On the number of irreducible polynomials with 0,1 coefficients

by

S. V. KONYAGIN (Moscow)

1. Introduction. For \( d \) a positive integer, let

\[ \mathcal{P}_d = \left\{ f(z) : f(z) = \sum_{j=0}^{d} a_j z^j, \quad a_j = 0 \text{ or } 1 \text{ for all } j, \quad a_0 = a_d = 1 \right\}. \]

By irreducibility we always mean irreducibility over the rationals. There is an intriguing conjecture that almost all polynomials \( f(z) \) are irreducible, namely, the portion of irreducible polynomials in \( \mathcal{P}_d \) tends to 1 as \( d \to \infty \) (see [7]). This is still open. In what follows, \( C, c \) will denote large and small absolute positive constants, respectively. In [2] it was proved that if \( f(2) \) is prime for some \( f \in \mathcal{P}_d \) then \( f(z) \) is irreducible (see also [4]). Consequently, there are at least \( c2^d/d \) irreducible polynomials \( f \in \mathcal{P}_d \). The same estimate can also be proved by calculation of polynomials \( f \in \mathcal{P}_d \) irreducible over \( \mathbb{F}_2 \) [6, p. 93].

In this paper we improve the lower estimate of the number of irreducible polynomials of degree \( d \) with 0,1 coefficients and establish

**Theorem 1.** For a positive integer \( d \geq 2 \) there are at least \( c2^d/\log d \) irreducible polynomials \( f \in \mathcal{P}_d \).

It is reasonable to conjecture that almost all reducible polynomials \( f \in \mathcal{P}_d \) are divisible by \( z + 1 \); it would give the upper estimate \( C2^d/\sqrt{d} \) of the number of reducible polynomials \( f \in \mathcal{P}_d \). We are able to prove this estimate of the number of polynomials with 0,1 coefficients possessing nontrivial divisors of small degree.

1991 *Mathematics Subject Classification*: Primary 11C08.

The author was supported by the National Science Foundation, grant DMS 9304580. This research was carried out while the author was a member of the Institute for Advanced Study, Princeton. It is a pleasure to thank the Institute for their hospitality and generosity.
Theorem 2. For a positive integer \( d \geq 2 \) and \( m_1 = \lfloor cd/\log d \rfloor \) there are at most \( C2^d/\sqrt{d} \) polynomials \( f \in \mathcal{P}_d \) divisible by at least one integral polynomial of positive degree \( \leq m_1 \).

Theorem 1 follows easily from Theorem 2. Indeed, consider the set \( \Phi \) of integers \( \gamma p \in [2^d, 2^{d+1}) \) where \( p \) is prime, \( \gamma \) is odd and \( \gamma < \gamma_1 = 1.12m_1 \). For any \( \gamma < \gamma_1 \) the number of primes \( p \in [2^d/\gamma, 2^{d+1}/\gamma) \), by the Prime Number Theorem, is

\[
\frac{2^d}{\gamma \log(2^d/\gamma)} (1 + o(1)) \gg 2^d/(d \gamma).
\]

Hence,

\[
\# \Phi \gg \frac{2^d}{d} \sum_{\gamma \equiv 1 \pmod{2}} \frac{1}{\gamma} \gg \frac{2^d}{d} \log \gamma_1 \gg 2^d/\log d,
\]

i.e., \( \# \Phi \geq c2^d/\log d \). If \( a_d \ldots a_0 \) is the base 2 representation of an element \( \varphi \in \Phi \), then the polynomial \( f(z) = \lambda(\varphi)(z) = \sum_{j=0}^d a_j z^j \in \mathcal{P}_d \) and \( f(2) = \varphi \). Suppose that \( f \in \lambda(\varphi) \) is reducible. Then \( f = g_1 g_2 \) where \( g_1, g_2 \) are integral polynomials of positive degree and \( |g_1(2)| \leq |g_2(2)| \). We have \( |g_1(2)| \cdot |g_2(2)| = |f(2)| = \varphi \). If we assume that \( g_1(2) \) is divisible by \( \gamma \), we get \( |g_2(2)| \leq \gamma \) and

\[\varphi = |g_1(2)| \cdot |g_2(2)| \leq |g_2(2)|^2 \leq \gamma^2 < 2^{m_1} < \varphi.\]

This contradiction shows that \( g_1(2) \) cannot be divisible by \( \gamma \). Hence, \( |g_1(2)| \leq \gamma_1 \).

To estimate the degree of \( g_1 \), we follow [2]. Let \( m = \deg g_1 \), \( g_1(z) = \pm \prod_{j=1}^m (z - z_j) \). Any \( z_j \) is a zero of the polynomial \( f \) with 0,1 coefficients. So, clearly, \( |z_j| < 2 \), and, by [7], \( \Re z_j < 1.14 \). These restrictions on \( z_j \) imply \( |z_j| - 2/|z_j - 1| > 1.12 \). Indeed, consider the function \( V(z) = (z-1)^2/(z-2)^2 \) on the closed domain \( \Omega \) restricted by the segment of the line \( \Re z = 1.14 \), \( |3z|^2 \leq 4 - 1.14^2 \), and the arc of the circle \( |z| = 2, \Re z \leq 1.14 \). The maximum of \( |V(z)| \) is attained on the boundary of \( \Omega \). If \( z \) is on the segment then

\[
|V(z)| = ((0.14^2 + 3z^2)/(0.86^2 + 3z^2)) \leq (0.14^2 + 4 - 1.14^2)/(0.86^2 + 4 - 1.14^2) = 34/43.
\]

If \( z \) is on the arc then

\[
|V(z)| = (|z|^2 + 1 - 2\Re z)/(|z|^2 + 4 - 4\Re z) = (5 - 2\Re z)/(8 - 4\Re z) \leq (5 - 2 \cdot 1.14)/(8 - 4 \cdot 1.14) = 34/43.
\]

Hence, for any \( z \in \Omega \) the inequality \( V(z) \leq 34/43 \) holds, and for any zero \( z_j \) of the polynomial \( g_1 \) we have

\[
|z_j - 2/|z_j - 1| = |V(z_j)|^{1/2} \geq (34/43)^{-1/2} > 1.12.
\]
Therefore, 
\[1.12^{m_1} = \gamma_1 \geq |g_1(2)|/|g_1(1)| \geq 1.12^m,\]
and \(\deg g_1 = m \leq m_1\). By Theorem 2, there are at most \(C2^d/\sqrt{d}\) reducible polynomials in the set \(\lambda(\Phi)\), but this set contains at least \(c2^d/\log d\) elements. Thus, \(\lambda(\Phi)\) contains as many irreducible polynomials as required in Theorem 1.

Throughout the following we assume that the number \(d\) is sufficiently large.

Denote by \(\mathcal{D}\) the set of polynomials
\[g(z) = \sum_{j=0}^{m} b_j z^j, \quad b_m = 1, \quad m \in \mathbb{N},\]
with integral coefficients. To prove Theorem 2, we will estimate the number of polynomials \(f \in \mathcal{P}_d\) divisible by an irreducible polynomial \(g \in \mathcal{D}\), and then take the sum over all polynomials \(g\) of degree at most \(m_1\). To motivate our proof of Theorem 2, we indicate how to obtain a weaker result: Theorem 2 is valid if we replace \(m_1\) by \(m_2 = \lfloor \sqrt{d}/(\log d)^2 \rfloor\). For any polynomial \(g\) with leading coefficient \(\pm 1\) we define
\[M(g) = \prod_{j=1}^{m} \max(1, |z_j|),\]
where \(z_1, \ldots, z_m\) are the zeros of \(g\) counted with multiplicity. By Jensen’s theorem (Theorem 3.61 of [10]),
\[\log M(g) = \frac{1}{2\pi} \int_{0}^{2\pi} \log |g(e^{i\varphi})| \, d\varphi.\]
Therefore,
\[(1.1) \quad M\left(\sum_{j=0}^{m} b_j z^j\right) \leq \sum_{j=0}^{m} |b_j|.

Clearly, \(M(g) \geq 1\), and Kronecker’s theorem [5] asserts that \(M(g) = 1\) implies that all zeros of \(g\) are roots of unity. Otherwise, as was proved by Dobrowolski [3],
\[(1.2) \quad M(g) \geq \exp(\lambda_m), \quad \lambda_m = c \left(\frac{\log \log m}{\log m}\right)^3 \quad (m \geq 3).\]

Take an arbitrary noncyclotomic irreducible polynomial \(g \in \mathcal{D}\) such that \(\deg g = m \leq m_2\), and let \(z_1, \ldots, z_m\) be the zeros of \(g\). By Lemma 3 of [3], there exists a prime \(p\) such that \(\log(d + 1)/\lambda_{m_2} < p < 2\log(d + 1)/\lambda_{m_2}\) and all \(z_j^p\) are algebraic numbers of degree \(m\) (and, therefore, are distinct). Set
\[ g_p(w) = \prod_{j=1}^{m} (w - z_j^p). \]

Then, taking into account (1.2), we get
\[ M(g_p) = M(g)^p \geq \exp(p\lambda m_2) > d + 1. \]

Suppose that \( g(z) \) divides two distinct polynomials \( f_1 \) and \( f_2 \) from \( \mathcal{P}_d \) such that
\[ f_1(z) - f_2(z) = \sum_{j=0}^{d/p} a_j z^j = h(z^p). \]

Clearly, all coefficients of the polynomial \( h \) are 0, ± 1. By (1.1), \( M(h) \leq d + 1 \).

On the other hand, any zero \( z_j^p \) of \( g_p \) is a zero of \( h \). Hence, \( h \) is divisible by \( g \), and (1.3) entails \( M(h) > d + 1 \). This contradiction shows that our supposition cannot occur. This means that if a polynomial \( f(z) = \sum_{j=0}^{d} a_j z^j \in \mathcal{P}_d \) is divisible by \( g \) then \( f \) is uniquely determined by its coefficients \( a_j, j \neq 0 \) (mod \( p \)). Hence,
\[ \# \{ f \in \mathcal{P}_d : g \mid f \} < 2^d / 2^d/p < 2^d / 2^d \lambda m_2 / (2 \log(d+1)) < 2^d \exp(-0.3d \lambda m_2 / \log d). \]

Let us estimate the number \( N \) of polynomials \( g \in \mathcal{D} \) of degree at most \( m_2 \) dividing at least one polynomial \( f \in \mathcal{P}_d \). We consider any such polynomial
\[ g(z) = \sum_{j=0}^{m} b_j z^j = \prod_{j=1}^{m} (z - z_j). \]

Since \( |z_j| < 2 \) for any \( j \), representing the coefficients of the polynomial \( g \) as symmetric polynomials of its zeros, we find \( |b_j| \leq 2^m - j \binom{m}{j} < 4^m \). Hence,
\[ N < \prod_{j=0}^{m_2} (2 \cdot 4^{m_2} + 1) < 5^{m_2}. \]

It follows from the last inequality and (1.4) that the total number of polynomials \( f \in \mathcal{P}_d \) divisible by at least one noncyclotomic polynomial of degree at most \( m_2 \) is less than
\[ 2^d 5^{m_2} \exp(-0.3d \lambda m_2 / \log d) < 2^d \exp(2d / (\log d)^4 - 0.3d \lambda m_2 / \log d) = o(2^d / \sqrt{d}). \]

It is not difficult to prove that the number of polynomials \( f \in \mathcal{P}_d \) divisible by at least one cyclotomic polynomial is \( O(2^d / \sqrt{d}) \) (see §4). Thus, we get the analog of Theorem 2 for \( m_2 \) instead of \( m_1 \).

To prove Theorem 2, we must have more accurate estimates for the number of possible divisors of polynomials \( f \in \mathcal{P}_d \). In Section 3 we will find upper bounds for the number of polynomials \( g \in \mathcal{D} \) with restrictions on their zeros. To do this, we need some estimates of \( \varepsilon \)-capacity of appropriate
Irreducible polynomials

2. Several geometric lemmas. In this section we fix two positive numbers $\alpha$ and $\tau$ such that

$$(2.1) \quad \alpha > 1, \quad \tau < 0.1/\alpha.$$

Also, $m$ will denote a sufficiently large positive integer exceeding some magnitude depending on $\alpha$ and $\tau$. Let $X = \mathbb{R}^m$ be the $m$-dimensional real coordinate space equipped with the $l_\infty$-norm:

$$|(x_1, \ldots, x_m)| = \max_{1 \leq j \leq m} |x_j|.$$

We denote by $\text{Vol}(A) = \text{Vol}_m(A)$ the volume of a convex closed bounded set $A \subset X$.

**Lemma 2.1.** Let $\Pi \subset \mathbb{R}^l$ be a parallellepiped and $A \subset \Pi$ be a convex polytope with $n \leq l^\alpha$ vertices. Then

$$\text{Vol}(A) < \text{Vol}(\Pi) \left( \frac{90\alpha \log l}{l^{1/2}} \right)^{1/2},$$

provided that $l$ is large enough.

**Proof.** We may suppose that $\Pi$ is a cube inscribed in the unit ball $B$, namely, $\Pi = [-1/\sqrt{l}, 1/\sqrt{l}]^l$. We have

$$\text{Vol}(B) = \frac{\pi^{l/2}}{l(1 + l/2)} < \frac{\pi^{l/2}}{(l/(2e))^{l/2}} = \left( \frac{2\pi e}{l} \right)^{l/2} = (\pi e)^{l/2} \text{Vol}(\Pi).$$

Using the inequality

$$\text{Vol}(A) \leq \text{Vol}(B) \left( \frac{10\alpha \log l}{l} \right)^{1/2}$$

for the volume of a convex polytope $A$ with $\leq l^\alpha$ vertices provided that $l > l(\alpha)$ (see [1]) we get

$$\text{Vol}(A) \leq \text{Vol}(\Pi) \left( \frac{10\pi e \alpha \log l}{l} \right)^{1/2} < \left( \frac{90\alpha \log l}{l} \right)^{1/2},$$

as required.

Let $e_1, \ldots, e_m$ be the coordinate vectors of $\mathbb{R}^m$. For a convex closed bounded set $A \subset X$ and $j = 1, \ldots, m$ define

$$O_j(A) = A + [-e_j/2, e_j/2] = \{ x + \mu e_j : x \in A, \ |\mu| \leq 1/2 \}.$$

Let $O(A)$ be the 1/2-neighborhood of $A$:

$$O(A) = \{ x + y : x \in A, \ |y| \leq 1/2 \}.$$
We have
\[(2.2) \quad O(A) = O_1(\ldots O_m(A) \ldots).\]
Let \(\Sigma = \Sigma(m)\) be the set of all subsets of the set \(\{1, \ldots, m\}\) and \(T \in \Sigma\). We denote by \(P_T(A)\) the orthogonal projection of the set \(A\) to the linear space spanned by \(e_j, \ j \in T\). We consider that \(\text{Vol}_0(P_\emptyset(A)) = 1\).

**Lemma 2.2.** For any \(T \in \Sigma\) and any \(j \in T\) we have
\[
\text{Vol}_T(P_T(O_j(A))) = \text{Vol}_T(P_T(A)) + \text{Vol}_{T \setminus \{j\}}(P_{T \setminus \{j\}}(A)).
\]
**Proof.** Set \(T' = T \setminus \{j\}\) and represent \(P_T\) in the following form:
\[
P_T(A) = \{\{x_t : t \in T\} : \{x_t : t \in T'\} \in P_{T'}(A), f_1(\{x_t : t \in T'\}) \leq x_j \leq f_2(\{x_t : t \in T'\})\}.
\]
Expressing the volumes of \(P_T(A)\) and \(P_T(O_j(A))\) as integrals over \(P_{T'}(A)\) we get the required relationship. Lemma 2.2 is proved.

Using (2.2), we can write
\[
O(A) = P_{\{1, \ldots, m\}}(O_1(\ldots O_m(A) \ldots)).
\]
Now, applying subsequently Lemma 2.2, and taking into account that the operators \(T\) and \(O_j\) commute for \(j \in T\), we obtain

**Lemma 2.3.** The following equality holds:
\[(2.3) \quad \text{Vol}(O(A)) = \sum_{T \in \Sigma} \text{Vol}_T(P_T(A)).\]

In the next lemma we estimate the 1/2-capacity [9, 1.1.7] of convex polytopes contained in a parallelepiped.

**Lemma 2.4.** Let \(\Pi = \prod_{j=1}^m [-u_j/2, u_j/2]\) be a parallelepiped and \(A \subset \Pi\) be a convex polytope with \(n \leq m^{\alpha - 1}\) vertices. Let \(D\) be a subset of \(A\) such that the distance between any two elements of \(D\) is at least 1. Then
\[
\# D < \exp(m^{1-9\tau}) \prod_{j=1}^m \left(1 + \frac{u_j}{m^{0.5-6\tau}}\right).
\]
**Proof.** The unit cubes with centers at the points of \(D\) are mutually nonoverlapping, and the union of these cubes is a subset of \(O(A)\). Therefore, \(\# D \leq \text{Vol}(O(a))\), and it remains to estimate the volume of \(O(A)\).

We use Lemma 2.3. Note that in view of the inequality (2.1), \(n < (m^{1-10\tau})^\alpha\). Therefore, for \(l = \# T \geq m^{1-10\tau}\) the volumes on the right-hand
side of (2.3) can be estimated by Lemma 2.1:
\[
\text{Vol}_l(P_T(A)) < \text{Vol}_l(P_T(II)) \left(\frac{90\alpha \log l}{l}\right)^{l/2} \\
\leq \text{Vol}_l(P_T(II)) \left(\frac{90\alpha \log m}{m^{1-10\tau}}\right)^{l/2} < \text{Vol}_l(P_T(II))(m^{0.5-6\tau})^{-l}.
\]
For \( l < m^{1-10\tau} \) using the trivial estimate \( \text{Vol}_l(P_T(A)) \leq \text{Vol}_l(P_T(II)) \) we have
\[
\text{Vol}_l(P_T(A)) \leq \text{Vol}_l(P_T(II))(m^{0.5-6\tau})^{-l}(m^{0.5-6\tau})^l < \text{Vol}_l(P_T(II))(m^{0.5-6\tau})^{-l} \exp(m^{1-9\tau}).
\]
In both cases we have the inequality
\[
(2.4) \quad \text{Vol}_{\#_T}(P_T(A)) < \text{Vol}_{\#_T}(P_T(II))(m^{0.5-6\tau})^{-\#_T} \exp(m^{1-9\tau}).
\]
Now, using (2.3), we find
\[
\text{Vol}(O(A)) < \exp(m^{1-9\tau}) \sum_{T \in \Sigma} \text{Vol}_{\#_T}(P_T(II))(m^{0.5-6\tau})^{-\#_T} \\
= \exp(m^{1-9\tau}) \prod_{j=1}^{m} \left(1 + \frac{u_j}{m^{0.5-6\tau}}\right).
\]
This completes the proof of Lemma 2.4.

The following lemma is the only statement of this section which will be used later on.

**Lemma 2.5.** For a vector \( w = (w_1, \ldots, w_m) \in \mathbb{C}^m \) define
\[
S_k(w) = \sum_{j=1}^{m} w_j^k \quad (k = 1, \ldots, m).
\]
Let \( W \) be a subset of \( \mathbb{C}^m \) such that \( \max_j |w_j| \leq \exp(0.4(\log m)/m) \) for any \( w = (w_1, \ldots, w_m) \in W \) and \( \max_{1 \leq k \leq m} |\Re S_k(w) - \Re S_k(w')|/k > 1/2 \) for any two distinct vectors \( w, w' \) from \( W \). Then \( \# W < \exp(m^{0.95}) \).

**Proof.** We associate with any vector \( w \in W \) the vector \( \tilde{w} = (\tilde{w}_1, \ldots, \tilde{w}_m) \) such that
\[
\tilde{w}_j = m^{-2.45}(\text{sgn}(\Re w_j)[m^{2.45}|\Re w_j|] + i \text{sgn}(\Im w_j)[m^{2.45}|\Im w_j|]) \\
(j = 1, \ldots, m),
\]
where \([\cdot]\) denotes the integral part. For any \( j \in \{1, \ldots, m\} \) and \( k \in \{1, \ldots, m\} \)
we have $|w_j - \tilde{w}_j| \leq \sqrt{2} m^{-2.45}$ and
\[
|w^k_j - \tilde{w}^k_j| \leq k|w_j - \tilde{w}_j| \max(|w^k_j|^{k-1}, |\tilde{w}^k_j|^{k-1}) \\
\leq 2km^{-2.45}(\exp(0.4(\log m)/m))^{k-1} \\
\leq 2m^{-1.45}(\exp(0.4(\log m)/m))^m = 2m^{-1.05}.
\]

From the last inequality and the assumption on $W$ we get
\[
\max_{1 \leq k \leq m} |\mathfrak{R}S_k(\tilde{w}) - \mathfrak{R}S_k(\tilde{w}')|/k > 1/3 \quad (w, w' \in W, \ w \neq w').
\]

Consider the mapping $\psi : W \to X$:
\[
\psi(w) = (3\mathfrak{R}S_1(\tilde{w}), 3\mathfrak{R}S_2(\tilde{w})/2, \ldots, 3\mathfrak{R}S_m(\tilde{w})/m).
\]

The condition (2.5) means that all distances between $\psi(w)$ and $\psi(w')$ for distinct $w, w' \in W$ are at least 1.

The set $D = \psi(W)$ is contained in the convex hull $A$ of the vectors $(3m\mathfrak{R}z, 3m\mathfrak{R}(z^2)/2, \ldots, 3m\mathfrak{R}(z^m)/m)$, where $|z| \leq \exp(0.4(\log m)/m)$ and $m^{2.45}\mathfrak{R}z, m^{2.45}\mathfrak{R}(z^2), \ldots, m^{2.45}\mathfrak{R}(z^m)$ are integers (i.e. $z$ runs over the set of all possible points $\tilde{w}_j$). The number $n$ of the vertices of the polytope $A$ does not exceed
\[
\pi (1 + \exp(0.4(\log m)/m)/m)^{-2.45}^2 < 6.
\]

Moreover, $A$ is contained in the parallelepiped
\[
\Pi = \prod_{j=1}^{m} [-u_j/2, u_j/2], \quad u_j = 6m \exp(0.4(j/m) \log m)/j \quad (j = 1, \ldots, m).
\]

Now we are ready to apply Lemma 2.4. Take $\alpha = 7$, $\tau = 1/150$. Lemma 2.4 asserts that
\[
\# D < \exp(m^{0.94}) \prod_{j=1}^{m} \left(1 + \frac{u_j}{m^{0.46}}\right).
\]

We have
\[
\log \prod_{j=1}^{m} \left(1 + \frac{u_j}{m^{0.46}}\right) \leq \sum_{j=1}^{m} \frac{u_j}{m^{0.46}} \leq \sum_{j=1}^{m} \frac{6m^{0.94}}{j} < m^{0.945}.
\]

Substitution of the last inequality into (2.6) implies
\[
\# D < \exp(m^{0.94}) \exp(m^{0.945}) < \exp(m^{0.95}).
\]

But $\# W = \# D$. Thus, $\# W < \exp(m^{0.95})$, as required.

3. Estimates of the number of irreducible polynomials with restrictions on its zeros. Let $g \in \mathcal{D}$ be an irreducible polynomial and $z$ be one of its zeros. For an integer $l$ we denote the number of zeros $z'$ of the polynomial $g$ such that $(z')^l = z$ by $k_l(g)$. Clearly, $k_l(g)$ does not depend on the
choice of \( z \). Moreover, \( k_l(g) \) divides the degree of \( g \). For a nonnegative number \( U \) and positive integers \( k, l, m, m \geq 2 \), we will denote by \( D(U, m, l, k) \) the set of irreducible polynomials \( g \) of degree \( m \) such that \( \log M(g) \leq U/m \) and \( k_l(g) = k \). We consider that \( k \) divides \( m \) since otherwise the set \( D(U, m, l, k) \) is empty.

**Lemma 3.1.** For sufficiently large \( m \) the cardinality of \( D(U, m, l, k) \) does not exceed

\[
\exp(m^{0.95})C^{U/k}(C_l/k)^{CU/\log m}.
\]

**Remark.** In the case \( l = 1 \) the proof of the lemma actually shows that the number of all polynomials \( g(z) = z^m + \sum_{j=0}^{m-1} b_j z^j \) with integral coefficients such that \( \log M(g) \leq U/m \) does not exceed \( \exp(m^{0.95})C^{U} \).

**Proof (of Lemma 3.1).** We say that the zeros \( v, v' \) of the polynomial \( g \in D(U, m, l, k) \) are equivalent if \( v^l = (v')^l \). Fix a maximal subset \( \{v_1, \ldots, v_{m/k}\} \) of mutually nonequivalent zeros of \( g \) such that \( |v_1| \geq \ldots \geq |v_{m/k}| \). Let \( |v_n| \geq \exp(0.4(\log m)/m) > |v_{n+1}| \) for definiteness, we consider \( v_0 = \infty, v_{m/k+1} = 0 \). Define \( n = \psi(g) \). Besides the mapping \( \psi \), we define several mappings on the set \( D(U, m, l, k) \). Let \( \psi_j(g) = |m \log |v_j|| (j = 1, \ldots, n) \). We have

\[
\prod_{j=1}^{n} |v_j| \leq \prod_{j=1}^{m/k} \max(1, |v_j|) = (M(g))^{1/k} \leq \exp(U/(mk)).
\]

On the other hand,

\[
\prod_{j=1}^{n} |v_j| \geq \exp(0.4n(\log m)/m)
\]

and

\[
\prod_{j=1}^{n} |v_j| \geq \prod_{j=1}^{n} \exp(\psi_j(g)/m) = \exp \left( \sum_{j=1}^{n} \psi_j(g)/m \right).
\]

Therefore,

(3.1) \quad \psi(g) = n \leq U/(0.4k \log m)

and

(3.2) \quad \sum_{j=1}^{n} \psi_j(g) \leq U/k.

For any \( u \in \mathbb{Z}_+ \) we cover the disk \( \{ z : |z| \leq \exp((u+1)/m) \} \) by disjoint squares

\[
S^u_\nu = [\alpha/(m^3v), (\alpha + 1)/(m^3v)] \times [\beta/(m^3v), (\beta + 1)/(m^3v)],
\]

\[
v = \exp((m-1)u/m), \quad \alpha, \beta \in \mathbb{Z}, \quad \nu \in \mathbb{Z}, \quad 1 \leq \nu \leq N_u.
\]
Taking into account that
\[ v \exp((m - 1)u/m) = \exp(u + 1/m) < 3 \exp(u), \]
we can write a rough estimate for the number \( N_u \) of squares intersecting the disk:

(3.3) \[ N_u \leq m^7 \exp(2u). \]

We define the mappings \( \Psi_j \) \((j = 1, \ldots, n)\) setting \( \Psi_j(g) = \nu \) if \( v_j \in S^n_u \) where \( u = \psi_j(g) \). Finally, for \( j = 1, \ldots, n \) we define the mapping \( \varphi_j \) from \( D(U, m, l, k) \) to the set \( \Sigma(k, l) \) of \( k \)-element subsets of \( \{1, \ldots, l\} \) by setting \( \varphi_j(g) = T \in \Sigma(k, l) \) if the set of zeros of \( g \) equivalent to \( v_j \) is the set of numbers \( v_j \zeta^t \), \( t \in T \), where \( \zeta \) is a fixed primitive \( l \)th root of unity.

We want to estimate the number of distinct images

\[ (n = \psi(g), \psi_1(g), \ldots, \psi_n(g), \Psi_1(g), \ldots, \Psi_n(g), \varphi_1(g), \ldots, \varphi_n(g)) \]

for \( g \in D(U, m, l, k) \).

For a fixed \( n = \psi(g) \) the values \( \psi_1(g), \ldots, \psi_n(g) \) are determined by \( n \) different numbers \( \psi_1(g), \psi_1(g) + \psi_2(g), \ldots, \psi_1(g) + \cdots + \psi_n(g) \) not exceeding \([U/k]\) by (3.2). Consequently,

(3.4) \[ \#\{(n, \psi_1(g), \ldots, \psi_n(g))\} \leq \sum_{n=0}^{[U/k]} \left( \frac{[U/k]}{n} \right) \leq 2^{U/k}. \]

Then, for fixed \( n, \psi_1(g), \ldots, \psi_n(g) \) we have, by (3.3), (3.1) and (3.2),

(3.5) \[ \#\{(\psi_1(g), \ldots, \psi_n(g))\} \leq \prod_{j=1}^{n} (m^7 \exp(2\psi_j(g))) \]

\[ \leq m^{7U/(0.4k \log m)} \exp(2U/k) \leq C^{U/k}. \]

Finally, for fixed \( n, \psi_1(g), \ldots, \psi_n(g), \Psi_1(g), \ldots, \Psi_n(g) \), using (3.1) again and the inequality

\[ \left( \frac{l}{k} \right) \leq l^k / k! \leq (el/k)^k, \]

we obtain

(3.6) \[ \#\{(\varphi_1(g), \ldots, \varphi_n(g))\} \]

\[ \leq \left( \frac{l}{k} \right)^n \leq (el/k)^{kU/(0.4k \log m)} \leq (el/k)^{CU/\log m}. \]

The combination of inequalities (3.4)–(3.6) implies

(3.7) \[ \#\{(n, \psi_1(g), \ldots, \psi_n(g), \Psi_1(g), \ldots, \Psi_n(g), \varphi_1(g), \ldots, \varphi_n(g))\} \]

\[ \leq N = (2C)^{U/k}(el/k)^{CU/\log m}. \]
Consider two polynomials \( g \in \mathcal{D}(U, m, l, k) \) and \( \tilde{g} \in \mathcal{D}(U, m, l, k) \) such that
\[
\psi(g) = \psi(\tilde{g}), \quad \psi_j(g) = \psi_j(\tilde{g}) \quad (j = 1, \ldots, n),
\]
\[
\Psi_j(g) = \Psi_j(\tilde{g}) \quad (j = 1, \ldots, n), \quad \varphi_j(g) = \varphi_j(\tilde{g}) \quad (j = 1, \ldots, n).
\]

Define
\[
Z = \{ z : g(z) = 0 \}, \quad \tilde{Z} = \{ z : \tilde{g}(z) = 0 \},
\]
\[
V = \{ v \in Z : |v| \geq \exp(0.4(\log m)/m) \},
\]
\[
\tilde{V} = \{ v \in \tilde{Z} : |v| \geq \exp(0.4(\log m)/m) \},
\]
\[
W = \{ w \in Z : |w| < \exp(0.4(\log m)/m) \},
\]
\[
\tilde{W} = \{ w \in \tilde{Z} : |w| < \exp(0.4(\log m)/m) \}.
\]

Let \( n = \psi(g) = \psi(\tilde{g}) \). For any \( j = 1, \ldots, n \) we take \( u = \psi_j(g) = \psi_j(\tilde{g}) \), \( v = \exp((m-1)u/m) \) and the corresponding zeros \( v_j \) of \( g \) and \( \tilde{v}_j \) of \( \tilde{g} \). Since the values of \( \psi_j \) at \( g \) and \( \tilde{g} \) coincide, we have
\[
|v_j - \tilde{v}_j| \leq \sqrt{2/(m^3v)} < 4/(m^3\exp((m-1)(u+1)/m)) \leq 4\max(|v_j|, |\tilde{v}_j|)1^{-m}/m^3.
\]

For any zero \( v \in V \) of \( g \) equivalent to \( v_j \) we set \( \chi(v) = v\tilde{v}_j/v_j \). As the values of \( \varphi_j \) at \( g \) and \( \tilde{g} \) coincide, \( \chi \) is a one-to-one correspondence \( V \rightarrow \tilde{V} \). By (3.9), \(|\chi(v) - v| \leq 4\max(|v|, |\chi(v)|)^1-1/{m}^3/m^3 \) for any \( v \in V \). Therefore,
\[
|(\chi(v))^i - v^i| \leq i \max(|v|, |\chi(v)|)^{i-1}\chi(v) - v < m \max(|v|, |\chi(v)|)^{m-1}|\chi(v) - v| \leq 4/m^2 \quad (i = 1, \ldots, m),
\]
and
\[
\left| \sum_{v \in V} v^i - \sum_{v \in V} v^i \right| < 1/2 \quad (i = 1, \ldots, m).
\]

Let
\[
g(z) = \sum_{j=0}^{m} b_j z^j, \quad b_m = 1,
\]
\[
S_i = \sum_{z \in Z} z^i = \sum_{v \in V} v^i + \sum_{w \in W} w^i \quad (i = 1, \ldots, m),
\]
\[
\tilde{S}_i = \sum_{z \in \tilde{Z}} z^i = \sum_{v \in V} v^i + \sum_{w \in \tilde{W}} w^i \quad (i = 1, \ldots, m).
\]

The numbers \( S_1, \ldots, S_m \) are integers. Moreover, by the Newton identities,
\[
S_i + b_{m-i} S_{i-1} + \ldots + b_{m-i+1} S_1 + i b_{m-i} = 0 \quad (i = 1, \ldots, m).
\]
Therefore, \( S_1, \ldots, S_{i-1} \) determine \( b_{m-1}, \ldots, b_{m-i+1} \) and the residue of \( S_i \) (mod \( i \)). If the integral polynomials \( g \) and \( \tilde{g} \) are distinct then we can take the minimal \( i \) such that \( S_i \neq \tilde{S}_i \). Then \( S_i \equiv \tilde{S}_i \) (mod \( i \)) and, hence,

\[ \exists i \quad |S_i - \tilde{S}_i| \geq i, \]

or

\[ (3.11) \quad \exists i \quad \left| \sum_{v \in \mathcal{V}} v^i + \sum_{w \in \mathcal{W}} w^i - \sum_{v \in \tilde{\mathcal{V}}} v^i - \sum_{w \in \tilde{\mathcal{W}}} w^i \right| \geq i. \]

Let

\[ W = \{ w_1, \ldots, w_{m-kn} \}, \quad \tilde{W} = \{ \tilde{w}_1, \ldots, \tilde{w}_{m-kn} \}, \]

\[ w_j = \tilde{w}_j = 0 \quad (m - kn < j \leq m). \]

Then we can deduce from (3.10) and (3.11) that

\[ \exists i \quad \left| \Re \sum_{j=1}^{m} w_j^i - \Re \sum_{j=1}^{m} \tilde{w}_j^i \right| > i/2. \]

Now we can apply Lemma 2.5: there are at most \( \exp(m^{0.95}) \) polynomials \( g \in \mathcal{D}(U, m, l, k) \) possessing any prescribed collection of values

\( (n = \psi(g), \psi_1(g), \ldots, \psi_n(g), \Psi_1(g), \ldots, \Psi_n(g), \varphi_1(g), \ldots, \varphi_n(g)). \)

Finally, by (3.7), we find

\[ \# \mathcal{D}(U, m, l, k) \leq \exp(m^{0.95})N \leq \exp(m^{0.95})C^U/k (C^{1/k})^{C_U/\log m}. \]

This completes the proof of Lemma 3.1.

4. Proof of Theorem 2. Let \( n \) be a positive integer and \( \zeta \) a primitive \( n \)th root of unity. Then the polynomial

\[ Q_n(z) = \prod_{j=1}^{\phi(n)/\gcd(j,n)=1} (z - \zeta^j) \]

is called the \( n \)th cyclotomic polynomial [6, p. 64]. Note that \( \deg Q_n = \phi(n) \) where \( \phi \) is the Euler totient function.

Denote by \( g \) an integral irreducible polynomial of positive degree \( \leq m_1 \).

Let \( N \) be the number of polynomials \( f \in \mathcal{P}_d \) divisible by at least one such \( g \).

Recall that \( m_2 = \lceil \sqrt{d}/(\log d)^2 \rceil \). Then

\[ (4.1) \quad N \leq N_1 + N_2 + N_3 + N_4, \]

where

- \( N_1 \) is the number of \( f \in \mathcal{P}_d \) divisible by at least one cyclotomic \( g \) with \( \deg g \leq m_2 \),
• $N_2$ is the number of $f \in \mathcal{P}_d$ divisible by at least one noncyclotomic $g$ with $\deg g \leq m_2$,
• $N_3$ is the number of $f \in \mathcal{P}_d$ divisible by at least one $g$ with $\deg g > m_2$ and $\log M(g) \leq c$,
• $N_4$ is the number of $f \in \mathcal{P}_d$ divisible by at least one $g$ with $m_2 < \deg g \leq m_1$ and $\log M(g) > c$.

Note that all the large constants $C$ can be effectively evaluated. Considering the values of all these constants fixed, we can choose the constant $c$ in the definitions of $N_3$ and $N_4$ and the constant $c$ in the definition of $m_1$ small enough to guarantee the validity of all the forthcoming inequalities including $C$ and $c$.

We have already estimated $N_2$ in Section 1:
\[(4.2)\quad N_2 = o\left(\frac{2^d}{\sqrt{d}}\right).\]
It remains to give upper bounds for $N_1$, $N_3$, and $N_4$.

Clearly, no $f \in \mathcal{P}_d$ is divisible by $Q_1(z) = z - 1$. For $n \geq 2$ denote by $N_{1,n}$ the number of $f \in \mathcal{P}_d$ divisible by $Q_n(z)$. Suppose that the polynomial
\[f(z) = \sum_{j=0}^{d} a_j z^j\]
is divisible by $Q_n$. Let
\[h(z) = \sum_{j=0}^{n-1} A_j z^j,\]
where
\[(4.3)\quad A_j = \sum_{k \equiv j \pmod{n}} a_k.\]
The polynomials $f$ and $h$ are congruent mod$(z^n - 1)$. Therefore, $h$ is divisible by $Q_n(z)$. Let $l = \varphi(n) = \deg Q_n$. It is well known that $n \leq Cl \log \log(l + 2)$ [8, Chapter 1, Theorem 5.1]. The divisibility of $h$ by $Q_n$ determines the coefficients $A_j$ ($0 \leq j < l$) of $h$ if its other coefficients are given. This means that for fixed $a_k$ ($k \equiv j \pmod{n}$, $l \leq j < n$) all sums (4.3) for $0 \leq j < l$ are determined. For any such $j$ the proportion of vectors $(a_j, a_{j+n}, \ldots, a_{j+[d-j]/n}]n)$ satisfying (4.3) among all 0,1-vectors is at most $C \sqrt{n/d}$. We will use the fact that $C \sqrt{n/d} \leq C \sqrt{2Cm_2 \log \log m_2}/d \leq 1/d^{1/4}$. Therefore,
\[N_{1,2} \leq (C \sqrt{2/d})2^d, \quad N_{1,n} \leq 2^d/d^{1/4}, \quad l = \varphi(n) > 1,\]
and

\[ N_1 \leq 2^d \left( \frac{2C}{\sqrt{d}} + \sum_{l=2}^{m_2} \frac{\# \{ n : \varphi(n) = l \}}{d^{l/4}} \right) \leq 2^d \left( \frac{2C}{\sqrt{d}} + \sum_{l=2}^{m_2} C l(\log \log(l+2))/d^{l/4} \right) \leq 3C \cdot 2^d/\sqrt{d}. \]

To estimate \( N_3 \), we use the following simple

**Lemma 4.1.** For any irreducible polynomial \( g \) with \( \deg g = m \), there are at most \( 2^{d-1-m} \) polynomials \( f \in \mathcal{P}_d \) divisible by \( g \).

**Proof.** There are \( 2^{d-1-m} \) choices of coefficients \( a_j \) \((j = m+1, \ldots, d-1)\) of a polynomial \( f \in \mathcal{P}_d \). If these coefficients are fixed, the other coefficients are determined by the condition of divisibility of \( f \) by \( g \). The lemma is proved.

Applying Lemma 3.1 for \( U = cm, k = l = 1 \), we find that there are at most \( 1.5^m \) distinct polynomials \( g \) with \( \deg g = m \) and \( \log M(g) \leq c \) (provided that \( c \) is small enough). Hence,

\[ N_3 \leq 2^{d-1} \sum_{m=m_2+1}^{\infty} 1.5^m \cdot 2^{-m} = o(2^d/\sqrt{d}). \]

**Remark.** We have not yet used the restriction \( \deg g \leq m_1 \). Thus, we have proved that the number of polynomials \( f \in \mathcal{P}_d \) having at least one nontrivial integral divisor \( g \) with \( \log M(g) \leq c \) (in particular, cyclotomic \( g \)) does not exceed \( C 2^d/\sqrt{d} \).

The most delicate part of the proof is the estimation of \( N_4 \). We will deal with an irreducible polynomial \( g \), dividing at least one polynomial \( f \in \mathcal{P}_d \), such that \( m_2 < \deg g = m \leq m_1 \) and \( \log M(g) > c \). Applying (1.1) to \( f \) we have

\[ M(g) \leq M(f) \leq d+1. \]

We use the notation of Section 3. Let

\[ l(g) = \min \{ l \in \mathbb{Z}_+ : (l + 1) \log M(g)/k_{l+1} > \log(d+1) \}. \]

By (4.6), \( l \geq 1 \). We need the upper estimate of \( l(g) \).

**Lemma 4.2.** The number \( l = l(g) \) satisfies

\[ (2C \log(d+1)/\log M(g))^{C \log M(g)/\log m} \leq 1.05^{d/l}, \]

where \( C \) is the same constant as in the statement of Lemma 3.1.

(We may consider \( C > 1 \).)
Proof. Set \( A = 2C\log(d + 1)/\log M(g) \),
\[
l_1 = \frac{d(\log 1.05) \log m}{Cm(\log M(g)) \log A}.
\]
(A > 2 by (4.6).) We have
\[
(\log M(g)) \log A < 2C\log(d + 1)/e \leq 2C\log m_2 \leq 2C\log m,
\]
d\( d(m)/m \geq (d/m_1) \log m \),
and, consequently,
\[
l_1 \geq d(\log 1.05) \log m \geq (d/m_1) \log m \geq (d/m_1) \log m \geq (d/m_1) \log m \geq (d/m_1) \log m.
\]
(4.7) \( l_1 \geq d(\log 1.05) \log m \geq d(\log 1.05)/(2C^2m_1) > 6 \log m \)
(for an appropriate choice of a small constant \( c \) in the definition of \( m_1 \)). The lemma asserts that \( l(g) \leq l_1 \). Assume the opposite. Then for any \( l \in (l_1/2, l_1] \) we have
\[
k_l \geq l \log M(g)/\log(d + 1) > l_1 \log M(g)/(2 \log(d + 1))
\]
\[
= \frac{d(\log 1.05) \log m}{2Cm(\log(d + 1)) \log A}
\]
\[
\geq \frac{d(\log 1.05) \log m_1}{2Cm_1(\log(d + 1)) \log(2C\log(d + 1)/c)}
\]
\[
> \frac{(\log d)^{1/2}}{(\log m)^{1/2}}.
\]
Let \( p \) run over primes in \( (l_1/2, l_1] \); as \( l_1 \) is sufficiently large, there are at least \( 0.4l_1/\log l_1 \) such primes. By the property (iii) of Lemma 3 from [3] and (4.8) for \( L = \prod_p p \) we have
\[
k_L \geq \prod_p k_p \geq (\log m)^{0.2l_1/\log l_1},
\]
and substitution of (4.7) gives
\[
k_L \geq (\log m)^{1.2 \log m/(\log(6 \log m))} > m.
\]
The last inequality is impossible. Thus, our assumption was not correct, and Lemma 4.2 is proved.

For a nonnegative number \( U \) such that \( 2cm \leq U \leq 2m\log(d + 1) \) and positive integers \( k, l, m \) with \( m_1 < m \leq m_2 \), we denote by \( \mathcal{D}(U, m) \) the set of irreducible polynomials \( g \) of degree \( m \) such that \( U/(2m) < \log M(g) \leq U/m \), and by \( \mathcal{D}(U, m, l) \) the set of polynomials \( g \in \mathcal{D}(U, m) \) such that \( l(g) = l \). By the definition of \( l(g) \),
\[
k_l \geq \frac{l \log M(g)}{\log(d + 1)} \geq \frac{lU}{2m \log(d + 1)} = K.
\]
Lemma 3.1 gives the estimate of the number of polynomials in \( \mathcal{D}(U, m, l) \):
\(\begin{align*}
\#D(U,m,l) & \leq \sum_{k=K}^l \#D(U,m,l,k) \leq \sum_{k=K}^l \exp(m^{0.95} \frac{C U}{k} (C l / K)^{C U / \log m}) \\
& \leq l \exp(m^{0.95} \frac{C U}{l} (C l / K)^{C U / \log m})
\end{align*}\)

We have
\(\begin{align*}
C^U/l & = C^{2m \log(d+1)/l} \leq C^{2m_1 \log(d+1)/l} \leq 1.05^{d/l}, \\
(C l / K)^{C U / \log m} & \leq \left( \frac{2Cm \log(d+1)}{U} \right)^{C U / \log m} \\
& \leq \left( \frac{2Cm \log(d+1)}{m \log M(g)} \right)^{2Cm \log M(g)/\log m},
\end{align*}\)

and, hence, by Lemma 4.2,
\(\begin{align*}
(C l / K)^{C U / \log m} & \leq 1.05^{2d/l}.
\end{align*}\)

Substituting (4.10) and (4.11) into (4.9), we get
\(\begin{align*}
\#D(U,m,l) & \leq \sum_{k=K}^l \#D(U,m,l,k) \leq l \exp(m^{0.95} 1.05^{3d/l}) \\
& \leq \exp(m^{0.96} 1.05^{3d/l}) \leq \exp(2m^{0.96}) + 1.05^{6d/l}.
\end{align*}\)

Repeating the same arguments as in Section 1, we now show that for any \(g \in D(U,m,l)\) the condition of divisibility of \(f(z) = \sum_{j=0}^d a_j z^j \in \mathcal{P}_d\) by \(g\) uniquely determines \(f\) by its coefficients \(a_j\) with \(j \not\equiv 0 \pmod{l+1}\). Indeed, let \(z_1, \ldots, z_m\) be the zeros of \(g\), and \(G\) be the minimal polynomial for \(z_1^{l+1}\). Then \(G^k(w) = \prod_{j=1}^m (w - z_j^{l+1})\) where \(k = k_{l+1}\). By the definition of \(l(g)\), we get
\(\begin{align*}
M(G) = M(g)^{(l+1)/k} > d + 1.
\end{align*}\)

Suppose that \(g(z)\) divides two distinct polynomials \(f_1\) and \(f_2\) from \(\mathcal{P}_d\) such that
\(\begin{align*}
f_1(z) - f_2(z) = \sum_{j=0}^{[d/p]} a_j z^{j(l+1)} = h(z^{l+1}).
\end{align*}\)

Clearly, all the coefficients of the polynomial \(h\) are 0, ±1. By (1.1), \(M(h) \leq d+1\). On the other hand, \(h\) is divisible by \(G\), and (4.13) entails \(M(h) > d+1\). This contradiction shows that our supposition cannot occur. Hence,
\(\begin{align*}
\# \{ f \in \mathcal{P}_d : g \mid f \} < 2^d/2^{d(l+1)} < 2^d/1.41^{d/l}.
\end{align*}\)

Combining this estimate with Lemma 4.1 and using (4.12) and the inequality
Irreducible polynomials

\[1.05^7 < 1.41, \text{ we get }
\]

\[(4.14) \quad \# \{ f \in \mathcal{P}_d : \exists g \in \mathcal{D}(U, m) \; g \mid f \} \]
\[< 2^d \sum_l \left( \exp(2m^{0.96}) + 1.05^{6d/l} \right) \min(2^{-m}, 1.41^{-d/l}) \]
\[\leq 2^d \left( \sum_l \exp(2m^{0.96})2^{-m} + \sum_l 1.05^{-d/l} \right),\]

where the sum is taken over \( l \) for which there exists at least one polynomial \( g \in \mathcal{D}(U, m, l) \) dividing some polynomial \( f \in \mathcal{P}_d \). By Lemma 4.2, any such \( l \) satisfies

\[1.05^{-d/l} \leq C^{-cCm/\log m}.\]

Hence, it follows from (4.14) that

\[(4.15) \quad \# \{ f \in \mathcal{P}_d : \exists g \in \mathcal{D}(U, m) \; g \mid f \} \]
\[\leq 2^d m \left( \exp(2m^{0.96})2^{-m} + C^{-cCm/\log m} \right) \]
\[< 2^d \exp(-\sqrt{m}).\]

Set \( U_{j,m} = cm \cdot 2^j \) and note that if \( f \in \mathcal{P}_d \) is divisible by some polynomial \( g \) with \( m_2 < m = \deg g \leq m_1 \) and \( \log M(g) > c \), then \( g \in \mathcal{D}(U_{j,m}, m) \) for some \( j \) with \( 1 \leq j \leq J = 1 + [\log(d + 1)/c] \). Thus, from (4.15) we get

\[(4.16) \quad N_4 < 2^d \sum_{j=1}^{J} \sum_{m=m_2+1}^{m_1} \exp(-\sqrt{m}) \]
\[< C^d m_1 \exp(-\sqrt{m_2}) \log(d + 1) = o(2^d/\sqrt{d}).\]

The substitution of (4.2), (4.4), (4.5), and (4.16) into (4.1) completes the proof of Theorem 2.

As we have seen in Section 1, Theorem 1 is a corollary of Theorem 2.

References


Department of Mechanics and Mathematics
Moscow State University
Moscow, 119899, Russia
E-mail: kon@nw.math.msu.su

Received on 28.5.1997
and in revised form on 28.11.1998