Journal of Integer Sequences, Vol. 17 (2014),
Article 14.2.4

On the Number of Polynomials of Bounded Height that Satisfy the Dumas Criterion

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

Abstract

We study integer coefficient polynomials of fixed degree and maximum height H that are irreducible by the Dumas criterion. We call such polynomials *Dumas polynomials*. We derive upper bounds on the number of Dumas polynomials as $H \to \infty$. We also show that, for a fixed degree, the density of Dumas polynomials in the set of all irreducible integer coefficient polynomials is strictly less than 1.

1 Introduction

The two most well-known polynomial irreducibility criteria based on coefficient primality divisibility are probably the Eisenstein criterion and the Dumas criterion. In the last decade and a half, results regarding the density of polynomials that satisfy the Eisenstein criterion have been obtained (see, for example, Dobbs and Johnson [2], Dubickas [3], and the author and Shparlinski [5, 6]). In this paper we explore densities of polynomials that satisfy the Dumas criterion. This criterion is a sufficient condition for polynomial irreducibility over $\mathbb{Z}$ (and hence $\mathbb{Q}$). It can be thought of as a generalization of the Eisenstein criterion since the Eisenstein criterion is an easy consequence of the Dumas criterion.

We can now state the Dumas criterion. Let

$$f(x) = \sum_{i=0}^{n} A_i x^i \in \mathbb{Z}[x] \tag{1}$$

be such that $A_0 A_n \neq 0$.

If the Newton polygon for f with respect to any prime is a single segment and contains no points with integer coordinates except the end points, then f is irreducible. The proof of the Dumas criterion is often based on the Newton diagram for a polynomial. The Newton diagram is similar to, but lesser known than, the Newton polygon. Construction of the Newton diagram and the proof of the Dumas criterion can be found in the book of Prasolov [8, Subsection 2.2.1]. Interested readers can also consult the 1906 paper by Dumas [4].

By way of example, the polynomial $f(x) = x^4 + 8$ with respect to the prime number 2 has a Newton polygon without integer coordinates (other than endpoints). Therefore f is irreducible by the Dumas criterion. By contrast, the reducible polynomial $f(x) = x^4 + 4$ cannot satisfy the Dumas criterion since the coordinate $(2, 2)$ or $(2, 0)$ will appear in any Newton polygon of f. So the determination of irreducibility using the Dumas criterion is not possible for $f(x) = x^4 + 4$. For integers $n \geq 2$ and $H \geq 1$ let $\mathcal{D}_n(H)$ be the number of Dumas polynomials of height at most H, that is, satisfying $\max\{|A_0|, \ldots, |A_n|\} \leq H$. Our main result is the following theorem.

Theorem 1. *We have*

$$\mathcal{D}_n(H) \leq (2H)^{n+1}\tau_n + \begin{cases} O\left(H^2(\log H)^2\right), & \text{if } n = 2; \\ O\left(H^n\right), & \text{if } n \geq 3, \end{cases}$$

where

$$\tau_n = \begin{cases} 1 - \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^2 \left(1 + \frac{2}{p}\right), & \text{if } n = 2; \\ 1 - \frac{1}{\zeta(n-1)}, & \text{if } n \geq 3. \end{cases}$$

We have already noted that the number of polynomials that satisfy the Eisenstein criterion, calculated by the author and Shparlinski [5], provides a lower bound on $\mathcal{D}_n(H)$. Specifically,

Lemma 2. *We have*

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

where

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

We note the appearance of values of the zeta function in the main term of the estimate in Theorem 1. This arises from the fact that estimates of the probability of k-tuples of positive integers being relatively prime play a major role in the proof of Theorem 1.

In Theorem 1 we also observe that the result for quadratics is quite different to the result for higher degree polynomials. For polynomials of degree greater than 2 we can use gcd conditions about the coefficients of the non-leading and non-constant terms to enumerate the number of Dumas polynomials. This is clearly not possible for quadratics and we are forced to consider the coefficients of the leading and non-constant terms as well.

2 Notation

Let $f(x)$ be as in (1). We define the height of the polynomial f as

$$H(f) = \max_{0 \leq i \leq n} |A_i|.$$

As usual the Riemann zeta function is given by

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s},$$

for all complex numbers s whose real part is greater than 1. We also recall that the notation $U = O(V)$ is equivalent to the assertion that the inequality $|U| \leq c|V|$ holds for some constant $c > 0$.

3 Preparations

Lemma 3. *Fix $n = 2$. Suppose that $f(x)$ is as in (1) with $H(f) \leq H$ and $A_1 \neq 0$. If f is a Dumas polynomial then $\gcd(A_j, A_k) \neq 1$ for every $j, k \in \{0, 1, 2\}$.*

Proof. Suppose there exists a polynomial with the property that $\gcd(A_j, A_k) = 1$ for some distinct $j, k \in \{0, 1, 2\}$. If for any prime p we have $p \mid A_1$ then clearly $p \nmid A_0$ and $p \nmid A_2$. So the Newton passes through the point $(1, 0)$, since it lies on the segment from $(0, 0)$ to $(2, 0)$. Thus f is not a Dumas polynomial. On the other hand, if for any prime p we have $p \nmid A_1$ then the Newton polygon includes the point $(1, 0)$. So again f is not a Dumas polynomial, completing the proof. □

Lemma 4. *Fix $n \geq 2$. Suppose $f(x)$ is as shown in (1) with $H(f) \leq H$ and $A_1 A_2 \cdots A_{n-1} \neq 0$. If f is a Dumas polynomial then $\gcd(A_1, A_2, \ldots, A_{n-1}) \neq 1$.*

Proof. Suppose f is as described above with $\gcd(A_1, A_2, \ldots, A_{n-1}) = 1$. For any prime p we must have $p \nmid A_i$ for some $1 \leq i \leq n - 1$. So the Newton diagram for f with respect to p includes the point $(A_i, 0)$. Thus the Newton diagram with respect to any prime p does not consist of a single segment. Therefore f is not a Dumas polynomial. □

4 Proof of Theorem 1

Let $f(x)$ be as in (1) with $H(f) \leq H$. We prove Theorem 1 for $n = 2$ and $n \geq 3$ separately.

We start with the $n = 2$ case. To ease notation we use $\gcd^*(A_0, A_1, A_2) \neq 1$ to mean that A_0, A_1 and A_2 are not pairwise coprime, that is, $\gcd(A_0, A_1) \neq 1$ or $\gcd(A_0, A_2) \neq 1$ or $\gcd(A_1, A_2) \neq 1$. We also use $\gcd_*(A_0, A_1, A_2) = 1$ to mean that A_0, A_1 and A_2 are pairwise coprime, that is, $\gcd(A_0, A_1) = \gcd(A_0, A_2) = \gcd(A_1, A_2) = 1$.

There are $O(H^2)$ polynomials with $A_0A_1A_2 = 0$. If we have $A_0A_1A_2 \neq 0$ then, by Lemma 3, the polynomial f can only be a Dumas polynomial if $\gcd^*(A_0, A_1, A_2) \neq 1$. Therefore,

$$\begin{aligned}\mathcal{D}_2(H) - O(H^2) &\leq \sum_{\substack{1\leq |A_0|,|A_1|,|A_2|\leq H \\ \gcd^*(A_0,A_1,A_2)\neq 1}} 1 \\ &= \sum_{\substack{1\leq A_0,A_1,A_2\leq H \\ \gcd^*(A_0,A_1,A_2)\neq 1}} 8 \\ &= (2H)^3 - \sum_{\substack{1\leq A_0,A_1,A_2\leq H \\ \gcd_*(A_0,A_1,A_2)= 1}} 8. \end{aligned} \tag{2}$$

From the paper of Tóth [9, Corollary 2] we have

$$\sum_{\substack{1\leq A_0,A_1,A_2\leq H \\ \gcd_*(A_0,A_1,A_2)= 1}} 1 = H^3 \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^2 \left(1 + \frac{2}{p}\right) + O\left(H^2(\log H)^2\right),$$

from which

$$\sum_{\substack{1\leq |A_0|,|A_1|,|A_2|\leq H \\ \gcd_*(A_0,A_1,A_2)= 1}} 1 = (2H)^3 \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^2 \left(1 + \frac{2}{p}\right) + O\left(H^2(\log H)^2\right). \tag{3}$$

Substituting (3) into (2) completes the proof for the $n = 2$ case.

Now fix $n \geq 3$. There are $O(H^n)$ polynomials for which $A_1A_2\cdots A_{n-1} = 0$. If $A_1A_2\cdots A_{n-1} \neq 0$ then, by Lemma 4, the polynomial f can only be a Dumas polynomial if $\gcd(A_1, A_2, \ldots, A_{n-1}) \neq 1$. Therefore,

$$\mathcal{D}_n(H) - O(H^n) \leq \sum_{\substack{1\leq |A_1|,|A_2|,\ldots,|A_n|\leq H \\ \gcd(A_1,A_2,\ldots,A_{n-1})\neq 1}} 1. \tag{4}$$

We infer from Nymann [7] that

$$\sum_{\substack{1\leq |A_1|,|A_2|,\ldots,|A_n|\leq H \\ \gcd(A_1,A_2,\ldots,A_{n-1})\neq 1}} 1 = (2H)^{n+1}\left(1 - \frac{1}{\zeta(n-1)}\right) + O(H^n). \tag{5}$$

Substituting (5) into (4) completes the proof for the $n \geq 3$ case. Thus Theorem 1 is proven.

5 Comments

Let $\mathcal{P}_n(H)$ be the number of polynomials of degree n and maximum height H. Let $\mathcal{I}_n(H)$ be the number of irreducible polynomials of degree n and maximum height H. Two results immediately follow from Theorem 1.

Firstly, we note that $\mathcal{P}_n(H)$ is precisely $(2H)(2H+1)^n$ and infer from Cohen [1, Theorem 1] that for $n \geq 2$

$$\lim_{H\to\infty} \frac{\mathcal{I}_n(H)}{\mathcal{P}_n(H)} = 1.$$

Thus, for $n \geq 2$,

$$\limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{P}_n(H)} = \limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{I}_n(H)} \leq \tau_n.$$

Secondly, $\tau_n < 1$ for all $n \geq 2$ and so for $n \geq 2$

$$\limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{P}_n(H)} = \limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{I}_n(H)} < 1.$$

Table 1 shows some calculated values of upper bounds on the limit superior of $\mathcal{D}_n(H)/\mathcal{P}_n(H)$ as H goes to infinity. It also includes limit inferior calculations derived from a paper by the author and Shparlinski [5]. Specifically, for various values of n, lower bounds on the limit inferior of $\mathcal{D}_n(H)/\mathcal{P}_n(H)$ as H goes to infinity. All summations are over all primes less than 100,000.

Table 1: Some upper bounds on $\limsup \mathcal{D}_n H/\mathcal{P}_n(H)$ as $H \to \infty$ and lower bounds on $\liminf \mathcal{D}_n(H)/\mathcal{P}_n(H)$ as $H \to \infty$

n	Lower bound	Upper bound
2	0.1677	0.7133
3	0.0556	0.3922
4	0.0224	0.1681
5	0.0099	0.0766
6	0.0046	0.0357
7	0.0022	0.0181
8	0.0010	0.0079
9	0.0005	0.0049
10	0.0003	0.0020

This prompts the following question. Is it possible to obtain tighter bounds or the exact values of

$$\liminf_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{P}_n(H)} \qquad \text{and} \qquad \limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{P}_n(H)}$$

(they most likely coincide)?

We also note that it is possible to find upper bounds on

$$\limsup_{H\to\infty} \mathcal{D}_n(H)/\mathcal{P}_n(H)$$

by directly calculating the number of Dumas polynomials for an arbitrary single segment Newton polygon that contains no points with integer coordinates other than endpoints, and then summing over all possible single segment Newton polygons that contain no points with integer coordinates other than endpoints. There are substantial problems using the inclusion exclusion principle with this approach; a Dumas polynomial with respect to more than one prime may exhibit a different Newton polygon for each of these primes. Whilst results for degree $n > 3$ are obtainable without the inclusion exclusion principle, it has not been possible to find any results that are superior to Theorem 1.

6 Acknowledgement

The author would like to thank Igor Shparlinski for numerous helpful suggestions. The author would also like to thank the referee for suggestions that have led to improvements in this paper.

References

[1] S. D. Cohen, The distribution of the Galois groups of integral polynomials, *Illinois J. of Math.* **23** (1979), 135–152.

[2] D. E. Dobbs and L. E. Johnson, On the probability that Eisenstein's criterion applies to an arbitrary irreducible polynomial, in *Proc. of 3rd Intern. Conf. Advances in Commutative Ring Theory*, Lect. Notes in Pure and Appl. Math., Vol. 205, Dekker, 1991, pp. 241–256.

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

[4] G. Dumas, Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels, *J. Math. Pures Appl.* **(6) 2** (1906), 191–258.

[5] R. Heyman and I. E. Shparlinski, On the number of Eisenstein polynomials of bounded height, *Appl. Algebra Engrg. Comm. Comput.* **24** (2013), 149–156.

[6] R. Heyman and I. E. Shparlinski, On shifted Eisenstein polynomials, *Period. Math. Hungar.*, to appear.

[7] J. E. Nymann, On the probability that k positive integers are relatively prime, *J. Number Theory* **4** (1972), 469–473.

[8] V. V. Prasolov, *Polynomials*, Springer, 2004.

[9] L. Tóth, The probability that k positive integers are pairwise relatively prime, *Fibonacci Quart.* **40** (2002), 13–18.

2010 *Mathematics Subject Classification*: Primary 11R09.
Keywords: irreducible polynomial, Dumas criterion, coprimality.

Received June 3 2013; revised version received December 12 2013. Published in *Journal of Integer Sequences*, January 4 2014.

Return to Journal of Integer Sequences home page.