ACTA ARITHMETICA
LXXXVIII.4 (1999)

On the number of irreducible polynomials with 0,1 coefficients

by

S. V. Konyagin (Moscow)

1. Introduction. For d a positive integer, let

$$\mathcal{P}_d = \Big\{ f(z) : f(z) = \sum_{j=0}^{d} a_j z^j,\ a_j = 0 \text{ or } 1 \text{ for all } j,\ a_0 = a_d = 1 \Big\}.$$

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 $d \ge 2$ 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 $m_1 = [cd/\log d]$ 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 Φ of integers $\gamma p \in [2^d, 2^{d+1})$ where p is prime, γ is odd and $\gamma < \gamma_1 = 1.12^{m_1}$. 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,

$$^{\#}\Phi \gg \frac{2^d}{d} \sum_{\substack{\gamma<\gamma_1 \\ \gamma\equiv 1 \,(\mathrm{mod}\, 2)}} \frac{1}{\gamma} \gg \frac{2^d}{d} \log \gamma_1 \gg 2^d/\log d,$$

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 p, we get $|g_2(2)| \leq \gamma$ and

$$\varphi = |g_1(2)| \cdot |g_2(2)| \leq |g_2(2)|^2 \leq \gamma_1^2 < 2^{m_1} < \varphi.$$

This contradiction shows that $g_1(2)$ cannot be divisible by p. 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 Ω restricted by the segment of the line $\Re z = 1.14$, $|\Im z|^2 \leq 4 - 1.14^2$, and the arc of the circle $|z| = 2$, $\Re z \leq 1.14$. The maximum of $|V(z)|$ is attained on the boundary of Ω. If z is on the segment then

$$\begin{aligned} |V(z)| &= (0.14^2 + \Im z^2)/(0.86^2 + \Im z^2) \\ &\leq (0.14^2 + 4 - 1.14^2)/(0.86^2 + 4 - 1.14^2) = 34/43. \end{aligned}$$

If z is on the arc then

$$\begin{aligned} |V(z)| &= (|z|^2 + 1 - 2\Re z)/(|z|^2 + 4 - 4\Re z) = (5 - 2\Re z)/(8 - 4\Re z) \\ &\leq (5 - 2 \cdot 1.14)/(8 - 4 \cdot 1.14) = 34/43. \end{aligned}$$

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 $m_2 = [\sqrt{d}/(\log d)^2]$. For any polynomial g with leading coefficient ± 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,

$$M\Big(\sum_{j=0}^{m} b_j z^j\Big) \leq \sum_{j=0}^{m} |b_j|. \tag{1.1}$$

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],

$$M(g) \geq \exp(\lambda_m), \qquad \lambda_m = c\left(\frac{\log\log m}{\log m}\right)^3 \qquad (m \geq 3). \tag{1.2}$$

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

$$M(g_p) = M(g)^p \geq \exp(p\lambda_{m_2}) > d + 1. \tag{1.3}$$

Suppose that $g(z)$ divides two distinct polynomials f_1 and f_2 from $\mathcal{P}_d$ such that

$$f_1(z) - f_2(z) = \sum_{j=0}^{[d/p]} a_j z^{jp} = h(z^p).$$

Clearly, all coefficients of the polynomial h are $0, \pm 1$. 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_p, 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, $j \not\equiv 0 \pmod{p}$. Hence,

$$\begin{aligned} {}^{\#}\{f \in \mathcal{P}_d : g \mid f\} &< 2^d/2^{d/p} < 2^d/2^{d\lambda_{m_2}/(2\log(d+1))} \\ &< 2^d \exp(-0.3 d\lambda_{m_2}/\log d). \end{aligned} \tag{1.4}$$

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,

$$N < \prod_{j=0}^{m_2} (2 \cdot 4^{m_2} + 1) < 5^{m_2^2}.$$

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

$$\begin{aligned} 2^d 5^{m_2^2} \exp(-0.3 d\lambda_{m_2}/\log d) &< 2^d \exp(2d/(\log d)^4 - 0.3 d\lambda_{m_2}/\log d) \\ &= o(2^d/\sqrt{d}). \end{aligned}$$

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 ε-capacity of appropriate convex bodies in finite-dimensional spaces. Such estimates will be found in Section 2. Theorem 2 will be proved in Section 4.

2. Several geometric lemmas. In this section we fix two positive numbers α and τ such that

$$\alpha > 1, \quad \tau < 0.1/\alpha. \tag{2.1}$$

Also, m will denote a sufficiently large positive integer exceeding some magnitude depending on α and τ. Let $X = X_m$ be the m-dimensional real coordinate space equipped with the l_∞-norm:

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

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

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

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

provided that l is large enough.

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

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

Using the inequality

$$\mathrm{Vol}(A) \le \mathrm{Vol}(B)\left(\frac{10\alpha \log l}{l}\right)^{l/2}$$

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

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

as required.

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

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

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

$$O(A) = \{x + y : x \in A,\ |y| \le 1/2\}.$$

We have

$$O(A) = O_1(\ldots O_m(A)\ldots). \tag{2.2}$$

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 $\mathrm{Vol}_0(P_\emptyset(A)) = 1$.

LEMMA 2.2. *For any $T \in \Sigma$ and any $j \in T$ we have*

$$\mathrm{Vol}_{\#T}(P_T(O_j(A))) = \mathrm{Vol}_{\#T}(P_T(A)) + \mathrm{Vol}_{\#T-1}(P_{T\setminus\{j\}}(A)).$$

Proof. Set $T' = T \setminus \{j\}$ and represent P_T in the following form:

$$P_T(A) = \{\{x_t : t \in T\} : \{x_t : t \in T'\} \in P_{T'}(A),$$
$$f_1(\{x_t : t \in T'\}) \le x_j \le f_2(\{x_t : t \in T'\})\}.$$

Then

$$P_T(O_j(A)) = \{\{x_t : t \in T\} : \{x_t : t \in T'\} \in P_{T'}(A),$$
$$f_1(\{x_t : t \in T'\}) - 1/2 \le x_j \le f_2(\{x_t : t \in T'\}) + 1/2\}.$$

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*:

$$\mathrm{Vol}(O(A)) = \sum_{T\in\Sigma} \mathrm{Vol}_{\#T}(P_T(A)). \tag{2.3}$$

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 $n \le m^{\alpha-1}$ 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, $^{\#}D \le \mathrm{Vol}(O(a))$, 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 $l = {}^{\#}T \ge m^{1-10\tau}$ the volumes on the right-hand side of (2.3) can be estimated by Lemma 2.1:

$$\begin{aligned}\mathrm{Vol}_l(P_T(A)) &< \mathrm{Vol}_l(P_T(\Pi))\left(\frac{90\alpha\log l}{l}\right)^{l/2}\\ &\le \mathrm{Vol}_l(P_T(\Pi))\left(\frac{90\alpha\log m}{m^{1-10\tau}}\right)^{l/2} < \mathrm{Vol}_l(P_T(\Pi))(m^{0.5-6\tau})^{-l}.\end{aligned}$$

For $l < m^{1-10\tau}$ using the trivial estimate $\mathrm{Vol}_l(P_T(A)) \le \mathrm{Vol}_l(P_T(\Pi))$ we have

$$\begin{aligned}\mathrm{Vol}_l(P_T(A)) &\le \mathrm{Vol}_l(P_T(\Pi))(m^{0.5-6\tau})^{-l}(m^{0.5-6\tau})^{l}\\ &< \mathrm{Vol}_l(P_T(\Pi))(m^{0.5-6\tau})^{-l}(m^{0.5-6\tau})^{m^{1-10\tau}}\\ &< \mathrm{Vol}_l(P_T(\Pi))(m^{0.5-6\tau})^{-l}\exp(m^{1-9\tau}).\end{aligned}$$

In both cases we have the inequality

$$\mathrm{Vol}_{\#T}(P_T(A)) < \mathrm{Vol}_{\#T}(P_T(\Pi))(m^{0.5-6\tau})^{-\#T}\exp(m^{1-9\tau}). \tag{2.4}$$

Now, using (2.3), we find

$$\begin{aligned}\mathrm{Vol}(O(A)) &< \exp(m^{1-9\tau})\sum_{T\in\Sigma}\mathrm{Vol}_{\#T}(P_T(\Pi))(m^{0.5-6\tau})^{-\#T}\\ &= \exp(m^{1-9\tau})\prod_{j=1}^{m}\left(1+\frac{u_j}{m^{0.5-6\tau}}\right).\end{aligned}$$

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 $\max_j|w_j| \le \exp(0.4(\log m)/m)$ for any $w=(w_1,\ldots,w_m)\in W$ and $\max_{1\le k\le m}|\Re S_k(w)-\Re S_k(w')|/k > 1/2$ 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 $\widetilde{w} = (\widetilde{w}_1,\ldots,\widetilde{w}_m)$ such that

$$\widetilde{w}_j = m^{-2.45}(\mathrm{sgn}(\Re w_j)[m^{2.45}|\Re w_j|] + i\,\mathrm{sgn}(\Im w_j)[m^{2.45}|\Im w_j|]) \quad (j=1,\ldots,m),$$

where $[\cdot]$ denotes the integral part. For any $j\in\{1,\ldots,m\}$ and $k\in\{1,\ldots,m\}$

we have $|w_j - \widetilde{w}_j| \le \sqrt{2}\, m^{-2.45}$ and

$$\begin{aligned}|w_j^k - \widetilde{w}_j^k| &\le k|w_j - \widetilde{w}_j| \max(|w_j|^{k-1}, |\widetilde{w}_j|^{k-1})\\ &\le 2km^{-2.45}(\exp(0.4(\log m)/m))^{k-1}\\ &\le 2m^{-1.45}(\exp(0.4(\log m)/m))^m = 2m^{-1.05}.\end{aligned}$$

From the last inequality and the assumption on W we get

$$\max_{1\le k\le m} |\Re S_k(\widetilde{w}) - \Re S_k(\widetilde{w}')|/k > 1/3 \qquad (w, w' \in W,\ w \ne w'). \tag{2.5}$$

Consider the mapping $\psi : W \to X$:

$$\psi(w) = (3\Re S_1(\widetilde{w}), 3\Re S_2(\widetilde{w})/2, \ldots, 3\Re S_m(\widetilde{w})/m).$$

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 $(3m\Re z, 3m\Re(z^2)/2, \ldots, 3m\Re(z^m)/m)$, where $|z| \le \exp(0.4(\log m)/m)$ and $m^{2.45}\Re z$, $m^{2.45}\Im z$ are integers (i.e. z runs over the set of all possible points $\widetilde{w}_j$). The number n of the vertices of the polytope A does not exceed

$$\pi(1 + \exp(0.4(\log m)/m)/m^{-2.45})^2 < m^6.$$

Moreover, A is contained in the parallelepiped

$$\Pi = \prod_{j=1}^{m} [-u_j/2, u_j/2], \qquad u_j = 6m\exp(0.4(j/m)\log m)/j \qquad (j = 1, \ldots, m).$$

Now we are ready to apply Lemma 2.4. Take $\alpha = 7$, $\tau = 1/150$. Lemma 2.4 asserts that

$$^{\#}D < \exp(m^{0.94}) \prod_{j=1}^{m} \left(1 + \frac{u_j}{m^{0.46}}\right). \tag{2.6}$$

We have

$$\log \prod_{j=1}^{m} \left(1 + \frac{u_j}{m^{0.46}}\right) \le \sum_{j=1}^{m} \frac{u_j}{m^{0.46}} \le \sum_{j=1}^{m} \frac{6m^{0.94}}{j} < m^{0.945}.$$

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 $(z')^l = z^l$ 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 $\mathcal{D}(U, m, l, k)$ 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 $\mathcal{D}(U, m, l, k)$ is empty.

LEMMA 3.1. *For sufficiently large m the cardinality of $\mathcal{D}(U, m, l, k)$ does not exceed*

$$\exp(m^{0.95})C^{U/k}(Cl/k)^{CU/\log m}.$$

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 $g \in \mathcal{D}(U, m, l, k)$ 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 ψ, we define several mappings on the set $\mathcal{D}(U, m, l, k)$. 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

$$\prod_{j=1}^{n} |v_j| \geq \prod_{j=1}^{n} \exp(\psi_j(g)/m) = \exp\Big(\sum_{j=1}^{n} \psi_j(g)/m\Big).$$

Therefore,

$$\psi(g) = n \leq U/(0.4k \log m) \tag{3.1}$$

and

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

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

$$S_\nu^u = [\alpha/(m^3 v), (\alpha+1)/(m^3 v)) \times [\beta/(m^3 v), (\beta+1)/(m^3 v)),$$
$$v = \exp((m-1)u/m), \quad \alpha, \beta \in \mathbb{Z}, \quad \nu \in \mathbb{Z},\ 1 \leq \nu \leq N_u.$$

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:

$$N_u \le m^7\exp(2u). \tag{3.3}$$

We define the mappings Ψ_j ($j=1,\dots,n$) setting $\Psi_j(g)=\nu$ if $v_j\in S_\nu^u$ where $u=\psi_j(g)$. Finally, for $j=1,\dots,n$ we define the mapping φ_j from $\mathcal{D}(U,m,l,k)$ to the set $\Sigma(k,l)$ of k-element subsets of $\{1,\dots,l\}$ 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 ζ is a fixed primitive lth root of unity.

We want to estimate the number of distinct images

$$(n=\psi(g),\psi_1(g),\dots,\psi_n(g),\Psi_1(g),\dots,\Psi_n(g),\varphi_1(g),\dots,\varphi_n(g))$$

for $g\in\mathcal{D}(U,m,l,k)$.

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

$$^{\#}\{(n,\psi_1(g),\dots,\psi_n(g))\}\le\sum_{n=0}^{[U/k]}\binom{[U/k]}{n}\le 2^{U/k}. \tag{3.4}$$

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

$$\begin{aligned}^{\#}\{(\Psi_1(g),\dots,\Psi_n(g))\}&\le\prod_{j=1}^{n}(m^7\exp(2\psi_j(g)))\\&\le m^{7U/(0.4k\log m)}\exp(2U/k)\le C^{U/k}.\end{aligned}\tag{3.5}$$

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

$$\binom{l}{k}\le l^k/k!\le(el/k)^k,$$

we obtain

$$\begin{aligned}&^{\#}\{(\varphi_1(g),\dots,\varphi_n(g))\}\\&\qquad\le\binom{l}{k}^n\le(el/k)^{kU/(0.4k\log m)}\le(el/k)^{CU/\log m}.\end{aligned}\tag{3.6}$$

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

$$\begin{aligned}&^{\#}\{(n,\psi_1(g),\dots,\psi_n(g),\Psi_1(g),\dots,\Psi_n(g),\varphi_1(g),\dots,\varphi_n(g))\}\\&\qquad\le N=(2C)^{U/k}(el/k)^{CU/\log m}.\end{aligned}\tag{3.7}$$

Consider two polynomials $g \in \mathcal{D}(U, m, l, k)$ and $\widetilde{g} \in \mathcal{D}(U, m, l, k)$ such that

$$\begin{aligned} \psi(g) = \psi(\widetilde{g}), \quad \psi_j(g) = \psi_j(\widetilde{g}) \quad (j = 1, \ldots, n), \\ \Psi_j(g) = \Psi_j(\widetilde{g}) \quad (j = 1, \ldots, n), \quad \varphi_j(g) = \varphi_j(\widetilde{g}) \quad (j = 1, \ldots, n). \end{aligned} \tag{3.8}$$

Define

$$\begin{aligned} Z &= \{z : g(z) = 0\}, \quad \widetilde{Z} = \{z : \widetilde{g}(z) = 0\}, \\ V &= \{v \in Z : |v| \geq \exp(0.4(\log m)/m)\}, \\ \widetilde{V} &= \{v \in \widetilde{Z} : |v| \geq \exp(0.4(\log m)/m)\}, \\ W &= \{w \in Z : |w| < \exp(0.4(\log m)/m)\}, \\ \widetilde{W} &= \{w \in \widetilde{Z} : |w| < \exp(0.4(\log m)/m)\}. \end{aligned}$$

Let $n = \psi(g) = \psi(\widetilde{g})$. For any $j = 1, \ldots, n$ we take $u = \psi_j(g) = \psi_j(\widetilde{g})$, $v = \exp((m-1)u/m)$ and the corresponding zeros v_j of g and $\widetilde{v}_j$ of $\widetilde{g}$. Since the values of Ψ_j at g and $\widetilde{g}$ coincide, we have

$$\begin{aligned} |v_j - \widetilde{v}_j| &\leq \sqrt{2}/(m^3 v) < 4/(m^3 \exp((m-1)(u+1)/m)) \\ &\leq 4 \max(|v_j|, |\widetilde{v}_j|)^{1-m}/m^3. \end{aligned} \tag{3.9}$$

For any zero $v \in V$ of g equivalent to v_j we set $\chi(v) = v\widetilde{v}_j/v_j$. As the values of φ_j at g and $\widetilde{g}$ coincide, χ is a one-to-one correspondence $V \to \widetilde{V}$. By (3.9), $|\chi(v) - v| \leq 4|\max(|v|, |\chi(v)|)^{1-m}|/m^3$ for any $v \in V$. Therefore,

$$\begin{aligned} |(\chi(v))^i - v^i| &\leq i \max(|v|, |\chi(v)|)^{i-1} |\chi(v) - v| \\ &< m \max(|v|, |\chi(v)|)^{m-1} |\chi(v) - v| \leq 4/m^2 \quad (i = 1, \ldots, m), \end{aligned}$$

and

$$\Big| \sum_{v \in V} v^i - \sum_{v \in \widetilde{V}} v^i \Big| < 1/2 \quad (i = 1, \ldots, m). \tag{3.10}$$

Let

$$\begin{aligned} g(z) &= \sum_{j=0}^{m} b_j z^j, \quad b_m = 1, \\ S_i &= \sum_{z \in Z} z^i = \sum_{v \in V} v^i + \sum_{w \in W} w^i \quad (i = 1, \ldots, m), \\ \widetilde{S}_i &= \sum_{z \in \widetilde{Z}} z^i = \sum_{v \in \widetilde{V}} v^i + \sum_{w \in \widetilde{W}} w^i \quad (i = 1, \ldots, m). \end{aligned}$$

The numbers $S_1, \ldots, S_m$ are integers. Moreover, by the Newton identities,

$$S_i + b_{m-1} S_{i-1} + \ldots + b_{m-i+1} S_1 + i b_{m-i} = 0 \quad (i = 1, \ldots, m).$$

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 $\widetilde{g}$ are distinct then we can take the minimal i such that $S_i \neq \widetilde{S}_i$. Then $S_i \equiv \widetilde{S}_i \pmod{i}$ and, hence,

$$\exists i \quad |S_i - \widetilde{S}_i| \geq i,$$

or

$$\exists i \quad \Big|\sum_{v\in V} v^i + \sum_{w\in W} w^i - \sum_{v\in\widetilde{V}} v^i - \sum_{w\in\widetilde{W}} w^i\Big| \geq i. \tag{3.11}$$

Let

$$W = \{w_1, \ldots, w_{m-kn}\}, \quad \widetilde{W} = \{\widetilde{w}_1, \ldots, \widetilde{w}_{m-kn}\},$$
$$w_j = \widetilde{w}_j = 0 \quad (m - kn < j \leq m).$$

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

$$\exists i \quad \Big|\Re\sum_{j=1}^{m} w_j^i - \Re\sum_{j=1}^{m} \widetilde{w}_j^i\Big| > i/2.$$

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

$$^{\#}\mathcal{D}(U, m, l, k) \leq \exp(m^{0.95})N \leq \exp(m^{0.95})C^{U/k}(Cl/k)^{CU/\log m}.$$

This completes the proof of Lemma 3.1.

4. Proof of Theorem 2. Let n be a positive integer and ζ a primitive nth root of unity. Then the polynomial

$$Q_n(z) = \prod_{\substack{j=1\\ \gcd(j,n)=1}}^{n} (z - \zeta^j)$$

is called the nth *cyclotomic polynomial* [6, p. 64]. Note that $\deg Q_n = \varphi(n)$ where φ 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 $m_2 = [\sqrt{d}/(\log d)^2]$. Then

$$N \leq N_1 + N_2 + N_3 + N_4, \tag{4.1}$$

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 $\deg g \le m_2$,

• N_3 is the number of $f \in \mathcal{P}_d$ divisible by at least one g with $\deg g > m_2$ and $\log M(g) \le c$,

• N_4 is the number of $f \in \mathcal{P}_d$ divisible by at least one g with $m_2 < \deg g \le m_1$ 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:

$$N_2 = o(2^d/\sqrt{d}). \tag{4.2}$$

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 $n \ge 2$ 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

$$A_j = \sum_{k \equiv j \pmod{n}} a_k. \tag{4.3}$$

The polynomials f and h are congruent $\bmod(z^n - 1)$. Therefore, h is divisible by $Q_n(z)$. Let $l = \varphi(n) = \deg Q_n$. It is well known that $n \le Cl \log\log(l+2)$ [8, Chapter 1, Theorem 5.1]. The divisibility of h by Q_n determines the coefficients A_j $(0 \le j < l)$ of h if its other coefficients are given. This means that for fixed a_k $(k \equiv j \pmod{n},\ l \le j < n)$ all sums (4.3) for $0 \le j < l$ 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 $C\sqrt{n/d} \le C\sqrt{2Cm_2(\log\log m_2)/d} \le 1/d^{1/4}$. Therefore,

$$N_{1,2} \le (C\sqrt{2/d})2^d, \quad N_{1,n} \le 2^d/d^{l/4}, \quad l = \varphi(n) > 1,$$

and

$$N_1 \le 2^d\Big(2C/\sqrt{d} + \sum_{l=2}^{m_2} {}^{\#}\{n : \varphi(n) = l\}/d^{l/4}\Big) \tag{4.4}$$
$$\le 2^d\Big(2C/\sqrt{d} + \sum_{l=2}^{m_2} Cl(\log\log(l+2))/d^{l/4}\Big) \le 3C \cdot 2^d/\sqrt{d}.$$

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 $\log M(g) \le c$ (provided that c is small enough). Hence,

$$N_3 \le 2^{d-1} \sum_{m=m_2+1}^{\infty} 1.5^m \cdot 2^{-m} = o(2^d/\sqrt{d}). \tag{4.5}$$

REMARK. We have not yet used the restriction $\deg g \le m_1$. Thus, we have proved that the number of polynomials $f \in \mathcal{P}_d$ having at least one nontrivial integral divisor g with $\log M(g) \le c$ (in particular, cyclotomic g) does not exceed $C2^d/\sqrt{d}$.

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 $m_2 < \deg g = m \le m_1$ and $\log M(g) > c$. Applying (1.1) to f we have

$$M(g) \le M(f) \le d+1. \tag{4.6}$$

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), $l \ge 1$. We need the upper estimate of $l(g)$.

LEMMA 4.2. *The number $l = l(g)$ satisfies*

$$(2C\log(d+1)/\log M(g))^{Cm\log M(g)/\log m} \le 1.05^{d/l},$$

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

(We may consider $C > 1$.)

P r o o f. 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

$$(\log M(g))\log A \le 2C\log(d+1)/e \le 2C\log m_2 \le 2C\log m,$$
$$d(\log m)/m \ge (d/m_1)\log m,$$

and, consequently,

$$l_1 \ge \frac{d(\log 1.05)\log m}{2C^2 m\log m} \ge d(\log 1.05)/(2C^2 m_1) > 6\log m \tag{4.7}$$

(for an appropriate choice of a small constant c in the definition of m_1). The lemma asserts that $l(g) \le l_1$. Assume the opposite. Then for any $l \in (l_1/2, l_1]$ we have

$$\begin{aligned} k_l &\ge l\log M(g)/\log(d+1) > l_1\log M(g)/(2\log(d+1)) \\ &= \frac{d(\log 1.05)\log m}{2Cm(\log(d+1))\log A} \\ &\ge \frac{d(\log 1.05)\log m_1}{2Cm_1(\log(d+1))\log(2C\log(d+1)/c)} \\ &> (\log d)^{1/2} > (\log m)^{1/2}. \end{aligned} \tag{4.8}$$

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

$$k_L \ge \prod_p k_p \ge (\log m)^{0.2l_1/\log l_1},$$

and substitution of (4.7) gives

$$k_L \ge (\log m)^{1.2\log m/\log(6\log m)} > m.$$

The last inequality is impossible. Thus, our assumption was not correct, and Lemma 4.2 is proved.

For a nonnegative number U such that $2cm \le U \le 2m\log(d+1)$ and positive integers k, l, m with $m_1 < m \le m_2$, we denote by $\mathcal{D}(U, m)$ the set of irreducible polynomials g of degree m such that $U/(2m) < \log M(g) \le U/m$, 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 $l(g)$,

$$k_l \ge \frac{l\log M(g)}{\log(d+1)} \ge \frac{lU}{2m\log(d+1)} = K.$$

Lemma 3.1 gives the estimate of the number of polynomials in $\mathcal{D}(U, m, l)$:

$$\begin{aligned}(4.9)\quad {}^{\#}\mathcal{D}(U,m,l)& \\ &\le \sum_{k=K}^{l} {}^{\#}\mathcal{D}(U,m,l,k) \le \sum_{k=K}^{l} \exp(m^{0.95}) C^{U/k} (Cl/k)^{CU/\log m} \\ &\le l\exp(m^{0.95}) C^{U/K} (Cl/K)^{CU/\log m}.\end{aligned}$$

We have

$$C^{U/K} = C^{2m\log(d+1)/l} \le C^{2m_1\log(d+1)/l} \le 1.05^{d/l},$$

$$(4.10)\qquad \begin{aligned}(Cl/K)^{CU/\log m} &\le \left(\frac{2Cm\log(d+1)}{U}\right)^{CU/\log m} \\ &\le \left(\frac{2Cm\log(d+1)}{m\log M(g)}\right)^{2Cm\log M(g)/\log m},\end{aligned}$$

and, hence, by Lemma 4.2,

$$(4.11)\qquad (Cl/K)^{CU/\log m} \le 1.05^{2d/l}.$$

Substituting (4.10) and (4.11) into (4.9), we get

$$\begin{aligned}(4.12)\quad {}^{\#}\mathcal{D}(U,m,l) &\le \sum_{k=K}^{l} {}^{\#}\mathcal{D}(U,m,l,k) \le l\exp(m^{0.95})1.05^{3d/l} \\ &\le \exp(m^{0.96})1.05^{3d/l} \le \exp(2m^{0.96}) + 1.05^{6d/l}.\end{aligned}$$

Repeating the same arguments as in Section 1, we now show that for any $g \in \mathcal{D}(U,m,l)$ 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

$$(4.13)\qquad M(G) = M(g)^{(l+1)/k} > d+1.$$

Suppose that $g(z)$ divides two distinct polynomials f_1 and f_2 from $\mathcal{P}_d$ such that

$$f_1(z) - f_2(z) = \sum_{j=0}^{[d/p]} a_j z^{j(l+1)} = h(z^{l+1}).$$

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

$${}^{\#}\{f \in \mathcal{P}_d : g \mid f\} < 2^d/2^{d/(l+1)} < 2^d/1.41^{d/l}.$$

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

$1.05^7 < 1.41$, we get

$$\begin{aligned}(4.14)\qquad {}^{\#}\{f \in \mathcal{P}_d : \exists g \in \mathcal{D}(U,m)\ g \mid f\} \\ &< 2^d \sum_l (\exp(2m^{0.96}) + 1.05^{6d/l}) \min(2^{-m}, 1.41^{-d/l}) \\ &\le 2^d \Big(\sum_l \exp(2m^{0.96}) 2^{-m} + \sum_l 1.05^{-d/l} \Big),\end{aligned}$$

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

$$1.05^{-d/l} \le C^{-cCm/\log m}.$$

Hence, it follows from (4.14) that

$$\begin{aligned}(4.15)\qquad {}^{\#}\{f \in \mathcal{P}_d : \exists g \in \mathcal{D}(U,m)\ g \mid f\} \\ &\le 2^d m (\exp(2m^{0.96}) 2^{-m} + C^{-cCm/\log m}) \\ &< 2^d \exp(-\sqrt{m}).\end{aligned}$$

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

$$\begin{aligned}(4.16)\qquad N_4 &< 2^d \sum_{j=1}^{J} \sum_{m=m_2+1}^{m_1} \exp(-\sqrt{m}) \\ &< C 2^d m_1 \exp(-\sqrt{m_2}) \log(d+1) = o(2^d/\sqrt{d}).\end{aligned}$$

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

[1] I. Bárány and Z. Füredi, *Computing the volume is difficult*, Discrete Comput. Geom. 2 (1987), 319–326.

[2] J. Brillhart, M. Filaseta and A. M. Odlyzko, *On an irreducibility theorem of A. Cohn*, Canad. J. Math. 33 (1981), 1055–1059.

[3] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.

[4] M. Filaseta, *Irreducibility criteria for polynomials with nonnegative coefficients*, Canad. J. Math. 40 (1988), 339–351.

[5] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 53 (1857), 133–175.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, 1983.

[7] A. M. Odlyzko and B. Poonen, *Zeros of polynomials with* $0,1$ *coefficients*, Enseign. Math. 39 (1993), 317–348.
[8] K. Prachar, *Primzahlverteilung*, Springer, Berlin, 1957.
[9] V. Tikhomirov, *Some Problems of Approximation Theory*, Moscow State University, Moscow, 1976 (in Russian).
[10] E. C. Titchmarsh, *The Theory of Functions*, 2nd ed., Oxford Univ. Press, 1939.

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 (3192)