COUNTING EISENSTEIN POLYNOMIALS SATISFYING A CONDITION FROM GENUS THEORY

Jongwoo Choi
Department of Mathematics and Statistics, California State University, Chico, California

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

Received: 2/7/20, Accepted: 7/28/20, Published: 8/14/20

Abstract

We give an asymptotic formula for the number of monic Eisenstein polynomials of odd prime degree satisfying an additional condition that arises in the study of the genus number of an algebraic number field.

1. Introduction

Let d denote an odd prime throughout. Our main theorem concerns counting the proportion of Eisenstein polynomials of degree d satisfying a specific condition. Before commencing with the statement of our result, it is perhaps useful to comment on where this condition arises.

Let K be an algebraic number field of degree d. One important invariant associated to K is the so-called genus number of K, denoted g_K; in our setting, g_K is a divisor of the class number h_K. It is very natural to ask about the statistical distribution of g_K as one runs through all number fields of a given degree. More specifically, one could ask what proportion of such fields have $g_K = 1$. Asymptotically, cyclic fields constitute zero percent of all fields of degree d, so we may assume our field K to be non-cyclic.

In [4], A. Tucker and the second author establish the precise proportion of cubic fields with genus number one; establishing a similar result for $d = 5$ is work in progress. However, when $d > 5$, counting number fields of degree d is an open problem.

It is well-known that one can choose $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$ such that the minimal polynomial $f(x)$ of α is p-Eisenstein if and only if p is totally ramified in

K. For example, see Ch. 2 of [3] for the precise recipe. Provided the generating polynomial $f(x)$ is chosen in this way, a theorem of Ishida gives a precise method for determining the genus number of K; in particular, this allows one to decide whether K has genus number one just by looking at p-divisibility of the polynomial.

Write

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$$

and let P denote the set of primes p for which $f(x)$ is p-Eisenstein. Then $g_K > 1$ if and only if $p \equiv 1 \pmod{d}$ for some $p \in P$ *or*

$$d \in P \quad \text{and} \quad a_2 \equiv \cdots \equiv a_{d-1} \equiv a_1 + a_d \equiv 0 \pmod{d^2}.$$

Putting aside the question of counting fields, one could ask, what proportion of Eisenstein polynomials $f(x)$ of degree d fail to satisfy this condition? For brevity, let us denote the negation of this condition by $(\star)$ so that, in this context, $g_K = 1$ if and only if condition $(\star)$ holds.

Let $\mathcal{E}_d(H)$ denote the collection of all monic Eisenstein polynomials of height at most H, and let $\mathcal{E}_d^\star(H)$ denote the collection of all $f \in \mathcal{E}_d(H)$ such that f satisfies condition $(\star)$. Building on work of Dubickas [1], Heymann and Shparlinski [2] prove that

$$\#\mathcal{E}_d(H) = \theta_d (2H)^d + \begin{cases} O(H^{d-1}) & \text{if } d > 2 \\ O(H(\log H)^2) & \text{if } d = 2 \end{cases} \tag{1}$$

where

$$\theta_d = 1 - \prod_p \left(1 - \frac{p-1}{p^{d+1}}\right).$$

Along the same lines, we obtain the following asymptotic:

Theorem 1.

$$\#\mathcal{E}_d^\star(H) = \theta_d^\star (2H)^d + \begin{cases} O(H^{d-1}) & \text{if } d > 2 \\ O(H(\log H)^2) & \text{if } d = 2 \end{cases}$$

where

$$\theta_d^\star = 1 - \frac{d-1}{d^{2d}} - \left(1 - \frac{(d-1)(d^{d-1}+1)}{d^{2d}}\right) \prod_{\substack{p \neq d \\ p \not\equiv 1 (d)}} \left(1 - \frac{p-1}{p^{d+1}}\right).$$

In particular,

$$\lim_{H \to \infty} \frac{\#\mathcal{E}_d^\star(H)}{\#\mathcal{E}_d(H)} = \frac{\theta_d^\star}{\theta_d}.$$

As a consequence, the answer to our question is given explicitly by the ratio $\theta_d^\star/\theta_d$. When $d = 3$, we have $\theta_3^\star/\theta_3 \approx 0.9681192$, and the sequence of these ratios tend to 1 as $d \to \infty$. We emphasize that counting the polynomials is dif and only iferent than counting the fields, but we found determining a closed form for the ratio $\theta_d^\star/\theta_d$ an interesting problem nonetheless.

2. Preliminary Lemmas

We define

$$\varphi(s,H) = \sum_{\substack{|a|\le H\\ \gcd(a,s)=1}} 1\,.$$

Lemma 1. *For any integer $s \ge 1$, we have*

$$\varphi(s,H) = \frac{2H\varphi(s)}{s} + O\left(2^{\omega(s)}\right)\,.$$

Proof. See Lemma 4 of [2]. □

Let $\mathcal{G}_d(s,H)$ be the set of degree d monic polynomials of height at most H satisfying:

1. $s \mid a_i$ for $i = 0, \ldots, d-1$,
2. $\gcd(a_0/s, s) = 1$.

Lemma 2. *For $s \le H$, we have*

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

Proof. See Lemma 3 of [2]. □

Let $\mathcal{G}'_d(s,H)$ be the set of degree d monic polynomials $f(x)$ of height at most H satisfying:

1. $s \mid a_i$ for $i = 0, \ldots, d-1$,
2. $\gcd(a_0/s, s) = 1$,
3. $f(x)$ is Eisenstein at d,
4. $a_1 \equiv \cdots \equiv a_{d-2} \equiv a_0 + a_{d-1} \equiv 0 \pmod{d^2}$.

Lemma 3. *For $s \le H$ with $\gcd(s,d) = 1$, we have*

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

Proof. Assume $s \le H$. For every $i = 1, 2, ..., d-2$, we have $d^2 s \mid a_i$ and thus the number of possibilities for each a_i is equal to

$$2\left\lfloor \frac{H}{d^2 s}\right\rfloor + 1.$$

We then wish to count the number of integers $|a_0| \le H$ satisfying $ds \mid a_0$ and $\gcd(a_0/(ds), ds) = 1$. Since $ds \mid a_0$, we may write $a_0 = kds$. Using Lemma 1, the number of possible a_0 is equal to

$$\varphi\left(ds, \frac{H}{ds}\right) = 2\frac{\varphi(ds)}{ds}\frac{H}{ds} + O\left(2^{\omega(ds)}\right) = 2H\frac{\varphi(ds)}{d^2s^2} + O\left(2^{\omega(s)}\right).$$

Having chosen a_0, we want to count $|a_{d-1}| \le H$ satisfying $d \mid a_{d-1}$, $s \mid a_{d-1}$, and $a_0 + a_{d-1} \equiv 0 \pmod{d^2}$. From the last condition, we know that d divides $a_0 + a_{d-1}$, and therefore $d \mid a_{d-1}$. Hence we may drop the first condition. Thus, the number of possibilities for a_{d-1} is

$$\frac{2H}{d^2s} + O(1).$$

Therefore,

$$\begin{aligned}
\#\mathcal{G}'_d(s,H) &= \left(\frac{2H}{d^2s} + O(1)\right)^{d-1}\left(2H\frac{\varphi(ds)}{d^2s^2} + O\left(2^{\omega(s)}\right)\right) \\
&= \left(\left(\frac{2H}{d^2s}\right)^{d-1} + O\left(\left(\frac{H}{s}\right)^{d-2}\right)\right)\left(2H\frac{\varphi(ds)}{d^2s^2} + O\left(2^{\omega(s)}\right)\right) \\
&= \frac{2^dH^d\varphi(ds)}{s^{d+1}d^{2d}} + O\left(\frac{H^{d-1}2^{\omega(s)}}{s^{d-1}}\right).
\end{aligned}$$

□

3. Proof of Theorem 1

Given $f \in \mathcal{E}_d(H)$, suppose f is Eisenstein at $p_1, p_2, ..., p_t$ and no other primes except possibly d. We consider the following two sets:

$$\begin{aligned}
\mathcal{E}_d^{(1)}(H) &= \{f \in \mathcal{E}_d(H) : p_i \equiv 1 \pmod{d} \text{ for some } i\}, \\
\mathcal{E}_d^{(2)}(H) &= \{f \in \mathcal{E}_d(H) : f \text{ is } d\text{-Eisenstein}, p_i \not\equiv 1 \pmod{d} \text{ for } i = 1,2,...,t, \\
&\qquad \text{and } a_1 \equiv \cdots \equiv a_{d-2} \equiv a_0 + a_{d-1} \equiv 0 \pmod{d^2}\}.
\end{aligned}$$

We observe that $\#\mathcal{E}_d^\star(H) = \#\mathcal{E}_d(H) - \#\mathcal{E}_d^{(1)}(H) - \#\mathcal{E}_d^{(2)}(H)$.

Proposition 1. *We have*

$$\#\mathcal{E}_d^{(1)}(H) = \alpha_d(2H)^d + \begin{cases} O(H^{d-1}) \text{ if } d > 2 \\ O(H(\log H)^2) \text{ if } d = 2 \end{cases}$$

where

$$\alpha_d = -\left(1 - \frac{d-1}{d^{d+1}}\right)\prod_{\substack{p \not\equiv 1 (d) \\ p \neq d}}\left(1 - \frac{p-1}{p^{d+1}}\right)\left[-1 + \prod_{p \equiv 1 (d)}\left(1 - \frac{p-1}{p^{d+1}}\right)\right].$$

Proof. The idea here is to mimic the proof of Theorem 1 from [2] but with the extra conditions we need thrown in. Let $\mathcal{S}$ be the set of square-free positive integers divisible by at least one prime $p \equiv 1 \pmod{d}$. Following [2] and applying Lemma 2, we have

$$\begin{aligned}
\#\mathcal{E}_d^{(1)}(H) &= -\sum_{\substack{s=2\\ s\in\mathcal{S}}}^{H} \mu(s)\#\mathcal{G}_d(s,H) \\
&= -\sum_{\substack{s=2\\ s\in\mathcal{S}}}^{H} \mu(s)\left(\frac{2^d H^d \varphi(s)}{s^{d+1}}\right) + O\left(\sum_{s=2}^{H}\left(\frac{H}{s}\right)^{d-1} 2^{\omega(s)}\right) \\
&= -\sum_{\substack{s=2\\ s\in\mathcal{S}}}^{\infty} (2H)^d \frac{\mu(s)\varphi(s)}{s^{d+1}} + O\left(H^d \sum_{s=H+1}^{\infty} \frac{\varphi(s)}{s^{d+1}} + \sum_{s=2}^{H}\left(\frac{H}{s}\right)^{d-1} 2^{\omega(s)}\right).
\end{aligned}$$

Since $\phi(s) \le s$, one has

$$H^d \sum_{s=H+1}^{\infty} \frac{\varphi(s)}{s^{d+1}} = O(H).$$

Moreover, one has

$$\sum_{s=1}^{H} \frac{2^{\omega(s)}}{s^{d-1}} = \begin{cases} O(1) & \text{if } d > 2 \\ O((\log H)^2) & \text{if } d = 2 \end{cases}.$$

See equations (11) and (12) in the proof of Theorem 1 from [2]. We also have

$$-\sum_{\substack{s=2\\ s\in\mathcal{S}}}^{\infty} \frac{\mu(s)\varphi(s)}{s^{d+1}} = -\left(1 - \frac{d-1}{d^{d+1}}\right) \prod_{\substack{p\not\equiv 1 (d)\\ p\neq d}} \left(1 - \frac{p-1}{p^{d+1}}\right)\left[-1 + \prod_{p\equiv 1(d)} \left(1 - \frac{p-1}{p^{d+1}}\right)\right].$$

This completes the proof. □

Proposition 2. *We have*

$$\#\mathcal{E}_d^{(2)}(H) = \beta_d (2H)^d + \begin{cases} O(H^{d-1}) & \text{if } d > 2 \\ O(H(\log H)^2) & \text{if } d = 2 \end{cases}$$

where

$$\beta_d = \frac{d-1}{d^{2d}}\left(1 - \prod_{\substack{p\not\equiv 1(d)\\ p\neq d}} \left(1 - \frac{p-1}{p^{d+1}}\right)\right).$$

Proof. Let $\mathcal{S}'$ be the set of square-free positive integers coprime to d which are products of primes $p \not\equiv 1 \pmod{d}$. Applying Lemma 3, we have:

$$\begin{aligned}
\#\mathcal{E}_d^{(2)}(H) &= -\sum_{\substack{s=2 \\ s\in\mathcal{S}'}}^{H} \mu(s)\#\mathcal{G}'_d(s,H) \\
&= -\sum_{\substack{s=2 \\ s\in\mathcal{S}'}}^{H} \mu(s)(2H)^d \frac{\varphi(ds)}{s^{d+1}d^{2d}} + O\left(\sum_{s=2}^{H}\left(\frac{H}{s}\right)^{d-1} 2^{\omega(s)}\right) \\
&= -(2H)^d \frac{d-1}{d^{2d}} \sum_{\substack{s=2 \\ s\in\mathcal{S}'}}^{\infty} \frac{\mu(s)\varphi(s)}{s^{d+1}} + O\left(H^d \sum_{s=H+1}^{\infty} \frac{\varphi(s)}{s^{d+1}} + \sum_{s=2}^{H}\left(\frac{H}{s}\right)^{d-1} 2^{\omega(s)}\right).
\end{aligned}$$

The error terms are handled as in the proof of the previous proposition. Finally, to complete the proof, we observe that

$$-\sum_{\substack{s=2 \\ s\in\mathcal{S}'}}^{\infty} \frac{\mu(s)\varphi(s)}{s^{d+1}} = 1 - \prod_{\substack{p\not\equiv 1(d) \\ p\neq d}} \left(1 - \frac{p-1}{p^{d+1}}\right).$$

□

Putting together Proposition 1, Proposition 2, and (1) establishes Theorem 1 in light of the fact that $\theta_d^\star = \theta_d - \alpha_d - \beta_d$.

Acknowledgement. This work represents a portion of the first author's honors thesis at California State University, Chico under the supervision of the second author. The authors would like to thank the Mathematics and Statistics Department for their support. In addition, the authors thank the anonymous referee for their helpful suggestions.

References

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

[2] 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.

[3] M. Ishida, *The Genus Fields of Algebraic Number Fields*, Lecture Notes in Mathematics, Vol. 555. Springer-Verlag, Berlin-New York, 1976.

[4] K. McGown and A. Tucker, Statistics of genus numbers of cubic fields, `arXiv:1611.07088`.