#A101 INTEGERS 18 (2018)

ON THE NUMBER OF PRIMES FOR WHICH A POLYNOMIAL IS EISENSTEIN

Shilin Ma
Department of Mathematics and Statistics, Carleton College, Northfield, Minnesota

Kevin J. McGown
Department of Mathematics and Statistics, California State University Chico, Chico, California
kmcgown@csuchico.edu

Devon Rhodes
Department of Mathematics and Statistics, California State University Chico, Chico, California

Mathias Wanner
Department of Mathematics and Statistics, Villanova University, Villanova, Pennsylvania

Received: 2/9/18, Revised: 9/16/18, Accepted: 12/5/18, Published: 12/10/18

Abstract

Previously Heyman and Shparlinski gave an asymptotic formula with error term for the number of Eisenstein polynomials of fixed degree and bounded height. Let $\psi(f)$ denote the number of primes for which a polynomial f is Eisenstein. We give expressions for the mean and variance of the function ψ for each fixed degree, where the polynomials are ordered according to their height.

1. Introduction

For an integer $d \geq 2$, let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. We say that f is Eisenstein if there exists a prime p such that $p \mid a_i$ for $i = 0, 1, \ldots, d-1$, $p^2 \nmid a_0$, and $p \nmid a_d$. The well-known fact that Eisenstein polynomials are irreducible is often encountered in an undergraduate algebra course. See [1] for a fascinating history of this result, which was proved independently by Schönemann and Eisenstein.

Dobbs and Johnson (see [2]) posed some probabilistic questions concerning Eisenstein polynomials. In particular, one could ask: What is the probability that a randomly chosen polynomial is Eisenstein? Dubickas answers this question in [4] by providing an asymptotic expression for the number of monic Eisenstein polynomials of fixed degree and bounded height. Later Heyman and Shparlinski (see [6]) gave an asymptotic expression for the number of Eisenstein polynomials (monic or not) of fixed degree and bounded height but with a stronger error term. We mention in passing that there are generalizations and variations one may consider; some results in this area include [5, 7, 8, 3].

Our paper builds naturally on [6] so we begin by stating their result. Define the height of a polynomial f to be $\max\{|a_0|, |a_1|, \ldots, |a_d|\}$. Let $\mathcal{F}_d(H)$ be the set of Eisenstein polynomials of degree d and height at most H.

Theorem 1 (Heyman–Shparlinski). *We have*

$$\#\mathcal{F}_d(H) = \gamma_d (2H)^{d+1} + \begin{cases} O(H^d) & \text{if } d > 2 \\ O(H^2(\log H)^2) & \text{if } d = 2\,. \end{cases}$$

Let $\psi(f)$ denote the number of primes for which f is Eisenstein. Our aim is to study the statistics of this function. We establish the following result, which gives an expression for the mean and variance of the function $\psi(f)$ as f ranges over all Eisenstein polynomials of a fixed degree.

Theorem 2. *Let*

$$\alpha_d := \sum_{p \text{ prime}} \frac{(p-1)^2}{p^{d+2}}\,, \qquad \beta_d := \sum_{p \text{ prime}} \left(\frac{(p-1)^2}{p^{d+2}}\right)^2$$

and

$$\gamma_d := 1 - \prod_{p \text{ prime}} \left(1 - \frac{(p-1)^2}{p^{d+2}}\right)\,.$$

Then we have

$$\mu_d := \lim_{H\to\infty} \frac{\sum_{f\in\mathcal{F}_d(H)} \psi(f)}{\sum_{f\in\mathcal{F}_d(H)} 1} = \frac{\alpha_d}{\gamma_d}\,,$$

$$\sigma_d^2 := \lim_{H\to\infty} \frac{\sum_{f\in\mathcal{F}_d(H)} (\psi(f)-\mu_d)^2}{\sum_{f\in\mathcal{F}_d(H)} 1} = \frac{\alpha_d + \alpha_d^2 - \beta_d - \mu_d\alpha_d}{\gamma_d}\,.$$

We note in passing that α_d and β_d can be expressed as finite linear combinations of values of the prime zeta function $P(s) = \sum_p p^{-s}$. Throughout this paper, the variables p and q will always denote primes. See Section 3 for additional comments on α_d, β_d, γ_d, μ_d, σ_d^2, including a table of numerical values for various values of d.

2. Proofs

As usual we let $\omega(n)$ denote the number of distinct prime factors of n and let $\phi(n)$ denote the Euler phi-function. Following [6], we let $\mathcal{H}_d(s,H)$ be the number of polynomials of degree d and height at most H satisfying $s \mid a_i$ for $i = 0,1,\ldots,d-1$, $\gcd(a_0/s, s) = 1$, and $\gcd(a_d, s) = 1$.

Lemma 1. *We have*

$$\#\mathcal{H}_d(s,H) = \frac{(2H)^{d+1}\phi^2(s)}{s^{d+2}} + O\left(\frac{2^{\omega(s)}H^d}{s^{d-1}}\right). \tag{1}$$

Proof. See Lemma 5 of [6]. □

Lemma 2. *We have*

$$\sum_{f\in\mathcal{F}_d(H)} \psi(f) = (2H)^{d+1}\alpha_d + \begin{cases} O(H^2) & \text{if } d > 2 \\ O(H^2 \log\log H) & \text{if } d = 2\,. \end{cases} \tag{2}$$

Proof. We rewrite the sum in question as a sum over primes and apply Lemma 1; this yields

$$\begin{aligned}
\sum_{f\in\mathcal{F}_d(H)} \psi(f) &= \sum_{p\le H} \#\mathcal{H}_d(p,H) \\
&= \sum_{p\le H}\left[\frac{(2H)^{d+1}\phi^2(p)}{p^{d+2}} + O\left(\frac{2^{\omega(p)}H^d}{p^{d-1}}\right)\right] \\
&= (2H)^{d+1}\sum_{p\le H}\frac{(p-1)^2}{p^{d+2}} + \sum_{p\le H} O\left(\frac{H^d}{p^{d-1}}\right) \\
&= (2H)^{d+1}\sum_{p}\frac{(p-1)^2}{p^{d+2}} - (2H)^{d+1}\sum_{p>H}\frac{(p-1)^2}{p^{d+2}} + \sum_{p\le H} O\left(\frac{H^d}{p^{d-1}}\right).
\end{aligned}$$

The splitting of $\sum_{p\le H}$ into $\sum_p$ and $\sum_{p>H}$ is justified since $\sum_p$ converges absolutely. It remains to bound the second and third terms in the last line above. We bound the second term using the integral test to obtain

$$(2H)^{d+1}\sum_{p>H}\frac{(p-1)^2}{p^{d+2}} = O\left(H^{d+1}\int_H^\infty \frac{(x-1)^2}{x^{d+2}}\,dx\right) = O\left(H^{d+1}H^{-d+1}\right) = O\left(H^2\right).$$

For the third term, we find

$$H^d\sum_{p\le H}\frac{1}{p^{d-1}} = \begin{cases} O\left(H^2\right) & \text{if } d > 2 \\ O\left(H^2\log\log H\right) & \text{if } d = 2\,, \end{cases}$$

where we have used Mertens' Theorem (see, for example, [9]) in the case of $d = 2$. □

Lemma 3. *We have*

$$\sum_{f\in\mathcal{F}_d(H)} \psi(f)^2 = (\alpha_d + \alpha_d^2 - \beta_d)(2H)^{d+1} + \begin{cases} O(H^2) & \text{if } d > 2 \\ O(H^2(\log\log H)^2) & \text{if } d = 2\,. \end{cases}$$

Proof. If we define

$$\tau(f,p) = \begin{cases} 1 & \text{if } f \text{ is } p\text{-Eisenstein} \\ 0 & \text{otherwise}\,, \end{cases}$$

then the first sum can be rewritten as

$$\begin{aligned}
\sum_{f\in\mathcal{F}_d(H)} \psi(f)^2 &= \sum_{f\in\mathcal{F}_d(H)} \left(\sum_{p \text{ prime}} \tau(f,p) \right)^2 \\
&= \sum_{f\in\mathcal{F}_d(H)} \left(\sum_{p \text{ prime}} \tau(f,p) \sum_{q \text{ prime}} \tau(f,q) \right) \\
&= \sum_{f\in\mathcal{F}_d(H)} \left(\sum_{p,q \text{ prime}} \tau(f,p)\tau(f,q) \right) \\
&= \sum_{p,q \text{ prime}} \left(\sum_{f\in\mathcal{F}_d(H)} \tau(f,p)\tau(f,q) \right) .
\end{aligned}$$

The inner sum above represents the number of polynomials of height at most H that are Eisenstein for both p and q, but the fact that p may equal q complicates matters. Consequently, we have

$$\sum_{f\in\mathcal{F}_d(H)} \psi(f)^2 = \sum_{p\le H} \#\mathcal{H}(p,H) + \sum_{\substack{pq\le H \\ p\ne q}} \#\mathcal{H}(pq,H)\,.$$

The first sum on the right-hand side above is exactly what appears in Lemma 2, and therefore is it equal to the right-hand side of (2). It remains to deal with the second sum, which equals

$$\begin{aligned}
&\sum_{\substack{pq\le H\\ p\ne q}} \#\mathcal{H}(pq,H)\\
&= (2H)^{d+1}\sum_{\substack{pq\le H\\ p\ne q}} \frac{(p-1)^2(q-1)^2}{p^{d+2}q^{d+2}} + O\left(\sum_{\substack{p,q \text{ prime}\\ pq\le H}} \frac{H^d}{(pq)^{d-1}} 2^{\omega(pq)}\right)\\
&= (2H)^{d+1}\sum_{pq\le H} \frac{(p-1)^2(q-1)^2}{p^{d+2}q^{d+2}} - (2H)^{d+1}\sum_{p^2\le H}\left(\frac{(p-1)^2}{p^{d+2}}\right)^2\\
&\qquad + O\left(H^d \sum_{\substack{p,q \text{ prime}\\ pq\le H}} \frac{1}{(pq)^{d-1}}\right).
\end{aligned}$$

For the first term, as in the proof of Lemma 2, we have

$$\begin{aligned}
&(2H)^{d+1}\sum_{pq\le H} \frac{(p-1)^2(q-1)^2}{p^{d+2}q^{d+2}}\\
&\qquad = (2H)^{d+1}\sum_{p,q} \frac{(p-1)^2(q-1)^2}{p^{d+2}q^{d+2}} + (2H)^{d+1}\sum_{p>H}\frac{1}{p^d}\sum_{q>H/p}\frac{1}{q^d}\\
&\qquad = (2H)^{d+1}\left(\sum_p \frac{(p-1)^2}{p^{d+2}}\right)^2 + O\left(H^{d+1}\sum_{p>H}\frac{1}{p^d}\right)\\
&\qquad = (2H)^{d+1}\alpha_d^2 + O(H^2).
\end{aligned}$$

For the second term,

$$\begin{aligned}
&(2H)^{d+1}\sum_{p^2\le H}\left(\frac{(p-1)^2}{p^{d+2}}\right)^2\\
&\qquad = (2H)^{d+1}\sum_p\left(\frac{(p-1)^2}{p^{d+2}}\right)^2 - (2H)^{d+1}\sum_{p>\sqrt{H}}\left(\frac{(p-1)^2}{p^{d+2}}\right)^2\\
&\qquad = (2H)^{d+1}\beta_d + O(H^{3/2}).
\end{aligned}$$

Finally, for the third term, we have

$$H^d \sum_{\substack{p,q \text{ prime}\\ pq\le H}} \frac{1}{(pq)^{d-1}} = \begin{cases} O(H^2), & \text{if } d>2\\ O(H^2(\log\log H)^2), & \text{if } d=2. \end{cases}$$

Putting this all together proves the lemma. □

Proof of Theorem 2. The part of the theorem concerning the mean μ_d follows immediately from Lemma 2 and Theorem 1. Now we consider the variance:

$$\begin{aligned}\sigma_d^2 &= \lim_{H\to\infty} \frac{\sum_{f\in\mathcal{F}_d(H)}(\psi(f)-\mu_d)^2}{\sum_{f\in\mathcal{F}_d(H)} 1} \\ &= \lim_{H\to\infty} \frac{1}{\#\mathcal{F}_d(H)} \sum_{f\in\mathcal{F}_d(H)} \left(\psi(f)^2 - 2\psi(f)\mu_d + \mu_d^2\right) \\ &= \lim_{H\to\infty} \frac{1}{\#\mathcal{F}_d(H)} \left[\sum_{f\in\mathcal{F}_d(H)} \psi(f)^2 - 2\mu_d \sum_{f\in\mathcal{F}_d(H)} \psi(f) + \mu_d^2 \sum_{f\in\mathcal{F}_d(H)} 1\right].\end{aligned}$$

By Lemma 2, Lemma 3, and Theorem 1, the limit above equals

$$\frac{1}{\gamma_d}\left[(\alpha_d + \alpha_d^2 - \beta_d) - 2\mu_d\alpha_d + \mu_d^2\gamma_d\right],$$

which simplifies to the desired expression. □

3. Remarks on the Constants

It is not hard to show that

$$\alpha_d = \frac{1}{2^{d+2}} + O\left(\frac{1}{3^d}\right), \qquad \beta_d = \frac{1}{2^{2(d+2)}} + O\left(\frac{1}{3^{2d}}\right), \qquad \gamma_d = \frac{1}{2^{d+2}} + O\left(\frac{1}{3^d}\right).$$

It then follows that $\lim_{d\to\infty}\mu_d = 1$ and $\lim_{d\to\infty}\sigma_d^2 = 0$, as one would expect. If one was interested in the mean $\hat{\mu_d}$ and variance $\hat{\sigma}_d^2$ of $\psi(f)$ as f ranges over all polynomials, instead of just Eisenstein polynomials, one would obtain the simpler expressions $\hat{\mu}_d = \alpha_d$ and $\hat{\sigma}_d^2 = \alpha_d - \beta_d$. We will not prove this explicitly but it essentially follows from the proof of Theorem 2. In this case, one observes that $\lim_{d\to\infty}\hat{\mu_d} = 0$ and $\lim_{d\to\infty}\hat{\sigma}_d^2 = 0$, as expected.

d	$\alpha_d = \hat{\mu}_d$	β_d	γ_d	μ_d	σ_d^2	$\hat{\sigma}_d^2$
2	0.17971	0.00731	0.16765	1.07192	0.07187	0.17239
3	0.05653	0.00127	0.05557	1.01714	0.01705	0.05525
4	0.02255	0.00027	0.02243	1.00519	0.00517	0.02227
5	0.00989	0.00006	0.00988	1.00169	0.00169	0.00983
6	0.00456	0.00001	0.00456	1.00056	0.00056	0.00454

Table 1: Approximate values of the constants for small d

Acknowledgement. This research was completed as part of the Research Experience for Undergraduates and Teachers program at California State University, Chico funded by the National Science Foundation (DMS-1559788).

References

[1] D. Cox, Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, *Amer. Math. Monthly* **118** (2011), no. 1, 3-21.

[2] D. Dobbs and L. Johnson, On the probability that Eisenstein's criterion applies to an arbitrary irreducible polynomial, *Advances in commutative ring theory* (Fez, 1997), 241-256, Lecture Notes in Pure and Appl. Math., **205**, Dekker, New York, 1999.

[3] E. Dotti and G. Micheli, Eisenstein polynomials over function fields, Preprint, 2015, available at arXiv:1506.05380 [math.NT].

[4] A. Dubickas, Polynomials irreducible by Eisenstein's criterion, *Appl. Algebra Engrg. Comm. Comput.* **14** (2003), no. 2, 127-132.

[5] R. Heyman, On the number of polynomials of bounded height that satisfy the Dumas criterion, *J. Integer Seq.*, **17** (2014), no. 2.

[6] R. Heyman and I. Shparlinski, On the number of Eisenstein polynomials of bounded height, *Appl. Algebra Engrg. Comm. Comput.* **24** (2013), no. 2, 149-156.

[7] R. Heyman and I. Shparlinski, On shifted Eisenstein polynomials, *Period. Math. Hungar.* **69** (2014), no. 2, 170-181.

[8] G. Micheli and R. Schnyder, The density of shifted and affine Eisenstein polynomials, Preprint, 2015, available at arXiv:1507.02753 [math.NT].

[9] P. Pollack, *Not always buried deep. A second course in elementary number theory*, American Mathematical Society, Providence, RI, 2009.