On the Number of Eisenstein Polynomials of Bounded Height

Randell Heyman
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
randell@unsw.edu.au

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

Abstract

We obtain a more precise version of an asymptotic formula of A. Dubickas for the number of monic Eisenstein polynomials of fixed degree $d$ and of height at most $H$, as $H \to \infty$. In particular, we give an explicit bound for the error term. We also obtain an asymptotic formula for arbitrary Eisenstein polynomials of height at most $H$.

1 Introduction

The Eisenstein criterion [4] is a simple well-known sufficient criterion to establish that an integer coefficient polynomial (and hence a polynomial with rational coefficients) is irreducible, see also [1]. We recall that

$$f(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$  \hspace{1cm} (1)

is called an Eisenstein polynomial if for some prime $p$ we have

(i) $p \mid a_i$ for $i = 0, \ldots, d - 1$, 

(ii) $p^2 \nmid a_0$.

(iii) $p \nmid a_d$.

For integers $d \geq 2$ and $H \geq 1$, we let $\mathcal{E}_d(H)$ be the set of all Eisenstein polynomials with $a_d = 1$ and of height at most $H$, that is, satisfying $\max\{|a_0|, \ldots, |a_{d-1}|\} \leq H$.

Dubickas [3] has given an asymptotic formula for the cardinality $E_d(H) = \#\mathcal{E}_d(H)$, see also [2]. Here we address this question again and obtain a more precise version of this result with an explicit error term. Using techniques different to those in [3], we also obtain an asymptotic formula for the number of polynomials, whether monic or non-monic, that satisfy the Eisenstein criterion.

**Theorem 1.** We have,

$$E_d(H) = \vartheta_d 2^d H^d + \begin{cases} O\left( H^{d-1} \right), & \text{if } d > 2, \\ O\left( H(H \log H)^2 \right), & \text{if } d = 2, \end{cases}$$

where

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

We remark that our argument is quite similar to that of Dubickas [3], and in fact the method of [3] can also produce a bound on the error term in an asymptotic formula for $E_d(H)$. However we truncate the underlying inclusion-exclusion formula differently. This allows us to get a better bound on the error term than that which follows from the approach of [3].

Furthermore, we obtain an asymptotic formula for the cardinality $F_d(H) = \#\mathcal{F}_d(H)$ of the set $\mathcal{F}_d(H)$ of Eisenstein polynomials of the form (1) of height at most $H$, that is, satisfying $\max\{|a_0|, \ldots, |a_d|\} \leq H$. This result does not seem to have any predecessors.

**Theorem 2.** We have,

$$F_d(H) = \rho_d 2^{d+1} H^{d+1} + \begin{cases} O\left( H^d \right), & \text{if } d > 2, \\ O\left( H^2 (H \log H)^2 \right), & \text{if } d = 2, \end{cases}$$

where

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

As usual, for any integer \( n \geq 1 \), let \( \omega(n) \), \( \tau(n) \) and \( \varphi(n) \) be the number of distinct prime factors, the number of divisors and Euler function respectively (we also set \( \omega(1) = 0 \)).

We also use \( \mu \) to denote the Möbius function, that is,

\[
\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is square free,} \\ 0 & \text{if } n \text{ otherwise.} \end{cases}
\]

Throughout the paper, the implied constants in the symbol ‘\( O \)’ may occasionally, where obvious, depend on the degree \( d \). We recall that the notation \( U = O(V) \) is equivalent to the assertion that the inequality \( |U| \leq c|V| \) holds for some constant \( c > 0 \). In addition to using \( d \) to indicate the degree of a polynomial we retain the traditional use of \( d \), the divisor, as the index of summation in some well-known identities.

3 Preparations

We start by deriving a formula for the number of monic polynomials for which a given positive number satisfies conditions that are similar, but not equivalent, to the Eisenstein criterion. Let \( s \) be a positive integer. Let \( G_d(s, H) \) be the set of monic polynomials (1) of height at most \( H \) and such that

(i) \( s \mid a_i \) for \( i = 0, \ldots, d - 1 \),

(ii) \( \gcd(a_0/s, s) = 1 \).

It is easy to see that \( \text{[Lemma 2]} \) immediately implies the following result.

**Lemma 3.** For \( s \leq H \), we have

\[
\#G_d(s, H) = \frac{2^dH^d\varphi(s)}{s^{d+1}} + O\left(\frac{H^{d-1}\omega(s)}{s^{d-1}}\right).
\]

We now derive a version of Lemma 3 for arbitrary polynomials. Let \( H_d(s, H) \) be the set of polynomials (1) of height at most \( H \) and such that
(i) \( s \mid a_i \) for \( i = 0, \ldots, d - 1 \),
(ii) \( \gcd(a_0/s, s) = 1 \),
(iii) \( \gcd(a_d, s) = 1 \).

We also use the well-known identity

\[
\sum_{d \mid s} \frac{\mu(d)}{d} = \frac{\varphi(s)}{s},
\]

see [5, Section 16.3].

We now define the following generalisation of the Euler function,

\[
\varphi(s, H) = \sum_{\substack{|a| \leq H \\ \gcd(a, s) = 1}} 1,
\]

and use the following well-known consequence of the sieve of Eratosthenes.

**Lemma 4.** For any integer \( s \geq 1 \), we have

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

**Proof.** Using the inclusion-exclusion principle we write

\[
\varphi(s, H) = \sum_{d \mid s} \mu(d) \sum_{\substack{|a| \leq H \\ d \mid a}} 1 = \sum_{d \mid s} \mu(d) \left( 2 \left\lfloor \frac{H}{d} \right\rfloor + 1 \right).
\]

Therefore,

\[
\varphi(s, H) = \sum_{d \mid s} \mu(d) \left( \frac{2H}{d} + O(1) \right) = 2H \sum_{d \mid s} \frac{\mu(d)}{d} + O \left( \sum_{d \mid s} |\mu(d)| \right).
\]

Recalling (2) and that

\[
\sum_{d \mid s} |\mu(d)| = 2^{\omega(s)},
\]

see [5, Theorem 264], we obtain the desired result. \( \square \)
We also recall that
\[ 2^{\omega(s)} \leq \tau(s) = s^{o(1)} \tag{3} \]
as \( s \to \infty \), see [5, Theorem 317].

Next we obtain an asymptotic formula for \( \#H_d(s, H) \).

**Lemma 5.** For \( s \leq H \), we have
\[
\#H_d(s, H) = \frac{2^{d+1}H^{d+1} \varphi^2(s)}{s^{d+2}} + O \left( \frac{H^d}{s^{d-1}} 2^{\omega(s)} \right).
\]

**Proof.** Fix a \( d > 1 \). For every \( i = 1, \ldots, d-1 \), the number of admissible values of \( a_i \) (that is, with \( |a_i| \leq H \) and \( s \mid a_i \)) is equal to
\[
2 \left\lfloor \frac{H}{s} \right\rfloor + 1 = \frac{2H}{s} + O(1). \tag{4}
\]

We now consider the admissible values of \( a_0 \). Writing \( a_0 = sm \) with an integer \( m \) satisfying \( |m| \leq H/s \) and \( \gcd(m, s) = 1 \) we see from Lemma 4 that \( a_0 \) takes
\[
\varphi(s, \lfloor H/s \rfloor) = \frac{2H\varphi(s)}{s^2} + O \left( 2^{\omega(s)} \right) \tag{5}
\]
distinct values.

Lemma 4 also implies that \( a_d \) takes
\[
\varphi(s, H) = \frac{2H\varphi(s)}{s} + O \left( 2^{\omega(s)} \right) \tag{6}
\]
distinct values.

Combining (4), (5) and (6) we obtain
\[
\#H_d(s, H) = \left( \frac{2H}{s} + O(1) \right)^{d-1} \left( \frac{2H\varphi(s)}{s^2} + O \left( 2^{\omega(s)} \right) \right) \left( \frac{2H\varphi(s)}{s} + O \left( 2^{\omega(s)} \right) \right).
\]

\[
= \left( \left( \frac{2H}{s} \right)^{d-1} + O \left( \left( \frac{H}{s} \right)^{d-2} \right) \right) \left( \frac{2H\varphi(s)}{s^2} + O \left( 2^{\omega(s)} \right) \right) \left( \frac{2H\varphi(s)}{s} + O \left( 2^{\omega(s)} \right) \right). \tag{7}
\]
Hence, using the trivial bound $\varphi(s) \leq s$ and that by (3) we have $2^{\omega(s)} = O(H)$, we see that
\[
\left(\frac{2H \varphi(s)}{s^2} + O(2^{\omega(s)})\right) \left(\frac{2H \varphi(s)}{s} + O(2^{\omega(s)})\right) = \frac{4H^2 \varphi^2(s)}{s^3} + O(H2^{\omega(s)}).
\]
Substituting into (7), and using that $\varphi(s) \leq s$ again, we obtain
\[
\#\mathcal{H}_d(s, H) = \frac{2d+1H^{d+1} \varphi^2(s)}{s^{d+2}} + O\left(\frac{H^d}{s^{d-1}} + \frac{H^{d-1}}{s^{d-2}} 2^{\omega(s)} + \frac{H^d}{s^{d-1}} 2^{\omega(s)}\right).
\]
Taking into account that $s \leq H$, we conclude the proof. \hfill \Box

4 Proof of Theorem 1

We now prove the main result for monic Eisenstein polynomials. The inclusion-exclusion principle implies that
\[
E_d(H) = -\sum_{s=2}^{H} \mu(s) \#\mathcal{G}_d(s, H).
\]
Substituting the asymptotic formula of Lemma 3 for $\#\mathcal{G}_d(s, H)$, yields
\[
E_d(H) = -\sum_{s=2}^{H} \mu(s) \left(\frac{2d+1H^{d+1} \varphi(s)}{s^{d+1}}\right) + O\left(\sum_{s=2}^{H} \left(\frac{H}{s}\right)^{d-1} 2^{\omega(s)}\right)
\]
\[
= -2dH^d \sum_{s=2}^{\infty} \frac{\mu(s) \varphi(s)}{s^{d+1}} + O\left(H^d \sum_{s=H+1}^{\infty} \frac{\varphi(s)}{s^{d+1}} + H^{d-1} \sum_{s=2}^{H} \frac{2^{\omega(s)}}{s^{d-1}}\right) \tag{8}
\]
(since $\varphi(s) \leq s$, the series in the main term converges absolutely for $d \geq 2$). Furthermore, since $\mu(s)\varphi(s)/s^{d+1}$ is a multiplicative function, it follows that
\[
-\sum_{s=2}^{\infty} \frac{\mu(s) \varphi(s)}{s^{d+1}} = 1 - \sum_{s=1}^{\infty} \frac{\mu(s) \varphi(s)}{s^{d+1}}
\]
\[
= 1 - \prod_{p \text{ prime}} \left(1 - \frac{\varphi(p)}{p^{d+1}}\right) = 1 - \prod_{p \text{ prime}} \left(1 - \frac{p-1}{p^{d+1}}\right). \tag{9}
\]
We also have
\[
\sum_{s=H+1}^{\infty} \frac{\varphi(s)}{s^{d+1}} \leq \sum_{s=H+1}^{\infty} \frac{1}{s^d} = O\left(H^{-d+1}\right). \tag{10}
\]
Recalling (3), for \( d > 2 \) we immediately obtain
\[
\sum_{s=2}^{H} \frac{2^{\omega(s)}}{s^{d-1}} = O(1). \tag{11}
\]

For \( d = 2 \) we recall that
\[
\sum_{s \leq t} 2^{\omega(s)} \leq \sum_{s \leq t} \tau(s) = (1 + o(1)) t \log t
\]
as \( t \to \infty \), see [5, Theorem 320].

Thus, via partial summation, we derive
\[
\sum_{s=2}^{H} \frac{2^{\omega(s)}}{s} = O \left( \sum_{t=2}^{H} \frac{\log t}{t} \right) = O \left( (\log H)^2 \right). \tag{12}
\]

Substituting (9), (10), (11) and (12) in (8), we conclude the proof.

5 Proof of Theorem 2

The inclusion exclusion principle implies that
\[
\# \mathcal{F}_d(H) = - \sum_{s=2}^{H} \mu(s) \# \mathcal{H}_d(s, H).
\]

Using the asymptotic formula of Lemma 5 yields
\[
\# \mathcal{F}_d(H) = - \sum_{s=2}^{H} \mu(s) \left( \frac{2^{d+1} H^{d+1} \varphi^2(s)}{s^{d+2}} \right) + O \left( \sum_{s=2}^{H} \frac{H^d 2^{\omega(s)}}{s^{d-1}} \right)
\]
\[
= -2^{d+1} H^{d+1} \sum_{s=2}^{\infty} \frac{\mu(s) \varphi^2(s)}{s^{d+2}}
\]
\[
+ O \left( H^{d+1} \sum_{s=H+1}^{\infty} \frac{\varphi^2(s)}{s^{d+2}} + H^d \sum_{s=2}^{H} \frac{2^{\omega(s)}}{s^{d-1}} \right) \tag{13}
\]
(since \( \varphi(s) \leq s \), the series in the main term converges absolutely for \( d \geq 2 \)).

In a similar manner to that used for (9), we note that \( \mu(s) \varphi^2(s)/s^{d+2} \) is a
multiplicative function, so it follows that

\[- \sum_{s=2}^{\infty} \frac{\mu(s) \varphi^2(s)}{s^{d+2}} = 1 - \sum_{s=1}^{\infty} \frac{\mu(s) \varphi^2(s)}{s^{d+2}} = 1 - \prod_{p \text{ prime}} \left(1 - \frac{\varphi^2(p)}{p^{d+2}}\right) = 1 - \prod_{p \text{ prime}} \left(1 - \frac{(p - 1)^2}{p^{d+2}}\right).\]  

(14)

Since \(\varphi(s) \leq s\), we also have

\[\sum_{s=H+1}^{\infty} \frac{\varphi^2(s)}{s^{d+2}} \leq \sum_{s=H+1}^{\infty} \frac{1}{s^{d}} = O\left(H^{-d+1}\right).\]

(15)

Substituting (14), (15), in (13), and recalling (11) and (12), we conclude the proof.

6 Further Comments on \(\vartheta_d\) and \(\rho_d\)

Clearly, as \(d \to \infty\),

\[\vartheta_d = 1 - \prod_{p \text{ prime}} \left(1 - \frac{p - 1}{p^{d+1}}\right) = \sum_{s=2}^{\infty} \frac{\mu(s) \varphi(s)}{s^{d+1}}\]

\[= \frac{1}{2d+1} - \frac{2}{3d+1} + \sum_{s=4}^{\infty} \frac{\mu(s) \varphi(s)}{s^{d}} = \frac{1}{2d+1} - \frac{2}{3d+1} + O\left(\int_{3}^{\infty} \frac{1}{\sigma^{d+1}} d\sigma\right)\]

\[= \frac{1}{2d+1} - \frac{2}{3d+1} + O\left(\frac{1}{d^{3d}}\right) = \frac{1}{2d+1} + O\left(\frac{1}{3d}\right).\]

Similarly,

\[\rho_d = \frac{1}{2d+2} + O\left(\frac{1}{3d}\right), \quad d \to \infty.\]

We have computed in Table [II] the approximate values of \(\vartheta_d\) and \(\rho_d\) for \(d = 2, \ldots, 10\). The first 10,000 primes have been used in the calculations. The values of \(\vartheta_d\) are consistent with those given in [3], but the table of the values of \(\rho_d\) seems to be new.
Table 1: Approximate values of $\vartheta_d$ and $\rho_d$ for $d = 2, \ldots, 10.$

| $d$ | $\vartheta_d$ | $\rho_d$ |
|-----|---------------|----------|
| 2   | 0.2515        | 0.1677   |
| 3   | 0.0953        | 0.0556   |
| 4   | 0.0409        | 0.0224   |
| 5   | 0.0186        | 0.0099   |
| 6   | 0.0088        | 0.0046   |
| 7   | 0.0042        | 0.0022   |
| 8   | 0.0021        | 0.0010   |
| 9   | 0.0010        | 0.0005   |
| 10  | 0.0005        | 0.0003   |

References

[1] D. A. Cox, ‘Why Eisenstein proved the Eisenstein criterion and why Schonemann discovered it first’, Amer. Math. Monthly 118 (2011), 3–21.

[2] D. E. Dobbs and L. E. Johnson, ‘On the probability that Eisenstein’s criterion applies to an arbitrary irreducible polynomial’, Proc. of 3rd Intern. Conf. Advances in Commutative Ring Theory, Fez, Morocco, Lecture Notes in Pure and Appl. Math., 205, Dekker, New York, 1999, 241–256.

[3] A. Dubickas, ‘Polynomials irreducible by Eisenstein’s criterion’, Appl. Algebra Engin. Comm. Comput., 14 (2003), 127–132.

[4] F. G. Eisenstein, Mathematische Werke, Vol. II, AMS Chelsea, Providence, RI, 1989, 536–555.

[5] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers (6th Edition), Oxford Univ. Press, Oxford, 2008.