THE BOUNIAKOWSKY CONJECTURE AND THE DENSITY
OF POLYNOMIAL ROOTS TO PRIME MODULI

Timothy Foo
Division of Mathematical Sciences, Nanyang Technological University, Singapore
S080074@ntu.edu.sg

Abstract
We establish a result linking the Bouniakowsky conjecture and the
density of polynomial roots to prime moduli.

Mathematics Subject Classification (2000): 11B05, 11C08, 11K06,
11N32
Keywords: Bouniakowsky conjecture, Schinzel Hypothesis, density, poly-
nomial roots, prime moduli

Introduction
In this paper, we study roots of irreducible polynomials to prime moduli. We
think of \( \mathbb{Z}/p\mathbb{Z} \) as the set \( 0, 1, 2, \ldots, p - 1 \) and hence we think of the root of
our polynomial as a number in that set. When the root \( z \) is divided by \( p \),
we naturally have a number in \( (0, 1) \). If we fix a polynomial \( f(x) \) of degree
\( n \geq 2 \) which is irreducible in \( \mathbb{Z}[x] \), we can consider the set
\[
A_f = \bigcup_p \{ \frac{z}{p} : f(z) \equiv 0 \mod{p}, 1 \leq z \leq p - 1 \}
\]
The aim of this paper is to prove that if a certain conjecture called the Bou-
niakowsky conjecture is true, then the set \( A_f \) is dense in \( (0,1) \). We stress that
our result is conditional. Results that are not dependent on open conjectures
have been proven about roots of polynomials to various moduli. Hooley [H]
proved that the roots of an irreducible polynomial, considered over the ring
\( \mathbb{Z}/n\mathbb{Z} \), \( n \) not necessarily prime, when suitably normalized by dividing by \( n \)
and considered over all \( n \), are in fact equidistributed in \( (0,1) \). Duke, Fried-
lander and Iwaniec[DFI] proved equidistribution for quadratic polynomials
of negative discriminant, to prime moduli. Toth[T] proved equidistribution
for quadratic polynomials of positive discriminant, to prime moduli. We now
state the main theorem of our paper.

Theorem If the Bouniakowsky conjecture is true, the set \( A_f = \bigcup_p \{ \frac{z}{p} : f(z) \equiv 0 \mod{p}, 1 \leq z \leq p - 1 \} \) is dense in \( (0,1) \).
The Bouniakowsky conjecture

We now discuss the Bouniakowsky conjecture to give some background.

Conjecture Bouniakowsky Conjecture: Let \( f(x) \) be a polynomial that is irreducible in \( \mathbb{Z}[x] \). Let \( r_f = \gcd\{f(x) : x \in \mathbb{Z}\} \). Then \( \frac{f(x)}{r_f} \) is prime infinitely often.

It is easy to construct polynomials which are always divisible by a given prime \( q \). We know by Fermat’s little theorem that the prime \( q \) always divides \( x^q - x \). Therefore, all we have to do is choose a value \( k \) so that \( x^q - x + qk \) is irreducible in \( \mathbb{Z}[x] \). It then follows that \( q \) divides all the values of this polynomial.

The Result

We first begin by considering a subset of \((0,1)\) which we will prove to be dense. We are then going to use this set to help prove the density of \( A_f \).

Here, we let \( n \) be the degree of \( f \) and \( c \) be the leading coefficient of \( f \).

Let \( B_f = \{ \frac{a}{b} : 1 \leq a < b, b \text{ odd prime}, (cr_f, b) = 1, acx^{n-1} = -r_f \mod b \text{ has a solution} \} \).

Lemma 1 \( B_f \) is dense in \((0,1)\).

Proof

Case 1: \( n \) is even. Consider the map \( x \to x^{n-1} \) on \((\mathbb{Z}/b\mathbb{Z})^*\). This map is injective and surjective if \((n-1, b-1) = 1\). For such \( b \), we can in fact solve \( acx^{n-1} \equiv -r_f \mod b \) for all \( a \in (\mathbb{Z}/b\mathbb{Z})^* \). Since \( b \) is prime, we can pick \( b \) larger than \( cr_f \) to ensure \((b, cr_f) = 1\). We can also pick infinitely many such \( b \) with \((n-1, b-1) = 1\). It thus follows that \( B_f \) is dense in this case.

Case 2: \( n \) is odd. Since \( n-1 \) is even, let \( n-1 = 2^e h, h \text{ odd} \). The map \( x \to x^{n-1} \) on \((\mathbb{Z}/b\mathbb{Z})^*\) is therefore a composition of the maps \( x \to x^2 \) applied \( e \) times and \( x \to x^h \). \( x \to x^h \) is a permutation of \((\mathbb{Z}/b\mathbb{Z})^* \) if \((b-1, h) = 1\). Also, if \( b \equiv 3 \mod 4 \), \( x \to x^2 \) is a permutation of the squares in \((\mathbb{Z}/b\mathbb{Z})^* \), so by choosing \( b \equiv 3 \mod 4 \) and \((b-1, h) = 1\), we can ensure that the image of \( x \to x^{n-1} \) is the squares. We also want \((b, cr_f) = 1\). We have infinitely many primes \( b \) satisfying these conditions, and for such \( b \), the numerator of the fractions \( \frac{a}{b} \) ranges over either only the squares or only the nonsquares in \((\mathbb{Z}/b\mathbb{Z})^* \). By a result of Brauer, the maximum number of consecutive squares or nonsquares in \((\mathbb{Z}/b\mathbb{Z})^* \) is less than \( b^{0.5} \) when \( b \equiv 3 \mod 4 \). [B] This ensures that \( B_f \) is dense in this case.

We will now show how \( \frac{a}{b} \) is related to the values in \( B_f \). To do this, first consider the original polynomial \( f \). From \( f = \sum c_i x^i \), we can construct a polynomial \( g(x, y) = \sum c_i x^i y^{n-i} \). Now for any prime \( b \) with \((b, cr_f) = 1\) we
have a polynomial in one variable \( g(bw + t, b) \) where \( w \) is the variable and \( t \in (\mathbb{Z}/b\mathbb{Z})^* \). Since we can vary \( b \) and \( t \), we have many such polynomials associated to \( f \). We will show that the gcd of the values of all these polynomials is also \( r_f \) and that they are also irreducible in \( \mathbb{Z}[w] \). It is these polynomials that we apply the Bouniakowsky conjecture to. If the Bouniakowsky conjecture is true, then there are infinitely many primes \( p \) with \( r_fp = g(bw + t, b) \) as \( w \to \infty \). Furthermore, for these primes \( p \), we can construct a root \( z \) of \( f \) mod \( p \) such that \( \frac{a}{b} \) is “close” to \( \frac{z}{b} \) where \( a \) is chosen so that \( \frac{ap+bw+t}{b} \) is an integer and \( \frac{a}{b} \in (0,1) \). This is the same as choosing \( 1 \leq a < b \) and \( a \) such that \( act^{-1} \equiv -r_f \mod b \). We thus see the relation to the set \( B_f \). We then let \( z = \frac{ap+bw+t}{b} \) and show that \( z \) is a root of \( f \mod p \).

**Lemma 2** The polynomial \( g(bw + t, b) \), where \( w \) is the variable, \( b \) is prime, \((b, cr_f) = 1, 1 \leq t < b \) is irreducible in \( \mathbb{Z}[w] \).

**Proof** \( g(bw + t, b) \) is related in a simple way to the original polynomial \( f \).

\[
g(bw+t,b) = \sum_i c_i(bw+t)^ib^{-i} = b^n \sum_i c_i(w+\frac{1}{b})^i = b^n g(w+\frac{1}{b},1) = b^n f(w+\frac{1}{b}).
\]

Since a polynomial is irreducible in \( \mathbb{Z}[x] \) if and only if it is irreducible in \( \mathbb{Q}[x] \), the lemma follows.

**Lemma 3** Let \( b \) be prime, \((b, cr_f) = 1 \), and \( 1 \leq t < b \). Then \( \gcd(\{g(bw+t,b) : w \in \mathbb{Z}\}) = r_f \)

**Proof** Let \( r = r_f \). Since \( f \) has integer coefficients, we can think of \( f \) as a polynomial in \((\mathbb{Z}/r\mathbb{Z})[x]\). But since \( r \) divides all the values of \( f \), it follows that \( f(x) = 0 \) in \((\mathbb{Z}/r\mathbb{Z})[x]\). We showed in the proof of Lemma 2 that \( g(bw + t, b) = b^n f(w + \frac{1}{b}) \) in \( \mathbb{Q}[x] \). Since \((b, r_f) = 1, b \) has an inverse mod \( r \) and hence the rational number \( \frac{1}{b} \) can be thought of as an element in \( \mathbb{Z}/r\mathbb{Z} \). Hence \( g(bw + t, b) = b^n f(w + \frac{1}{b}) = 0 \) in \((\mathbb{Z}/r\mathbb{Z})[x]\). Therefore, for each such \( b \) and \( t \), we have that \( r \) divides \( \gcd(\{g(bw+t,b) : w \in \mathbb{Z}\}) \). Conversely, let \( r_{b,t} = \gcd(\{g(bw+t,b) : w \in \mathbb{Z}\}) \). We have \( g(bw + t, b) = 0 \) in \((\mathbb{Z}/r_{b,t}\mathbb{Z})[w]\). But \( f(w) = (b^n)^{-1} g(b(w - \frac{1}{b}) + t, b) \), so \( f(w) = 0 \) in \((\mathbb{Z}/r_{b,t}\mathbb{Z})[w] \). Therefore \( r_{b,t} \) divides \( r \) for each such \( b \) and \( t \). It follows that the polynomials \( g(bw+t,b) \) have the same \( \gcd \) as \( f \).

**Lemma 4** If \( a \) is chosen such that \( z = \frac{ap+bw+t}{b} \) is an integer, then \( z \) is a root of the polynomial \( f \) mod \( p \).

**Proof** \( b^n f(z) = b^n f(\frac{ap+bw+t}{b}) = b^n \sum_i c_i(\frac{ap+bw+t}{b})^i = \sum_i c_i(a \cdot p + b \cdot w + t)^i b^{-i} = g(bw + t, b) = r_fp \equiv 0 \mod p \). Since \((b, p) = 1 \), the lemma is proven.

Having proven these lemmas, we know that \( \hat{z} \) is close to \( \frac{a}{b} \). Assuming the Bouniakowsky conjecture, we can let \( w \to \infty \) and obtain infinitely many primes \( p \) and a root \( z \) for each prime. As \( w \to \infty \), \( \hat{z} \) is arbitrarily close to
\[ \frac{a}{b}, \text{ since } n \geq 2. \text{ Since we showed in Lemma 1 that } B_f \text{ is dense in } (0, 1), \text{ the theorem is now proved.} \]

Acknowledgements

Thanks to Professor Zhengyu Mao for suggesting the problem to me and for many helpful discussions.

References

[B] A. Brauer, Über die Verteilung der Potenzreste, Math Z. 35 (1932) 39-50.
[DFI] W. Duke, J.B. Friedlander, H. Iwaniec, Equidistribution of roots of a quadratic congruence to prime moduli, Annals of Mathematics (2) 141 (1995), no. 2, 423-441.
[H] C. Hooley, On the distribution of the roots of a polynomial congruences, Mathematika 11 (1964) 39-49
[T] A. Toth, Roots of quadratic congruences, IMRN 2000, no. 14, 719-739