.

In 2015, I. Rivin showed the following using a very streamlined argument:

Theorem 1.3. Consider random polynomials $f(x)$ of degree d as in Theorem 1.1. Then the probability that $f(x)$ is reducible is at most $O\left(\frac{\log N}{N}\right)$.

In this paper, we study the probability that a random polynomial $f(x)$ is reducible over $\mathbb{Z}$ using Rivin's argument. After providing a sketch of his results (with slight variations on his proofs) in Section 2, we apply Rivin's method to more restricted models in Section 3. In particular, we will define $P_{d,N} = \{x^d + ax^m + b : 0 < m < d; a, b \in [-N, N]\}$, the set of trinomials of degree d with height bounded by N, and apply Rivin's versatile argument to prove analogous results about the irreducibility of random polynomials from this set. In particular, we show:

Theorem 1.4. The probability that a randomly chosen polynomial from $P_{d,N}$, for fixed d, is reducible is at most $O(\frac{\log N}{N})$. When d is even, this bound is tight; that is, the probability that a randomly chosen polynomial from $P_{d,N}$ is reducible is at least $\Omega\left(\frac{\log N}{N}\right)$.

We conclude the paper in Section 4 with a discussion of similarly restricted models of Conjecture 1.2. We will prove the following classic result (see [3]) on the Galois groups of cubic integer-coefficient trinomials, using only elementary techniques:

Theorem 1.5. $p(x) = x^3 + c_1 x \pm 1$ has Galois group S_3 unless $c_1 = 0, -2, -3$. Moreover, if q is a rational prime, then $p(x) = x^3 + c_1 x \pm q$ does not have Galois group S_3 for only finitely many integers c_1.

2 Rivin's Irreducibility Results

The main tool used in Rivin's argument is a slight variant of the Schwartz-Zippel bound.

Lemma 2.1 (Schwartz-Zippel bound)**.** *Let* V *be a variety defined over* $\mathbb{Z}$*. Then, the number* $|V(N)|$ *of* $\mathbb{Z}$*-points of* V *of height bounded above by* $N > 1$ *is bounded by*

$$|V(N)| \ll_M N^{dim(V)}.$$

Proof. See Lemma 1.2 in [5]. □

Proof of Theorem 1.3. Consider

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0,$$

and suppose that it was reducible as $f(x) = g(x)h(x)$ where

$$g(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0.$$

We begin by fixing a_0, but we continue to allow $\{a_1,\ldots,a_{d-1}\}$ to vary in $[-\mathrm{N},\mathrm{N}]$.

Next, we take $\{r_1,\ldots,r_d\}$ to be the set of roots of $f(x)$. It is evident that $a_0 = \prod_{i=1}^{d} r_i$. We also have that $b_0|a_0$. Furthermore, we have that the roots of $g(x)$ are some $k-$subset of the roots of $f(x)$ and therefore b_0 equals the product of some $k-$subset of the roots of $f(x)$. Expressed another way, we have that

$$\prod_{1\le i_1\le\cdots\le i_k\le d}(r_{i_1}r_{i_2}...r_{i_k}-b_0)=0.$$

Because the product is fixed under all automorphisms of the roots r_i (with b_0 fixed), it is a symmetric polynomial. Hence it can be expressed as a polynomial in the elementary symmetric polynomials of the roots of f, which are precisely the coefficients of f. As such, there exists some polynomial g_k in the coefficients of $f(x)$ such that

$$g_k(a_1,\ldots,a_{d-1})=\prod_{1\le i_1\le\cdots\le i_k\le d}(r_{i_1}r_{i_2}...r_{i_k}-b_0)=0.$$

Note that g_k is in terms of $\{a_1,\ldots,a_{d-1}\}$, since at the beginning of this process, we fixed a_0 as some integer in $[-\mathrm{N},\mathrm{N}]$. With g_k, we have a variety in the coefficients of $f(x)$, so we may now use Lemma 2.1. Before doing so, it is important to show that this variety is non-trivial. In other words, it does not reduce to $0=0$ and the statement $g_k=0$ actually carries significance. A proof of this fact can be found in [4].

We see that the dimension of the variety $g_k=0$ is $d-2$ because we have one equation and $d-1$ unknowns. By Lemma 2.1,

$$|g_k(\mathrm{N})|=\mathrm{O}(\mathrm{N}^{d-2}),$$

where $|g_k(\mathrm{N})|$ is the number of $\mathbb{Z}$-points of the variety $\{g_k=0\}$. This tells us that, given a fixed a_0, there are at most $\mathrm{O}(\mathrm{N}^{d-2})$ reducible polynomials with constant a_0. Thus, the probability that such a polynomial is reducible at most is $\mathrm{O}(1/\mathrm{N})$. We must then account for the variability in b_0. It is well-known that the average number of divisors of $n\in[1,\mathrm{N}]$ tends to $\log\mathrm{N}$. This means that are on average $\log\mathrm{N}$ choices for b_0 given any a_0. Ranging over all nonzero a_0 and the associated $\log\mathrm{N}$ choices for b_0, we have that the probability that a random polynomial is reducible is at most $\mathrm{O}\left(\frac{\log\mathrm{N}}{\mathrm{N}}\right)$.

□

3 Further Discussion of Rivin's Method

It is natural to apply Rivin's counting method, which gives an upper bound on the probability that a random polynomial (selected from some finite set) is reducible, to similar situations. We may ask the following general question:

Question 3.1. When does Rivin's method give a tight upper bound on the number of reducible random polynomials?

Clearly, this is not always the case. From Theorem 1.1 and Theorem 1.3, we see that Rivin's method does not give a tight upper bound for any $d \geq 3$. We now simplify our discussion a bit and consider the strength of Rivin's method when applied to *random monic trinomials*.

For a fixed degree d, consider the set of trinomials of degree d with height bounded by N:

$$P_{d,N} = \{x^d + ax^m + b : 0 < m < d; a, b \in [-N, N]\}.$$

The size of $P_{d,N}$ is $(d-1)(2N-1)^2 = O(N^2)$. We may ask for the probability that a randomly chosen polynomial from $P_{d,N}$ (with all choices equally likely) is reducible. An immediate lower bound is $\frac{1}{2N+1} = O\left(\frac{1}{N}\right)$, since that is exactly the probability that $b = 0$, and in that case $x^d + ax^m$ is clearly reducible. The same line of argument as in Section 2 gives us the following upper bound:

Theorem 3.2. The probability that a randomly chosen polynomial from $P_{d,N}$ is reducible is at most $O\left(\frac{\log N}{N}\right)$.

In fact, one could say the exact same thing for families of monic polynomials where we fix arbitrary coefficients to (possibly nonzero) constants. Suppose for some fixed degree d and set of non-leading, non-constant coefficients $\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\} \subseteq \{a_1, a_2, \ldots, a_{d-1}\}$, we have $\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\} = \{c_1, \ldots, c_k\}$ for fixed constants $c_1, \ldots, c_k$. Then consider the set

$$Q = \left\{x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 : a_j \in [-N, N]\ \forall j \not\subseteq \{i_1, \ldots, i_k\}\right\}.$$

That is, we vary the coefficients that we didn't fix to one of the constants c_i. Then Rivin's argument tells us that

Theorem 3.3. The probability that a randomly chosen polynomial from Q is reducible is at most $O\left(\frac{\log N}{N}\right)$.

Proof Sketch: We basically repeat the proof of Theorem 1.3. Randomly choose a polynomial $f(x)$ from Q, so that k of the coefficients of f are fixed. As in the proof of Theorem 1.3, if f was reducible as a product gh, then consider all possible constant terms of g, depending on the constant term of f (which is not fixed, by assumption). We can then create an integral variety in the coefficients of f with 1 equation and $d-k-1$ unknowns, which has dimension $d-k-2$. By Lemma 1.7, given a fixed $f(0)$, there are at most $O(N^{d-k-2})$ reducible polynomials in Q with that constant term, giving a probability of $O(1/N)$ for a randomly chosen polynomial in Q with constant $f(0)$ to be reducible. Taking into account the average number of divisors of $f(0)$, we have that the probability of randomly choosing a reducible polynomial from Q is at most $O\left(\frac{\log N}{N}\right)$. □

This shows the versatility of Rivin's argument, since we can usually obtain (quite easily) a reasonably good upper bound on the number of reducible polynomials in some family of polynomials.

We now return to the case of monic trinomials. When d is even, this upper bound is indeed tight:

Theorem 3.4. For even d, the probability that a randomly chosen polynomial from $\mathrm{P}_{d,\mathrm{N}}$ is reducible is at least $\Omega\left(\frac{\log \mathrm{N}}{\mathrm{N}}\right)$.

Proof. Recall that there are $\Omega(\mathrm{N}\log\mathrm{N})$ reducible quadratics of height bounded by N. We briefly sketch the proof of this fact. Note that the desired number is equal to the number of *unordered* pairs of integers (a,b) such that $-\mathrm{N} \le ab \le \mathrm{N}$ and $-\mathrm{N} \le a+b \le \mathrm{N}$, since any such pair (a,b) corresponds to a unique reducible quadratic of height bounded by N, namely $f(x) = (x+a)(x+b)$, and vice versa. Suppose we count the number of such points subject to the constraints $0 < a, b \le \mathrm{N}$. The number of possible points in this case is

$$\frac{1}{2}\left(\sum_{a=1}^{\mathrm{N}} \left\lfloor \frac{\mathrm{N}}{a} \right\rfloor\right) - 1 \sim \frac{\mathrm{N}\log\mathrm{N}}{2},$$

where the approximation comes from dropping the floor function and using the well-known approximation $\sum_{k=1}^{n} \frac{1}{k} \sim \log n$. Note that we divide by 2 since the above sum double-counts each unordered pair (a,b) (once as (a,b) and once as (b,a)), and we subtract 1 since we shouldn't count the pair $(1,\mathrm{N})$. This counts the number of such unordered pairs when a and b are both positive. The same argument holds for the cases $a < 0 < b$, $b < 0 < a$, and $a, b < 0$. Finally, we need to count the number of unordered pairs where at least one of a, b is 0, but there are only $\mathrm{O}(\mathrm{N})$ of those. Summing all the counts together, we get the desired $\Omega(\mathrm{N}\log\mathrm{N})$.

Therefore there are $\Omega(\mathrm{N}\log\mathrm{N})$ reducible trinomials of the form $x^d + ax^{\frac{d}{2}} + b$. For any other m strictly between 0 and d, there are at least $\Omega(\mathrm{N})$ reducible trinomials of the form $x^d + ax^m + b$. Hence there are at least $\Omega(\mathrm{N}\log\mathrm{N}) + (d-2)\Omega(\mathrm{N}) = \Omega(\mathrm{N}\log\mathrm{N})$ reducible trinomials in $\mathrm{P}_{d,\mathrm{N}}$, from which the theorem follows. □

However, when d is odd, there are no obvious symmetries to exploit, and the situation becomes much more difficult. We believe that this lack of symmetry implies that Rivin's upper bound is *not* tight:

Conjecture 3.5. For odd d, the probability that a randomly chosen polynomial from $\mathrm{P}_{d,\mathrm{N}}$ is reducible is (asymptotically) strictly greater that $\Omega\left(\frac{\log \mathrm{N}}{\mathrm{N}}\right)$.

More generally:

Heuristic 3.6. Let P be a set of *similarly structured* monic polynomials of height bounded by N, more specifically, a set of monic polynomials of fixed degree d where a certain subset $\{a_{i_1}, a_{i_2}, \ldots\}$ of the coefficients (i.e. $\{i_1, i_2, \ldots\} \subset \{1, \ldots, d-1\}$) of each $p \in \mathrm{P}$ are fixed (not necessarily to 0), and the rest of the nonconstant coefficients are allowed to vary in $[-\mathrm{N}, \mathrm{N}]$. Assume that the polynomials in P have no *"obvious"* algebraic symmetries. Then Rivin's bound is not tight; in other words, the probability that a randomly chosen polynomial from P is reducible is (asymptotically) strictly greater that $\Omega\left(\frac{\log \mathrm{N}}{\mathrm{N}}\right)$.

4 A Toy Case: Cubic Trinomials

The authors were interested in trinomials of low degree so as to investigate very simplified variants of van der Waerden's Conjecture 1.2. The following Theorem 4.1, Theorem 4.2 and Theorem 4.3 can be found at [3], but we will give original and basic proofs of the first two results that do not rely on any results concerning elliptic curves.

We investigate integer-coefficient polynomials of the form $p(x) = x^3 + c_1 x + c_0$. The discriminant of p is

$$\mathrm{D} = -4c_1^3 - 27c_0^2.$$

Recall that if p is irreducible, its Galois group is completely determined by the value of D. Furthermore, the Galois groups of $x^3 + c_1 x + c_0$ and $x^3 + c_1 x - c_0$ are equal, as the roots of the latter polynomial are negatives of the roots of the former.

The following theorems are proved using only basic number-theoretic techniques:

Theorem 4.1. $p(x) = x^3 + c_1 x \pm 1$ has Galois group S_3 unless $c_1 = 0, -2, -3$. In the first two cases, p is reducible; in the third case, p is irreducible with Galois group A_3.

Theorem 4.2. If q is a rational prime, then $p(x) = x^3 + c_1 x \pm q$ does not have Galois group S_3 for only finitely many integers c_1.

First, the following preliminary lemmas are needed:

Lemma 4.1 (Thue, [6])**.** *Let $f(x, y) \in \mathbb{Z}[x, y]$ be an irreducible homogeneous polynomial in two variables of degree at least 3. Then $f(x, y) = m$ for any fixed $m \in \mathbb{Z} - \{0\}$ has only finitely many solutions.*

Lemma 4.2. *The only integer solutions to*

$$(x + y)^3 - 9x^2 y = 1 \tag{4.1}$$

are $(-1, -1), (1, 0)$, *and* $(0, 1)$.

Proof. Notice that (a, b) is a solution to Equation 4.1 if and only if $(a + b, -a)$ is a solution to $x^3 - 9xy^2 - 9y^3 = 1$. From [7], Appendix B, Equation B.3, the only integer solutions to this equation are $(1, 0), (-2, 1)$, and $(1, -1)$, which gives the result. □

Lemma 4.3. *The only solutions in integers to* $r^2-3r+9=c^3$ *are* $(r,c)=(-3,3);(6,3)$. *In particular,* $c=3$.

Proof. Let (r,c) be a solution to the given equation. We see that $r^2-3r+9=(r+3\omega)(r+3\omega^2)$, where $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ is a primitive cube root of unity. First, we rule out the possibility that $(r+3\omega)$ and $(r+3\omega^2)$ are coprime in $\mathbb{Z}[\omega]$. For if this were the case, they would each be cubes in $\mathbb{Z}[\omega]$, hence,

$$\begin{aligned} r+3\omega &= (a+b\omega)^3 \\ &= a^3+b^3-3ab^2+(3a^2b-3ab^2)\omega \end{aligned}$$

for some integers a,b. Comparing coefficients of ω, we see that $(ab)(a-b)=1$, which has no solutions in integers.

Hence some non-unit $d\in\mathbb{Z}[\omega]$ divides both $r+3\omega$ and $r+3\omega^2$. Then d divides their difference, $3\omega-3\omega^2=6\omega+3$, which has norm 27. Therefore $3|\mathrm{N}(d)$. Since $\mathrm{N}(d)|r^2-3r+9$, we must have $3|r$, so that c is also a multiple of 3. Write $r=3m$ and $c=3n$, so we are now looking for integer solutions to $m^2-m+1=3n^3$. From this we immediately see that $3\nmid m$, $3\nmid n$, and $9\nmid m^2-m+1$.

Therefore we have $(m+\omega)(m+\omega^2)=3n^3=(-1+\omega)(-1+\omega^2)n^3$. Neither factor on the left hand side divides 3 (which has norm 9), so $m+\omega$ divides exactly one of $-1+\omega$ or $-1+\omega^2$ (and $m+\omega^2$ divides the other). Consider the first case, that $m+\omega$ divides $-1+\omega$.

Now, if there was some non-unit d dividing both $(m+\omega)$ and $(m+\omega^2)$, d would divide the difference $\omega-\omega^2=2\omega+1$, which has norm 3, meaning $\mathrm{N}(d)=3$. Therefore $\frac{m+\omega}{-1+\omega}$ and $\frac{m+\omega^2}{-1+\omega^2}$ are coprime in $\mathbb{Z}[\omega]$.

Hence, there exist integers a,b such that

$$\begin{aligned} m+\omega &= (-1+\omega)(a+b\omega)^3 \\ &= (-a^3-b^3-3a^2b+6ab^2)+(a^3+b^3-6a^2b+3ab^2)\omega. \end{aligned}$$

Comparing coefficients of ω, we see

$$a^3+b^3-6a^2b+3ab^2=(a+b)^3-9a^2b=1. \tag{4.2}$$

From Lemma 4.2, we know all the possible values of a and b; in each case, $m=-a^3-b^3-3a^2b+6ab^2=-1$. This means that the only solution for the first case is $m=-1$.

In the second case, $m+\omega$ divides $-1+\omega^2$, so that $\frac{m+\omega}{-1+\omega^2}=\frac{m+\omega}{-2-\omega}$ is a cube in $\mathbb{Z}[\omega]$. Thus, for some integers a and b,

$$\begin{aligned} m+\omega &= (-2-\omega)(a+b\omega)^3 \\ &= (-2a^3-2b^3+3a^2b+3ab^2)+(-a^3-b^3-3a^2b+6ab^2)\omega. \end{aligned}$$

Comparing coefficients of ω, we see

$$-a^3-b^3-3a^2b+6ab^2=1. \tag{4.3}$$

Now, (a,b) is a solution to Equation 4.3 if and only if $(-b,-a)$ is a solution to Equation 4.2. Therefore the only solutions to Equation 4.3 are $(1,1);(0,-1);(-1,0)$. In all three cases, $m=-2a^3-2b^3+3a^2b+3ab^2=2$. This means that the only solution for the second case is $m=2$. This exhausts all possibilities.

Recalling that $r=3m$, the only solutions for r are $r=-3$ and $r=6$, and in both cases, $r^2-3r+9=27$, meaning that $c=3$.

□

Lemma 4.4. *The only integral values c_1 for which $x^3+c_1x\pm1$ is reducible are $c_1=0,-2$.*

Proof. If $x^3+c_1x\pm1$ were reducible, it must have an integral root, which must be 1 or -1. Thus the only compatible values of c_1 are 0 and -2. □

We are ready to prove Theorems 4.1 and 4.2.

Proof of Theorem 4.1. Consider the cases where $x^3+c_1x\pm1$ is irreducible, so it has Galois group A_3 if and only if the discriminant $\mathrm{D}=-4c_1^3-27$ is a rational square. To find such c_1, it suffices to compute integer solutions (r,c_1) to $c_1^3+r^2-3r+9=0$, since the discriminant of this as a quadratic in r is precisely D. From Lemma 4.3, we see that the only solutions (r,c_1) are $(3,-3)$ and $(6,-3)$, which, along with Lemma 4.4, gives Theorem 1. □

Proof of Theorem 4.2. Fix c_0 to be a (positive) rational prime q. Note that there are only finitely many c_1 such that x^3+c_1x+q is reducible. Therefore we may assume that x^3+c_1x+q is irreducible, so it has Galois group A_3 if and only if the discriminant $\mathrm{D}=-4c_1^3-27q^2$ is a rational square. Then there is some integer r such that (r,c_1) is a solution to $c_1^3+r^2-3rq+9q^2=0$, since the discriminant of this as a quadratic in r is precisely D. Hence

$$r^2-3rq+9q^2=(r+3q\omega)(r+3q\omega^2)=c^3 \tag{4.4}$$

for an integer $c=-c_1$. So to prove Theorem 4.2, it suffices to show that there are only finitely many integers r such that the norm of $r+3q\omega$ is an integral cube.

Case 0: Suppose that $r+3q\omega, r+3q\omega^2$ are coprime. Then by the same argument as in Lemma 4.3, there exist integers a,b such that $r+3q\omega=(a+b\omega)^3 \Rightarrow q=(ab)(a-b)$, which is not possible unless $q=2$ (and in this case, there are only finitely many solutions). Since r is also a polynomial in the a,b, there can only be finitely many (r,c) satisfying Equation 4.4 such that $r+3q\omega, r+3q\omega^2$ are coprime.

For the other cases, suppose that $r+3q\omega, r+3q\omega^2$ are not coprime with greatest common divisor $d\in\mathbb{Z}[\omega]$. Then $\mathrm{N}(d)|\mathrm{N}(3q\omega-3q\omega^2)\Rightarrow\mathrm{N}(d)|27q^2$. Since $\mathrm{N}(d)>1$, it can only have 3 or q as prime factors.

Case 1: $q \equiv 2 \mod 3$. Now, if $q|\mathrm{N}(d)$, because $\mathrm{N}(d)|r^2-3rq+9q^2$, we must have $q|r$ and $q|c$. Then writing $r = qm$ and $c = qn$, we have $m^2-3m+9 = (m+3\omega)(m+3\omega^2) = qn^3$. But since $q \equiv 2 \mod 3$, it is prime in $\mathbb{Z}[\omega]$, so either $m+3\omega$ or $m+3\omega^2 = (m-3)-3\omega$ is a multiple of the integer q, a contradiction.

Thus $\mathrm{N}(d)$ is a power of 3, so we may write $r = 3m$ and $c = 3n$, so that $m^2-mq+q^2 = 3n^3$. Going through the possibilities, we find that $9 \nmid m^2-mq+q^2$, so that $\frac{m+q\omega}{-1+\omega}, \frac{m+q\omega^2}{-1+\omega^2}$ are coprime, hence both are cubes in $\mathbb{Z}[\omega]$. From the argument in Lemma 4.3, there must exist integers a, b such that $q = a^3+b^3-6a^2b+3ab^2$, and by Lemma 4.1, there are only finitely many solutions (a, b) (setting $b = 1$ shows that $a^3+b^3-6a^2b+3ab^2$ is irreducible). Since $r = 3m$ is also a polynomial in the a, b, there can only be finitely many (r, c) satisfying Equation 4.4 in this case.

Case 2: $q \equiv 1 \mod 3$. If $q|\mathrm{N}(d)$, as above, we write $r = qm$ and $c = qn$, so

$$m^2-3m+9 = (m+3\omega)(m+3\omega^2) = qn^3 \tag{4.5}$$

Suppose that these two factors are relatively prime. Clearly, neither divides q, but q is not prime in $\mathbb{Z}[\omega]$. Write $q = c^2-ce+e^2$ for some integers c, e. We note the following facts:

- Because q is prime, c and e are coprime.
- Because $3 \nmid q$, the following combinations $(c, e) \equiv (0,0); (1,2); (2,1) \mod 3$ do not occur. In particular, $2c-e$ does not divide 3.
- q factorizes as $(c+e\omega)((c-e)-e\omega)$. Furthermore, $c+(c-e)\omega = -\omega^2((c-e)-e\omega) = (-\frac{1}{\omega})((c-e)-e\omega)$ is also a factor of q.
- At least one of e or $c-e$ is not a multiple of 3.
- $3 \nmid m$. Therefore none of $\mathrm{A} = m+3\omega$, $\mathrm{B} = (-\omega)\mathrm{A} = -\omega(m+3\omega) = 3+(3-m)\omega$, $\mathrm{C} = m+3\omega^2 = (m-3)-3\omega$, $\mathrm{D} = (-\omega)\mathrm{C} = -\omega((m-3)-3\omega) = -3-m\omega$ are real.

Now, one of A, B, C, or D equals $(c+e\omega)(a+b\omega)^3$, where $q = c^2-ce+e^2$ and $3 \nmid e$ (this must happen by the fourth item above). It was necessary to introduce B and D above to possibly correct for the $-\omega^2$ unit. However, it does not matter which of A, B, C, or D it is, since each has nonzero ω component s. Equating ω components, we have

$$s = (e)a^3+(3c-3e)a^2b-(3c)ab^2+(e)b^3. \tag{4.6}$$

To apply Lemma 4.1 and conclude there are only finitely many integral solutions (a, b) (implying that there are only finitely many m that satisfy Equation 4.5), we need to show that the right-hand side of Equation 4.6 is irreducible. To see this, set $b = 1$ and apply the transformation $a \to a-1$, so that the right-hand side of Equation 4.6 becomes

$$(e)a^3+(3c-6e)a^2+(-9c+9e)a+3(2c-e). \tag{4.7}$$

By construction, $3 \nmid e$, and by the second bullet point, $3 \nmid 2c - e$. Hence the above polynomial is Eisenstein at 3, so the right-hand side of Equation 4.6 is indeed irreducible, and there are only finitely many possibilities for $r = qm$ in this case.

Otherwise, $m + 3\omega, m + 3\omega^2$ are not relatively prime. Then the norm of their greatest common divisor is a multiple of 3, so that $3|m, 3|n$. Writing $m = 3m', n = 3n'$, we have

$$(m')^2 - m' + 1 = (m' + \omega)((m' - 1) - \omega) = 3q(n')^3. \tag{4.8}$$

We know that $9 \nmid (m')^2 - m' + 1$, and $3 = (-1+\omega)(-1+\omega^2) = (-1+\omega)(-2-\omega)$, so $m' + \omega$ divides either $-1+\omega$ or $-2-\omega$, and $(m'-1)-\omega$ divides the other. Note that after this division, the two quotients are coprime. Futhermore, $m' \neq 0, \pm 1, \pm 2$ as the left-hand side of Equation 4.8 divides both 3 and the prime $q \equiv 1 \mod 3$, so each of the four possible quotients has nonzero ω component, even after multiplying each by $-\omega$. Then one of the four possible quotients (possibly adjusting by $-\omega$) is equal to $(c + e\omega)(a + b\omega)^3$ with $q = c^2 - ce + e^2, 3 \nmid e$. By the same argument as above, this case only gives finitely many possibilities for $r = 3qm'$.

The final possibility is that $\mathrm{N}(d)$ is a power of 3. Then write $r = 3m$ and $c = 3n$, so that $m^2 - mq + q^2 = 3n^3$. Going through the possibilities, we find that $9 \nmid m^2 - mq + q^2$, so we may finish as in Case 1. So this case only gives finitely many possibilities for r.

Case 3: $q = 3$. Then $\mathrm{N}(d)|27q^2$ is a power of 3. Thus $r^2 - 3rq + 9q^2 = r^2 - 9r + 81$ is a multiple of 3, whereupon we write $r = 3m$ and $c = 3n$, so that

$$m^2 - 3m + 9 = 3n^3. \tag{4.9}$$

From this we see that $3|m$, which makes the left-hand side of Equation 4.9 a multiple of 9, implying $3|n$. Writing $m = 3m', n = 3n'$, we obtain $(m')^2 - m' + 1 = 9(n')^3$. But this is a contradiction, as the left-hand side never divides 9. So this case does not give any possibilities for r.

Combining the results of cases 0, 1, 2, and 3 (i.e. zero or finitely many possibilities for r in each), we obtain Theorem 4.2.

□

We end with a natural generalization of Theorem 4.2:

Theorem 4.3. For any nonzero integer c_0, $p(x) = x^3 + c_1 x + c_0$ does not have Galois group S_3 for only finitely many integers c_1.

Proof. This proof relies on more advanced machinery—in particular, results on elliptic curves. See Example 2.5, [3]. □

References

[1] Chela, R. Reducible polynomials. *J. Lond. Math. Soc.* 38 (1963), 183–188.

[2] Chow, S. & Dietmann, R. Enumerative Galois Theory for Cubics and Quartics. *Advances in Mathematics* 372 (2020) 107282.

[3] Conrad, K. *Galois groups of cubics and quartics (not in characteristic 2)* (n.d.). http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf.

[4] Pham, H. T. & Xu, M. *Irreducibility of random polynomials of bounded degree* (2020). https://arxiv.org/abs/2002.10554.

[5] Rivin, I. *Galois Groups of Generic Polynomials* (2015). https://arxiv.org/abs/1511.06446.

[6] Thue, A. Über Annäherungswerte algebraischer Zahlen. *J. reine angew. Math.* 135 (1909), 284-305.

[7] Tzanakis, N. The diophantine equation $x^3 - 3xy^2 - y^3 = 1$ and related equations. *J.Number Th.* 18, No 2 (1984), 192–205.

[8] van der Waerden, B. L. Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. *Monatsh. Math. Phys.* 43 (1936), 133–147.

Hanson Hao
Stanford University
hhao@stanford.edu

Eli Navarro
Stanford University
enava22@stanford.edu

Henri Stern
Stanford University
hsstern@stanford.edu