POLYNOMIAL DENSITIES AND HEILBRONN'S CRITERION

ALEXIS HIBBLER, KEVIN J. MCGOWN, AND ENRIQUE TREVIÑO

Abstract. Heilbronn gave a sufficient condition for a number field with a totally ramified prime to fail to be norm-Euclidean. We say that Heilbronn's criterion applies to a polynomial f if it applies to the number field $K = \mathbb{Q}[x]/(f)$ generated by f.

Suppose $n \geq 3$ is odd and $p \geq 5$ is prime with $\gcd(p-1, n) = 1$. Let $\mathcal{F}_{p,n}$ denote the collection of monic polynomials $f \in \mathbb{Z}[x]$ of degree n that are Eisenstein at the prime p. We order our polynomials by the natural height $\mathrm{Ht}(f)$. Define $\delta_{p,n}(X)$ to be the proportion of polynomials $f \in \mathcal{F}_{p,n}$ with $\mathrm{Ht}(f) \leq X$ for which Heilbronn's criterion applies. One has

$$\liminf_{X\to\infty} \delta_{p,n}(X) \geq \max\left\{ \frac{2}{27}\,,\ 1 - \varepsilon(p) \right\}\,,$$

where $\varepsilon(p) \to 0$ and is effectively computable. In particular, the lower density tends to 1 as $p \to \infty$ uniformly in n. We also give a version of this result where we weaken the condition on $\gcd(p-1, n)$.

As a corollary, we show that given an integer $n \geq 2$, a positive proportion of Eisenstein polynomials of degree n fail to generate norm-Euclidean fields.

1. Introduction

We are interested in proving statistical results concerning polynomials with integer coefficents. Let $\mathcal{F} \subseteq \mathbb{Z}[x]$. Before proceeding, we must have an ordering on our set, which is typically endowed by a height function. Let $\mathcal{F} \subseteq \mathbb{Z}[x]$ be a collection of polynomials. Most importantly, a height function $H : \mathcal{F} \to \mathbb{R}_{\geq 0}$ should satisfy the following property: For any $X > 0$, the set

$$\{ f \in \mathcal{F} \mid H(f) \leq X \}$$

is finite. Given

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]\,,$$

we define the standard height function

$$\mathrm{Ht}(f) = \max\{|a_0|, |a_1|, \ldots, |a_n|\}\,.$$

One might consider other height functions, but here we will always use $\mathrm{Ht}(f)$ as defined above. Given a subset $\mathcal{F} \subseteq \mathbb{Z}[x]$, we define the associated counting

Date: September 2025.

Key words and phrases. Eisenstein polynomials, Heilbronn's criterion, norm-Euclidean fields, polynomial statistics.

function

$$N(X) = \#\{f \in \mathcal{F} \mid \mathrm{Ht}(f) \le X\}\,.$$

Given a distinguished subset $\mathcal{F}^* \subseteq \mathcal{F}$, we let $\delta(X)$ denote the proportion of elements of $\mathcal{F}$ that belong to $\mathcal{F}^*$; that is

$$\delta(X) = \frac{N^*(X)}{N(X)}\,,$$

where we have written $N^*(X)$ to denote the counting function associated to $\mathcal{F}^*$. One then defines the density of $\mathcal{F}^*$ in $\mathcal{F}$ to be

$$\delta := \lim_{X\to\infty} \delta(X)\,,$$

provided the limit exists. In cases where it is difficult to prove this limit exists, one might seek bounds on the lower and upper densities:

$$\underline{\delta} := \liminf_{X\to\infty} \delta(X)\,, \quad \overline{\delta} := \limsup_{X\to\infty} \delta(X)\,.$$

We begin with an important example. Fix a positive integer n. Denote by $\mathcal{F}_n$ the collection of all monic polynomials in $\mathbb{Z}[x]$ of degree n. It is easy to show that

$$N(X) \sim (2X)^n\,.$$

Let $\mathcal{F}_n^*$ be the subset of $\mathcal{F}_n$ consisting of Eisenstein polynomials. Dubickas considers the probability that a randomly chosen polynomial of degree n is Eisenstein (see [5]). Indeed, he proves that the associated density exists and that it equals

$$\delta = 1 - \prod_p \left(1 - \frac{1}{p^n} + \frac{1}{p^{n+1}}\right)\,. \tag{1.1}$$

This appears to be a topic of interest, as this paper led to the papers [12, 11, 17, 14], among others.

On the other hand, one of the central objects of study in algebraic number theory are number fields. As an Eisenstein polynomial $f \in \mathcal{F}_n^*$ is always irreducible, it generates a number field K of degree n. That is, if we define $K = \mathbb{Q}[x]/(f)$ then one has $[K:\mathbb{Q}] = n$. We can ask various questions about properties of this number field as we vary the polynomial. As is standard, we let $\mathcal{O}_K$ denote the ring of integers in K, and let $N : K \to \mathbb{Q}$ denote the norm map.

One classical question is regarding when the Euclidean algorithm holds in K. We call a number field K norm-Euclidean if for every $\alpha, \beta \in \mathcal{O}_K$, $\beta \neq 0$, there exists $\gamma, \rho \in \mathcal{O}_K$ such that $\alpha = \gamma\beta + \rho$ and $|N(\rho)| < |N(\gamma)|$. This is the generalization of the division property of $\mathbb{Z}$, which ensures that the Euclidean algorithm terminates after a finite number of steps. The statement that K is norm-Euclidean is equivalent to $\mathcal{O}_K$ being a Euclidean domain with respect to the function $\partial(\alpha) = |N(\alpha)|$. The quadratic fields that are norm-Euclidean have been completely determined (see [4, 3, 1, 7]), but this has not been accomplished in full for any degree $n > 2$. The reader may be interested to consult the survey article [13].

One knows that all norm-Euclidean fields have class number one, but the converse is not true in general. Recall that K having class number one is equivalent to $\mathcal{O}_K$ being a unique factorization domain. We expect the norm-Euclidean property to be rather rare in general, but proving this is quite difficult. On the other hand, if K is generated by an Eisenstein polynomial, we actually have a tool available to us, due to the existence of a totally ramified prime. More specifically, if f is Eisenstein at the prime p, then p is totally ramified in K; that is, $(p) = \mathfrak{p}^n$ for some prime ideal $\mathfrak{p}$. The tool we refer to is as follows (see [8, 9, 10, 6]):

Lemma 1.1 (Heilbronn's criterion)**.** *Let K be a number field of degree n. Let p be a prime that is totally ramified in K. If we can write $p = a + b$ where $\{a, -b\}$ are not norms and a is an n-th power residue modulo p, then K is not norm-Euclidean.*

For clarity, recall that we refer to $a \in \mathbb{Z}$ as a norm (from $\mathcal{O}_K$) when there exists $\alpha \in \mathcal{O}_K$ such that $N(\alpha) = a$. Note that if n is odd, then b is a norm if and only if $-b$ is norm and hence one can simply write $\{a, b\}$ where we have written $\{a, -b\}$ in the lemma above. Additionally, note that the criterion never applies when $p = 2$ or $p = 3$, so we should always be considering $p \geq 5$ in our applications of this result.

A natural question to ask is: How often does Heilbronn's criterion apply to a number field K? One could ask this question in the case of all number fields of fixed degree, ordered by their discriminant. There are some results in this direction when $n = 3$ and $n = 5$ (see [16, 15]). However, such questions are intractable at present when $n > 5$ (see, for example, the introduction to [2]). On the other hand, if we consider the corresponding statistical questions for polynomials, then something can be said. For convenience, we will say Heilbronn's criterion applies to a polynomial $f \in \mathbb{Z}[x]$ if the criterion applies to the number field $K = \mathbb{Q}[x]/(f)$. We establish the following result:

Theorem 1.2. *Suppose $n \geq 3$ is an odd integer and $p \geq 5$ is a prime with $\gcd(p-1, n) = 1$. Let $\mathcal{F}_{p,n}$ denote the collection of monic polynomials $f \in \mathbb{Z}[x]$ of degree n that are Eisenstein at the prime p. Define $\delta_{p,n}(X)$ to be the proportion of polynomials $f \in \mathcal{F}_{p,n}$ with $\mathrm{Ht}(f) \leq X$ for which Heilbronn's criterion applies. One has*

$$\liminf_{X\to\infty} \delta_{p,n}(X) \geq \max\left\{\frac{2}{27}\,,\ 1 - \varepsilon(p)\right\}.$$

Here $\varepsilon(p) \to 0$ and is effectively computable.

When p is large, there are many ways to write $p = a + b$ and hence determining the exact density of polynomials that satisfy Heilbronn's criterion is likely very difficult. However, the previous theorem says that the lower density tends to 1 as $p \to \infty$, uniformly in the variable n.

As a result, we immediately obtain the following consequence: When $n \geq 3$ is odd, a positive proportion of Eisenstein polynomials of degree n fail to generate norm-Euclidean fields.

The condition from Theorem 1.2 that $\gcd(p-1, n) = 1$ is not a severe restriction as there are infinitely many primes p that satisfy this condition for each fixed n. Nonetheless, we show that we can relax this condition at the expense of considering larger primes. This will allow us to deal with the case where n is even.

Theorem 1.3. *Suppose $n \geq 2$ and $p \geq 5$ is a prime with*

$$\gcd(p-1, n) < \frac{p^{1/2}}{(\log p)^2}\,.$$

Define $\delta_{p,n}(X)$ as in Theorem 1.2. One has

$$\liminf_{X\to\infty} \delta_{p,n}(X) \geq 1 - \hat{\varepsilon}(p)\,,$$

where $\hat{\varepsilon}(p) \to 0$ and is effectively computable.

Corollary 1.4. *Fix an integer $n \geq 2$. A positive proportion of Eisenstein polynomials of degree n fail to generate norm-Euclidean fields.*

In §2 we discuss Eisenstein polynomials and Heilbronn's criterion, and outline the strategy of our proof. In addition, we establish some preliminary lemmas. In the case where the proofs are very short, we err on the side of giving proofs of known results for the sake of completeness. In §3 we prove our main counting result for Eisenstein polynomials satisfying certain other local conditions. In §4 we prove a formula for the relevant local densities, which is then used to establish the necessary bounds. In §5 we put everything together and prove Theorem 1.2. Finally, in §6, we prove Theorem 1.3.

2. Eisenstein polynomials and Heilbronn's criterion

Let $f \in \mathbb{Z}[x]$ and write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0\,.$$

We say that f is Eisenstein at the prime p (or p-Eisenstein for short) if $p \mid a_i$ for $i = 0, \ldots, n-1$, $p \nmid a_n$, and $p^2 \nmid a_0$. We refer to a polynomial as Eisenstein, if it is p-Eisenstein for some prime p. It is well-known that Eisenstein polynomials are irreducible in $\mathbb{Z}[x]$. We will always assume f is monic (i.e., $a_n = 1$) which makes the condition at a_n unnecessary.

We will write $\mathbb{Z}[x]_{\mathrm{mon}}$ for the collection of monic polynomials with coefficents in $\mathbb{Z}$. Throughout the rest of this section we will always consider $f \in \mathbb{Z}[x]_{\mathrm{mon}}$ and set $K = \mathbb{Q}[x]/(f)$. The letters p, q will always denote primes in $\mathbb{Z}$.

We outline our strategy. Let $f \in \mathbb{Z}[x]_{\mathrm{mon}}$ be a p-Eisenstein polynomial with $p \geq 5$. By Lemma 2.1 below, we know that p is totally ramified in K. This opens up the possibility of applying Heilbronn's criterion (i.e., Lemma 1.1). We can simplify matters by assuming $\gcd(n, p-1) = 1$, which guarantees that every integer is an n-th power residue modulo p. As mentioned earlier, this will not be a severe restriction as there are infinitely many primes p that satisfy this condition for each fixed n.

Given two primes $q_1 < q_2 < p$ we write $p = uq_1 + vq_2$ for $(u, q_1) = 1$ and $(u, q_2) = 1$. This is possible when p is large enough compared to q_1, q_2 (see Lemma 2.2). If q_1 and q_2 are not norms from K, then this is enough to invoke Heilbronn's criterion. Moreover, the condition that $f(x)$ has no roots modulo q is sufficient to guarantee that q is not a norm (see Lemma 2.3).

Lemma 2.1. *If $f(x)$ is p-Eisenstein, then p is totally ramified in K.*

Proof. Let $\mathfrak{p}$ be a prime in K over p, and set $e = v_{\mathfrak{p}}(p)$. We aim to show $e = n$. Of course, a priori one has $e \leq n$. Let α be a root of f in K. From $f(\alpha) = 0$, using the p-Eisenstein condition, we find $\mathfrak{p}$ divides (α), and therefore $v_{\mathfrak{p}}(\alpha^n) \geq n$. Moreover, $v_{\mathfrak{p}}(a_0) = e$ and $v_{\mathfrak{p}}(a_i\alpha^i) \geq e + 1$ for $i = 1, \ldots, n-1$, which implies $v_{\mathfrak{p}}(\alpha^n) = e$. It follows that $n \leq e$, completing the proof. □

Lemma 2.2. *Let $q_1 < q_2$ be primes. Let $p \geq q_1^2 q_2^2$. Then there exist $u, v \in \mathbb{Z}^+$ such that*

(1) $p = uq_1 + vq_2$,
(2) $q_1 \nmid u$, $q_2 \nmid v$.

Proof. Let $r_1 \in \{1, 2, \ldots, q_1 - 1\}$ and $r_2 \in \{1, 2, \ldots, q_2 - 1\}$ be fixed. Then $p \geq q_1^2 q_2^2$ implies

$$p - r_1q_1 - r_2q_2 \geq q_1^2q_2^2 - (q_1 - 1)q_1 - (q_2 - 1)q_2 \geq (q_1^2 - 1)(q_2^2 - 1).$$

By the Frobenius coin-exchange problem, since q_1^2 and q_2^2 are coprime, and

$$p - r_1q_1 - r_2q_2 \geq (q_1^2 - 1)(q_2^2 - 1),$$

there exist nonnegative integers t_1, t_2 such that

$$p - r_1q_1 - r_2q_2 = q_1^2t_1 + q_2^2t_2.$$

Then

$$p = q_1(q_1t_1 + r_1) + q_2(q_2t_2 + r_2) = q_1u + q_2v,$$

where $u = q_1t_1 + r_1$ and $v = q_2t_2 + r_2$ with $q_1 \nmid u$ and $q_2 \nmid v$. □

Lemma 2.3. *Let q be prime. If q is a norm from K, then $f(x)$ has a root in $\mathbb{F}_q$.*

Proof. Suppose q is a norm. Then there is a prime $\mathfrak{q}$ in K such that $N(\mathfrak{q}) = q$. This means $|\mathcal{O}_K/\mathfrak{q}| = q$ and hence $\mathcal{O}_K/\mathfrak{q} \cong \mathbb{F}_q$. Let α be a root of $f(x)$ in K and consider $\overline{\alpha}$, the image of α under the reduction map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{q}$. Since $f(\alpha) = 0$, we must have $f(\overline{\alpha}) = 0$ in $\mathbb{F}_q$, which proves the result. □

Proof of Lemma 1.1. Suppose p is totally ramified and we can write $p = a+b$ as in the statement of the result. By way of contradiction, suppose K is norm-Euclidean. By hypothesis, $(p) = \mathfrak{p}^n$, where $N(\mathfrak{p}) = p$. It follows that $p = u\pi^n$ in K, for some $u \in \mathcal{O}_K^\times$ and some $\pi \in \mathcal{O}_K$ irreducible with $N(\pi) = p$. Since a is an n-th power residue modulo n, there exists $x \in \mathbb{Z}$ such that $x^n \equiv a \pmod p$. Using the norm-Euclidean condition, we find $x = \gamma\pi + \rho$ for some $\gamma, \rho \in \mathcal{O}_K$ with $|N(\rho)| < |N(\pi)| = p$. We have $x \equiv \rho \pmod \pi$ and hence $x \equiv \rho^\sigma \pmod \pi$ for any embedding $\sigma : K \to \mathbb{C}$. This leads to $a \equiv x^n \equiv N(\rho) \pmod p$. We have $0 < a < p$ and $-p < N(\rho) < p$. Thus either $N(\rho) = a$ or $N(\rho) + p = a$. This implies one of $\{a, -b\}$ is a norm, a contradiction. $\square$

3. Counting p-Eisenstein polynomials with local specifications

Given $a = (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n$, we define

$$\mathrm{Ht}(a) = \max\{|a_0|, \dots, |a_{n-1}|\}$$

so that it agrees with our polynomial height. The next result is what allows us to count polynomials of bounded height with local specifications. This type of result is certainly well-known, but the proof is short and so we include it for the sake of completeness.

Lemma 3.1. *Let S be a subset of $(\mathbb{Z}/m\mathbb{Z})^n$. We have*

$$\#\{a \in \mathbb{Z}^n \mid a \mod m \in S\,,\ \mathrm{Ht}(a) \le X\} = \frac{|S|}{m^n}(2X)^n + O\left(n2^n m(2X)^{n-1}\right)\,.$$

Proof. Let $\mathcal{A} := [-X, X]^n \cap \mathbb{Z}^n$. Choose the maximal $k \in \mathbb{Z}^+$ such that

$$\mathcal{B} := (-km, km]^n \cap \mathbb{Z}^n \subseteq \mathcal{A}\,.$$

The set $\mathcal{B}$ is chosen so that

$$\#\{a \in \mathcal{B} \mid a \mod m \in S\} = |S|(2k)^n$$

Using the Binomial Theorem, one has

$$\left(\frac{X}{m}\right)^n \ge k^n \ge \left(\frac{X}{m} - 1\right)^n = \left(\frac{X}{m}\right)^n + O\left(n2^n\left(\frac{X}{m}\right)^{n-1}\right)\,,$$

and therefore

$$\#\{a \in \mathcal{B} \mid a \mod m \in S\} = \frac{|S|}{m^n}(2X)^n + O\left(n2^n m(2X)^{n-1}\right)\,.$$

Next one bounds

$$\#(\mathcal{A} \setminus \mathcal{B}) \le (2X+1)^n - (2km)^n \ll n2^n m(2X)^{n-1}\,.$$

The result follows. $\square$

Remark 3.2. *One can think of the quantity $|S|/m^n$ in the statement of the previous lemma as a density in $(\mathbb{Z}/m\mathbb{Z})^n$, and using the Chinese Remainder Theorem, we can recover it as a product of local densities at the prime powers dividing m.*

Our typical application of Lemma 3.1 will be to impose a condition modulo q_1 and q_2, as well as the p-Eisenstein condition, which is a condition modulo p^2. In this case, the modulus is given as $m = q_1 q_2 p^2$.

Before proceeding, we require a couple definitions. First we define

$$E_p(n) := \frac{1}{p^n} - \frac{1}{p^{n+1}}, \tag{3.1}$$

which is the p-Eisenstein density that contributes to (1.1). Secondly, we write $C_q(n)$ to denote — the number of $(a_0, \dots, a_{n-1}) \in (\mathbb{Z}/q\mathbb{Z})^n$ such that the corresponding polynomial in $\mathbb{F}_q[x]$ has no roots in $\mathbb{F}_q$ — divided by q^n. We are now ready to prove the following result, which will be used in the proof of Theorem 1.2.

Proposition 3.3. *Let $n \in \mathbb{Z}^+$. Suppose $q_1 < \cdots < q_t < p$ are primes. Let $\mathcal{F}_{p,n}$ denote the collection of monic polynomials $f \in \mathbb{Z}[x]$ of degree n that are Eisenstein at the prime p. The number of polynomials $f \in \mathcal{F}_{p,n}$ with $\mathrm{Ht}(f) \le X$ for which f has no roots in $\mathbb{F}_q$ for all $q \in \{q_1, \dots, q_t\}$ equals*

$$E_p(n) \left(\prod_{i=1}^{t} C_{q_i}(n) \right) (2X)^n + O\left(n 2^n q_1 \dots q_t p^2 (2X)^{n-1} \right) .$$

Proof. This is an application of Lemma 3.1 with the modulus $m = q_1 \dots q_t p^2$. By Remark 3.2 we can determine the density $|S|/m^n$ for each prime power separately. The condition that f is p-Eisenstein corresponds to

$$\begin{aligned} &a_0 \mod p^2 \in \{p, 2p, \dots, (p-1)p\}, \\ &a_i \mod p^2 \in \{0, p, \dots, (p-1)p\}, \ i = 1, \dots, p-1 . \end{aligned}$$

Therefore the density mod p^2 equals $(p-1)p^{n-1}/p^{2n}$ in agreement with (3.1). The values of $C_q(n)$ are correct tautologically. ∎

Remark 3.4. *In Proposition 3.3, if one wants to specify that for certain primes q, the condition described in the statement does not hold, then one simply replaces $C_q(n)$ with $1 - C_q(n)$.*

4. Evaluation and estimation of the local densities

The following lemma gives a formula for our local density $C_p(n) = A_p(n)/p^n$. Here $C_p(n)$ is the quantity defined immediately before Proposition 3.3 and $A_p(n)$ is defined forthwith.

Lemma 4.1. *The number of monic polynomials in $\mathbb{F}_p[x]$ of degree n with no roots equals*

$$A_p(n) := \sum_{\substack{f \in \mathbb{F}_p[x]_{mon} \\ f \text{ has no roots} \\ \deg(f) = n}} 1 = \sum_{k=0}^{n} (-1)^k \binom{p}{k} p^{n-k} . \tag{4.1}$$

When $n \geq p$, this becomes

$$\left(1 - \frac{1}{p}\right)^p p^n .$$

Proof. The count proceeds by inclusion-exclusion. We start with all polynomials, then remove the polynomials that are multiples of $(x-a)$ for $a \in \mathbb{F}_p$. Therefore, we get that the number of monic polynomials in $\mathbb{F}_p[x]$ of degree n with no roots equals

$$\sum_{k=0}^{n} (-1)^k \binom{p}{k} p^{n-k}.$$

Note that as $\binom{p}{k} = 0$ whenever $k > p$, we find that for $n \geq p$, one has

$$\begin{aligned}\sum_{k=0}^{n} (-1)^k \binom{p}{k} p^{n-k} &= \sum_{k=0}^{p} (-1)^k \binom{p}{k} p^{n-k} \\ &= p^n \sum_{k=0}^{p} \binom{p}{k} \left(\frac{-1}{p}\right)^k = p^n \left(1 - \frac{1}{p}\right)^p .\end{aligned}$$

□

Finally, we require bounds on $C_p(n)$.

Lemma 4.2. *For $n \geq 2$ we have*

$$\frac{1}{4} \leq \frac{p^2-1}{3p^2} \leq C_p(n) \leq \frac{p-1}{2p} < \frac{1}{2} . \tag{4.2}$$

Proof. First note that $f(k) = \binom{p}{k}/p^k$ is a decreasing function. Indeed, for $k \leq p-1$

$$\frac{f(k)}{f(k+1)} = \frac{(k+1)p}{p-k} > 0,$$

so $f(k) > f(k+1)$ for all $k \leq p-1$. Since $f(k) = 0$ for $k > p$, and $f(k) > 0$ for $k \leq p$, it follows that $f(k)$ is decreasing. Since $f(k)$ is decreasing and $A_p(n)$ is an alternating sum of positive decreasing terms, we get for $n \geq 2$,

$$\frac{\binom{p}{2}}{p^2} - \frac{\binom{p}{3}}{p^3} \leq \frac{A_p(n)}{p^n} \leq \frac{\binom{p}{2}}{p^2}.$$

□

5. Proof of the main result

Proof of Theorem 1.2. Adopt the notation from the statement of the theorem. Further, write $N_{p,n}(X)$ to denote the number of $f \in \mathcal{F}_{p,n}$ with $\mathrm{Ht}(f) \leq X$. We have $N_{p,n}(X) \sim E(p)(2X)^n$ where $E(p)$ is given in (3.1). This follows from [5] or alternatively, from Proposition 3.3 with $t = 0$.

First we will establish the lower bound $\liminf_{X\to\infty} \delta_{p,n}(X) \geq 2/27$. Assume $p \neq 7, 11, 19$. By Lemma 2.2, we can write $p = 2u + 3v$ with $(2, u) = 1$ and $(3, v) = 1$ for $p \geq 36$. One can then manually check that the only examples of primes up to 36 that cannot be expressed in such a way are

$p = 7, 11, 19$. Therefore, provided $f(x)$ has no roots in $\mathbb{F}_2$ or $\mathbb{F}_3$, Heilbronn's criterion applies. (Recall Lemma 1.1 and the discussion in §2.) Write $N^*_{p,n}(X)$ to denote the counting function for this collection of polynomials. Using Proposition 3.3 with $q_1 = 2$, $q_2 = 3$, we have

$$N^*_{p,n}(X) \sim E_p(n) C_2(n) C_3(n) (2X)^n \,,$$

and therefore, via Lemma 4.1 with $n \geq 3$, we find

$$\liminf_{X\to\infty} \delta_{n,p}(X) \geq C_2(n) C_3(n) = (1/4)(8/27) = 2/27 \,.$$

In the case where $p \in \{7, 11, 19\}$, we can write $p = 2u + 5v$ with $(2, u) = 1$ and $(5, v) = 1$. The same approach proves

$$\liminf_{X\to\infty} \delta_{n,p}(X) \geq C_2(n) C_5(n) \geq (1/4)(8/25) > 2/27 \,.$$

Indeed, by Lemma 4.2, as $n \geq 3$ is odd, one has $C_5(n) \geq 8/25$.

It remains to establish a lower bound $\delta_{p,n}(X) \geq 1 - \varepsilon(p)$ where $\varepsilon(p) \to 0$. We may assume that p is large. Choose Y maximal such that $Y^4 < p$. Let $q_1 < \cdots < q_t \leq Y$ be all the primes less than Y. In particular, Lemma 2.2 applies to any pair of primes in $Q := \{q_1, \ldots, q_t\}$ and we have $t = \pi(Y) \leq \pi(p^{1/4})$. Before proceeding with the final estimate, observe that by Lemma 4.2, one has

$$D := \max_{j=1,\ldots,t} \left\{ \frac{C(q_j)}{1 - C(q_j)} \right\} \leq 1 \,.$$

We wish to bound from above the number of p-Eisenstein polynomials with $\mathrm{Ht}(f) \leq X$ such that Heilbronn's criterion does not apply for any pair of primes in Q. This means that f has no root modulo q for at most one $q \in Q$. Using Proposition 3.3 in the situation where $\{q \in Q \mid f \text{ has a root in } \mathbb{F}_q\}$ equals Q, $Q \setminus \{q_1\}$, $Q \setminus \{q_2\}$, and so on, we obtain

$$\begin{aligned} 1 - &\liminf_{X\to\infty} \delta_{n,p}(X) \\ &\leq \prod_{i=1}^{t} (1 - C(q_i)) + \sum_{j=1}^{t} C(q_j) \left((1 - C(q_j))^{-1} \prod_{i=1}^{t} (1 - C(q_i) \right) \\ &\leq (1 + tD) \prod_{i=1}^{t} (1 - C(q_i)) \\ &\leq \left(1 + \pi\left(p^{1/4}\right)\right) \left(\frac{3}{4}\right)^{\pi(p^{1/4})} =: \varepsilon(p) \,. \end{aligned} \tag{5.1}$$

In the last step, we have used the fact that $C_p(n) \geq 1/4$ for $p \geq 2$ which follows from Lemma 4.2. ∎

6. Weakening the gcd condition

Proof of Theorem 1.3. Let $Y > 0$ be a parameter to be chosen later. Let $\mathcal{F}_{p,n}^*$ denote the subset of $\mathcal{F}_{p,n}$ consisting of polynomials for which there exist primes $q_1 < q_2 \le Y$ that are not norms in K. Applying the argument from the proof of Theorem 1.2 leading up to (5.1), we find that the lower density of $\mathcal{F}_{p,n}^*$ in $\mathcal{F}_{p,n}$ is bounded below by $1 - \hat{\varepsilon}(p)$ where

$$\hat{\varepsilon}(p) := (1 + \pi(Y)) \left(\frac{3}{4}\right)^{\pi(Y)} .$$

Set $g := \gcd(n, p-1)$. Next we show that Heilbronn's criterion applies when g is small enough compared to p. Let $f \in \mathcal{F}_{p,n}^*$. Then there exist primes $q_1 < q_2 \le Y$ that are not norms in K. Let ψ be a primitive Dirichlet character modulo p of order g, so that $\psi(u) = 1$ if and only if u is an n-th power residue modulo p. Note that there are $(p-1)/g$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ that are n-th power residues modulo p.

Set $X := p/q_1 - 2q_2$. Assume $Y < p/4$ so that $X < p$. For the moment, assume we can find a positive integer $u < X$ such that

$$(u, q_1) = 1\,, \quad q_1 u \equiv p \pmod{q_2}\,, \quad \psi(uq_1) = 1\,. \tag{6.1}$$

Since $u < p/q_1$, this implies we can write $p = uq_1 + vq_2$ with $v > 0$. Observe that Heilbronn's criterion applies, except possibly when $q_2 \mid v$. In the case where $q_2 \mid v$, we try $p = (u+q_2)q_1 + (v-q_1)q_2$, which works unless $q_1 \mid u+q_2$. If this is the case, we try $p = (u + 2q_2)q_1 + (v - 2q_1)q_2$ which is forced to work. Note that $u < X$ implies $u < u + q_2 < u + 2q_2 < p/q_1$ and hence the aforementioned expressions all involve positive integers.

Let us count the number of $u < X$ satisfying (6.1). Using standard techniques, this count equals

$$X \frac{q_1 - 1}{q_1} \cdot \frac{1}{q_2} \cdot \frac{1}{g} + O\left(m^{1/2} \log m\right), \tag{6.2}$$

where the error term comes from an application of the Pólya–Vinogradov inequality to a Dirichlet character of modulus $m = pq_1q_2$. Indeed, one sums the product of the following indicator functions over $u < X$:

$$\phi_0(u) = \begin{cases} 1 & \text{if } \gcd(u, q_1) = 1\,, \\ 0 & \text{if } \gcd(u, q_1) > 1\,, \end{cases}$$

$$\frac{1}{\phi(q_2)} \sum_{\chi \bmod q_2} \chi(uq_1)\chi(p)^{-1} = \begin{cases} 1 & \text{if } q_1 u \equiv p \pmod{q_2}\,, \\ 0 & \text{otherwise}\,, \end{cases}$$

$$\frac{1}{g} \sum_{k=1}^{g} \psi^k(uq_1) = \begin{cases} 1 & \text{if } \psi(uq_1) = 1\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

In the above ϕ_0 is the principal character modulo q_1, the sum $\sum_{\chi \bmod q_2}$ is taken over all Dirichlet characters modulo q_2, and ψ is the character modulo p defined above.

In order to guarantee that $u < X$ satisfying (6.1) exists, we must have the main term of (6.2) strictly greater than the error term. Using $q_1 \geq 2$ and the definition of X, the following condition suffices

$$\frac{1}{2}\left(\frac{p}{q_1 q_2} - 2\right)\frac{1}{g} > Cm^{1/2}\log m\,,$$

where C is the constant from Pólya–Vinogradov. Using $m = pq_1q_2$ with $q_1, q_2 \leq Y$, and some simple manipulation, the sufficient condition becomes

$$g < \frac{p^{1/2}}{2CY^3\log(pY^2)} - \frac{1}{Cp^{1/2}\log p}\,.$$

It suffices to prove the theorem when p is sufficiently large, and the result follows for large p upon choosing $Y = (\log p)^{1/4}$. □

Proof of Corollary 1.4. First suppose n is odd. From Theorem 1.2, we have

$$\liminf_{X\to\infty} \delta_{5,n}(X) \geq 2/27\,.$$

Since $\mathcal{F}_{5,n}$ is of positive density inside $\mathcal{F}_n$, the set of all monic $f \in \mathbb{Z}[x]$ with $\deg(f) = n$, the result follows.

Next, suppose n is even. We would like to invoke Theorem 1.3. We know there is a p_0 such that $\hat{\varepsilon}(p) < 1$ and $2 < \sqrt{p}/(\log p)^2$ when $p \geq p_0$. To invoke the theorem, we need a prime $p \geq p_0$ such that $\gcd(p-1, n)$ is small enough. We claim there exists infinitely many primes p satisfying the condition. Indeed, when $p \equiv -1 \pmod{2n}$ one finds $\gcd(p-1,n) = 2$. Choosing such a prime with $p \geq p_0$ allows us to conclude that

$$\liminf_{X\to\infty} \delta_{p,n}(X) > 0\,,$$

completing the proof. □

7. Acknowledgements

This research was conducted as part of the Research Experience for Undergraduates and Teachers program at California State University, Chico, supported by NSF grant DMS2244020. The authors would like to thank Paul Pollack for helpful conversations, including suggesting Theorem 1.3.

References

[1] E. S. Barnes and H. P. F. Swinnerton-Dyer. The inhomogeneous minima of binary quadratic forms. I. *Acta Math.*, 87:259–323, 1952.

[2] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[3] H. Chatland and H. Davenport. Euclid's algorithm in real quadratic fields. *Canad. J. Math.*, 2:289–296, 1950.

[4] H. Davenport. Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields. *Proc. London Math. Soc. (2)*, 53:65–82, 1951.

[5] Artūras Dubickas. Polynomials irreducible by Eisenstein's criterion. *Appl. Algebra Engrg. Comm. Comput.*, 14(2):127–132, 2003.

[6] Shigeki Egami. On finiteness of the numbers of Euclidean fields in some classes of number fields. *Tokyo J. Math.*, 7(1):183–198, 1984.
[7] R. B. Eggleton, C. B. Lacampagne, and J. L. Selfridge. Euclidean quadratic fields. *Amer. Math. Monthly*, 99(9):829–837, 1992.
[8] Paul Erdös and Chao Ko. Note on the Euclidean Algorithm. *J. London Math. Soc.*, 13(1):3–8, 1938.
[9] H. Heilbronn. On Euclid's algorithm in cubic self-conjugate fields. *Proc. Cambridge Philos. Soc.*, 46:377–382, 1950.
[10] H. Heilbronn. On Euclid's algorithm in cyclic fields. *Canad. J. Math.*, 3:257–268, 1951.
[11] Randell Heyman and Igor E. Shparlinski. On shifted Eisenstein polynomials. *Period. Math. Hungar.*, 69(2):170–181, 2014.
[12] Randell Heyman and Igora E. Shparlinski. On the number of Eisenstein polynomials of bounded height. *Appl. Algebra Engrg. Comm. Comput.*, 24(2):149–156, 2013.
[13] Franz Lemmermeyer. The Euclidean algorithm in algebraic number fields. *Exposition. Math.*, 13(5):385–416, 1995.
[14] Shilin Ma, Kevin J. McGown, Devon Rhodes, and Mathias Wanner. On the number of primes for which a polynomial is Eisenstein. *Integers*, 18:Paper No. A101, 7, 2018.
[15] Kevin J. McGown, Frank Thorne, and Amanda Tucker. Counting quintic fields with genus number one. *Math. Res. Lett.*, 30(2):577–588, 2023.
[16] Kevin J. McGown and Amanda Tucker. Statistics of genus numbers of cubic fields. *Ann. Inst. Fourier (Grenoble)*, 73(4):1365–1383, 2023.
[17] Giacomo Micheli and Reto Schnyder. The density of shifted and affine Eisenstein polynomials. *Proc. Amer. Math. Soc.*, 144(11):4651–4661, 2016.

Acera School, Winchester, MA 01890, USA
Email address: `alexis@aceraschool.org`

Department of Mathematics and Statistics, California State University, Chico, Chico, CA 95929, USA
Email address: `kmcgown@csuchico.edu`

Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, IL 60045, USA
Email address: `trevino@lakeforest.edu`