ON THE NUMBER OF MONIC ADMISSIBLE POLYNOMIALS IN THE RING $\mathbb{Z}[x]$

Abstract. In this paper we study admissible polynomials. We establish an estimate for the number of admissible polynomials of degree n with coeffients a_i satisfying $0 \leq a_i \leq H$ for a fixed H, for $i = 0, 1, 2, \ldots, n-1$. In particular, letting $\mathcal{N}(H)$ denotes the number of monic admissible polynomials of degree $n \geq 3$ with coefficients satisfying the inequality $0 \leq a_i \leq H$, we show that

$$\frac{H^{n-1}}{(n-1)!} + O(H^{n-2}) \leq \mathcal{N}(H) \leq \frac{n^{n-1}H^{n-1}}{(n-1)!} + O(H^{n-2}).$$

Also letting $\mathcal{A}(H)$ denotes the number of monic irreducible admissible polynomials, with coefficients satisfying the same condition , we show that

$$\mathcal{A}(H) \geq \frac{H^{n-1}}{(n-1)!} + O\Big(H^{n-4/3}(\log H)^{2/3}\Big).$$

1. Introduction and problem statement

Let us consider the polynomial

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

of degree n in the ring $\mathbb{R}[x]$. Then $f(x)$ is said to be admissible if

$$n! = \sum_{i=0}^{n} a_i = a_0 + a_1 + \cdots + a_{n-1} + a_n.$$

Let $a_n = 1$ and let $\mathcal{N}(H)$ denotes the number of admissible monic polynomials belonging to the ring $\mathbb{Z}[x]$. Interest is on the number of such monic irreducible polynomial of a given degree under certain constraint. Admissible polynomials, by their nature, form an important class of polynomials. In some sense admissible polynomials gives us much information about the distribution of the coefficients. These polynomials becomes very useful in practice, because it allows us to recover with some precision the possible coefficients of any such polynomials. Through out this paper, using a sieve theoritical technique, we will be concerned with the model problem of estimating the number of monic irreducible admissible polynomials that can be formed from any given constraint on the coefficients. Letting $\mathcal{A}(H)$ denotes the number of irreducible admissible polynomials

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

with $0 \leq a_i \leq H$ for $i = 0, 1, \ldots, n-1$ and $a_i \in \mathbb{Z}[x]$, we ask the question of how small can this quantity be? This paper will be concerned with addressing such a

Date: August 29, 2018.

2000 *Mathematics Subject Classification.* Primary 54C40, 14E20; Secondary 46E25, 20C20.

Key words and phrases. monic, irreducible, admissible.

problem. But before then, we seek to find the counting function for the number admissible monic polynomials in $\mathbb{Z}[x]$. We obtain a lower bound in the following sequel.

2. Notations

Through out this paper a prime number will either be denoted by p or q. Any other letter will be clarified. The quantity $\mathcal{A}_p := \{a_n : a_n \equiv 0 \pmod p\}$ for $\mathcal{A} = (a_n)$, and $S(\mathcal{A}, \rho, z) := \#(\mathcal{A} \setminus \cup_{p|P(z)}\mathcal{A}_p)$, where ρ is the set of all primes. The inequality $|k(n)| \leq Mp(n)$ for sufficiently large values of n will be compactly written as $k(n) \ll p(n)$ or $k(n) = O(p(n))$. Similarly the inequality $|k(n)| \geq Mp(n)$ for sufficiently large values of n will be represented by $k(n) \gg p(n)$. The limit $\lim\limits_{n\longrightarrow\infty} \frac{k(n)}{p(n)} = 0$ will be represented in a compact form as $k(n) = o(p(n))$ as $n \longrightarrow \infty$. Also by $k(n) \asymp p(n)$, we mean there exist some constant $c_1, c_2 > 0$ such that $c_1 p(n) \leq k(n) \leq c_2 p(n)$. The quantity δ or any of it subscripts are positive numbers that are taken to be small.

3. Preliminary results

Theorem 3.1. *(Chebychev) Let $\pi(z) := \sum\limits_{p\leq z} 1$, then there exist some constants $c_1, c_2 > 0$ such that*

$$c_1 \frac{z}{\log z} \leq \pi(z) \leq c_2 \frac{z}{\log z}.$$

Proof. For a proof, see for instance [2]. □

Remark 3.2. Now we state a very classical theorem concerning the distribution of irreducible monic polynomials in the ring $\mathbb{F}_p[x]$, which will play a crucial role in our subsequent works. It comes in the following sequel.

Theorem 3.3. *Let N_n denotes the number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$. Then*

$$N_n = \frac{p^n}{n} + O(p^{n/2}).$$

Proof. For a proof, See for instance [1]. □

Remark 3.4. Next we state a sifting technology due to Turán, which will play a crucial role in obtaining an estimate for the number monic irreducible polynomials with coefficient that can be controlled.

Theorem 3.5. *(Turán) Let us set*

$$U(z) := \sum_{p|P(z)} \delta_p,$$

where $0 \leq \delta_p < 1$. Then

$$S(\mathcal{A}, \rho, z) \leq \frac{|\mathcal{A}|}{U(z)} + \frac{2}{U(z)} \sum_{p|P(z)} |R_p| + \frac{1}{U^2(z)} \sum_{p,q|P(z)} |R_{p,q}|,$$

where

$$P(z) = \prod_{\substack{p<z \\ p\in\rho}} p, \quad |\mathcal{A}_p| = \delta_p |\mathcal{A}| + R_p.$$

Proof. For a proof, See for instance [1]. □

4. Main results

Theorem 4.1. *Let $\mathcal{N}(H)$ denotes the number of polynomials $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ in $\mathbb{Z}[x]$, satisfying $a_0 + a_1 + \cdots + a_{n-1} = n! - 1$ and $0 \leq a_i \leq H$ for $i = 0, 1, \ldots n-1$. Then*

$$\frac{H^{n-1}}{(n-1)!} + O(H^{n-2}) \leq \mathcal{N}(H) \leq \frac{n^{n-1}H^{n-1}}{(n-1)!} + O(H^{n-2}).$$

In particular, there exist some constant $\frac{1}{(n-1)!} < c < \frac{n^{n-1}}{(n-1)!}$, such that

$$\mathcal{N}(H) = (1 + o(1))cH^{n-1},$$

as $H \longrightarrow \infty$.

Proof. Consider the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, with coefficients satisfying the conditions $0 \leq a_i \leq H$ and

$$1 + a_{n-1} + a_{n-2} + \cdots + a_0 = n!.$$

We let each of this polynomials corresponds to elements of the set

$$\mathcal{M} = \{(a_0, a_1, \ldots, a_{n-1}) | a_0 + a_1 + \cdots + a_{n-1} = n! - 1,\ 0 \leq a_i \leq H\}.$$

We remark that $\mathcal{N}(H)$ is the number of elements of the set $\mathcal{M}$. To obtain these bounds for the counting function $\mathcal{N}(H)$, we first observe that $H \leq n!$. For suppose $H > n!$, then we find that $H > n! > n! - 1 = a_0 + a_1 + a_2 + \cdots a_{n-1}$. This contradicts the inequality $a_0 + a_1 + a_2 + \cdots a_{n-1} \leq Hn$, since $n \geq 3$. Thus the inequality

$$\lfloor H \rfloor - 1 \leq n! - 1 = a_0 + a_1 + \ldots + a_{n-1} \leq \lfloor Hn \rfloor + 1$$

is valid. The lower bound is obtained by finding the number of possible representations of the form

$$a_0 + a_1 + \cdots + a_{n-1} = \lfloor H \rfloor - 1 := K.$$

Letting $R_n(K)$ denotes the number of such different representations, then we claim that

$$R_n(K) = \binom{K-1}{n-1}.$$

To see this, consider the power series

$$l(z) = \sum_{K=0}^{\infty} z^K$$

valid in the unit disc $|z| < 1$. Then it follows that

$$l^n(z) = \sum_{K=0}^{\infty} R_n(K) z^K.$$

On the other hand, we observe that

$$\begin{aligned} l^n(z) &= \frac{1}{(n-1)!}\frac{d^{n-1}}{dz^{n-1}}\bigg(\frac{1}{1-z}\bigg) \\ &= \frac{1}{(n-1)!}\frac{d^{n-1}}{dz^{n-1}}\bigg(\sum_{K=0}^{\infty} z^K\bigg) \\ &= \sum_{K=n-1}^{\infty} \frac{K(K-1)\cdots(K-n+2)}{(n-1)!} z^{K-n+1} \\ &= \sum_{K=n-1}^{\infty} \binom{K}{n-1} z^{K-n+1} \\ &= \sum_{K=0}^{\infty} \binom{K+n-1}{n-1} z^K. \end{aligned}$$

By comparism and using the fact that $R_n(K) = R_n(K-n)$, the claimed lower bound follows immediately. The upper bound follows by finding the number of different representations of the form

$$a_0 + a_1 + \cdots + a_{n-1} = \lfloor Hn \rfloor + 1,$$

by adapting the same argument, and the proof of the theorem is complete. □

Remark 4.2. The above result does gives us an order of growth of monic admissible polynomials with carefully controlled coefficients. The next result highlights this very fact.

Corollary 1. Let $\mathcal{N}(H)$ denotes the number of monic admissible polynomials of degree n in $\mathbb{Z}[x]$, with coefficients satisfying $0 \leq a_i \leq H$ for $i = 0, 1, \ldots, n-1$, then

$$\mathcal{N}(H) \asymp H^{n-1}.$$

Proof. The result follows from Theorem 4.1. □

We recall that there are H^n monic polynomials of degree n with coefficients satisfying $0 \leq a_i \leq H$. Corollary 1 also indicates that the number of admissible monic polynomials of degree n with carefully controlled coefficients as before is of the order H^{n-1}. Thus when a polynomial is chosen at random, with coefficients controlled by the quantity H, the probability that it is admissible must be roughly $\frac{c}{H}$, where $c = c(n)$. We state the next result, which gives us a lower bound for the number monic irreducible admissible polynomials, with carefully controlled coefficients.

Theorem 4.3. *Let $\mathcal{A}(H)$ denotes the number of monic admissible irreducible polynomials of degree $n \geq 3$ in the ring $\mathbb{Z}[x]$, with coefficients satisfying the relation $0 \leq a_i \leq H$ for $i = 0, 1, \ldots n-1$ and a fixed H. Then*

$$\mathcal{A}(H) \geq \frac{H^{n-1}}{(n-1)!} + O\bigg(H^{n-4/3}(\log H)^{2/3}\bigg)$$

for $H \leq n!$, and where the implied constant depends on n.

[1].

Proof. We adopt the traditional technique by way of estimating first the number of monic admissible irreducible polynomials modulo a prime p. By letting $\mathcal{N}(H)$ denotes the number of monic admissible polynomials in $\mathbb{Z}[x]$, we find by Theorem 4.1 that

$$\begin{aligned}\mathcal{N}(H) &\geq \binom{\lfloor H \rfloor - 2}{n-1} \\ &= \frac{H^{n-1}}{(n-1)!} + O\bigg(H^{n-2}\bigg). \end{aligned} \tag{4.1}$$

In particular, by Theorem 4.1, we find that $\mathcal{N}(H) = cH^{n-1} + O(H^{n-2})$, for some $c := c(n) > 0$. Let $z = z(H)$ be a real number to be chosen later and consider the polynomial

$$g(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \tag{4.2}$$

satisfying the condition $1 + a_{n-1} + \cdots + a_0 = n!$, for each $0 \leq a_i \leq H$. We let each of these polynomials corresponds to an element of the set

$$\mathcal{R} = \{(a_{n-1}, a_{n-2}, \ldots, a_0) | a_{n-1} + a_{n-2} + \cdots a_0 = n! - 1, \quad 0 \leq a_i \leq H\}.$$

Let $\mathcal{R}_p$ be a set of monic polynomials whose elements corresponds to polynomials in $\mathcal{R}$ whose elements are irreducible modulo p. Now we remark that if a polynomial is irreducible in $\mathcal{R}_p$ for some prime p, then it is irreducible in $\mathcal{R}$. We observe that the number of polynomials in $\mathcal{R}$ that corresponds to each polynomial $g(x) \pmod p$ in $\mathcal{R}_p$ is given by

$$\frac{c}{H}\bigg(\frac{H}{p} + O(1)\bigg)^n + o(1),$$

where $c = c(n)$. Letting $z^2 < H$, we can write

$$\frac{c}{H}\bigg(\frac{H}{p} + O(1)\bigg)^n + o(1) = \frac{cH^{n-1}}{p^n} + O\bigg(\frac{H^{n-2}}{p^{n-1}}\bigg).$$

Appealing to Theorem 3.3, we find that the number of polynomials in $\mathcal{R}$ that correspond to polynomials in $\mathcal{R}_p$ is given by

$$\begin{aligned}|\mathcal{R}_p| &= \bigg(\frac{cH^{n-1}}{p^n} + O\bigg(\frac{H^{n-2}}{p^{n-1}}\bigg)\bigg)\bigg(\frac{p^n}{n} + O(p^{n/2})\bigg) \\ &= \frac{cH^{n-1}}{n} + O\bigg(\frac{H^{n-1}}{p^{n/2}}\bigg) + O(H^{n-2}p).\end{aligned}$$

We see in relation to Theorem 3.5, that

$$\delta_p = \frac{1}{n}, \quad R_p = \frac{H^{n-1}}{p^{n/2}} + H^{n-2}p,$$

and

$$R_{p,q} = \frac{H^{n-1}}{p^{n/2}} + \frac{H^{n-1}}{q^{n/2}} + H^{n-2}pq, \tag{4.3}$$

[1] .

so that by appealing to Theorem 3.1, we find that

$$U(z) = \sum_{p|P(z)} \delta_p = \sum_{p|P(z)} \frac{1}{n} \gg \frac{z}{\log z}.$$

We find that

$$\frac{|\mathcal{R}|}{U(z)} \ll \frac{H^{n-1}\log z}{z}. \tag{4.4}$$

Again

$$\begin{aligned}\frac{2}{U(z)} \sum_{p|P(z)} |R_p| &= \frac{2}{U(z)} \sum_{p|P(z)} \left(\frac{H^{n-1}}{p^{n/2}} + H^{n-2}p \right) \\ &\ll \frac{H^{n-1}\log z}{z} \sum_{p|P(z)} \frac{1}{p^{n/2}} + \frac{H^{n-2}\log z}{z} \sum_{p|P(z)} p \\ &\ll \frac{H^{n-1}\log z}{z} + H^{n-2}z.\end{aligned}$$

Similarly we find that

$$\begin{aligned}\frac{1}{U^2(z)} \sum_{\substack{p|P(z)\\ q|P(z)}} |R_{p,q}| &= \frac{\log^2 z}{z^2} \sum_{\substack{p|P(z)\\ q|P(z)}} \left(\frac{H^{n-1}}{p^{n/2}} + \frac{H^{n-1}}{q^{n/2}} + H^{n-2}pq \right) \\ &= \frac{H^{n-1}\log^2 z}{z^2} \sum_{\substack{p|P(z)\\ q|P(z)}} \frac{1}{p^{n/2}} + \frac{H^{n-1}\log^2 z}{z^2} \sum_{\substack{p|P(z)\\ q|P(z)}} \frac{1}{q^{n/2}} \\ &+ \frac{H^{n-2}\log^2 z}{z^2} \sum_{\substack{p|P(z)\\ q|P(z)}} pq.\end{aligned}$$

Thus, we find that

$$\frac{1}{U^2(z)} \sum_{\substack{p|P(z)\\ q|P(z)}} R_{p,q} \ll \frac{H^{n-1}\log z}{z} + H^{n-2}z^2,$$

where the implied constant depends on n. It follows, by Theorem 3.5 that

$$S(\mathcal{R}, \rho, z) \ll \frac{H^{n-1}\log z}{z} + H^{n-2}z^2.$$

By choosing $z := H^{1/3}(\log H)^{1/3}$, it follows that

$$S(\mathcal{R}, \rho, z) = O\bigg(H^{n-4/3}(\log H)^{2/3} \bigg),$$

and the result follows immediately. □

5. Final remarks

In this paper we have been able to quantify at the very least the number of admissible polynomials in the ring $\mathbb{Z}[x]$; in particular, we have shown that the number of admissible polynomials with coefficients controlled by the quantity H is of the

order $\asymp H^{n-1}$, and that the number of monic reducible admissible polynomials is of the order

$$\ll H^{n-4/3}(\log H)^{2/3}.$$

Aside making an improvement to the following quantitative bounds, admissible polynomials has a property that could be usefull in other areas of research, most especially in the area of cryptography.

References

1. A. Carmen Cojocaru and M.Ram Murty *An introduction to sieve methods and their applications*, vol. 66, Cambridge University Press, 2005.
2. Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory*, vol. 163, American Mathematical Soc., 2015.