PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 124, Number 6, June 1996

POLYNOMIALS WITH ROOTS MODULO EVERY INTEGER

DANIEL BEREND AND YURI BILU

(Communicated by William W. Adams)

ABSTRACT. Given a polynomial with integer coefficients, we calculate the density of the set of primes modulo which the polynomial has a root. We also give a simple criterion to decide whether or not the polynomial has a root modulo every non-zero integer.

1. INTRODUCTION

In [BO] and [BH] the diophantine equation

$$P(x) = n!\,,$$

where P is a polynomial with integer coefficients, was studied (we refer to [EO] and [Gu, Sec.D25] for related equations and more information). On probabilistic grounds, one expects that, if $\deg P \geq 2$, then the equation has only finitely many solutions. One case in which this is trivial is when the congruence

$$P(x) \equiv 0 \pmod{m} \tag{1}$$

happens to have no root for some integer m. This raises the following

Question. Given a polynomial $P(x) \in \mathbf{Z}[x]$, decide whether or not (1) has a solution for every m.

The same question is also motivated by a more general result. A *measure-preserving system* is a quadruple $(X, \mathcal{B}, \mu, T)$, in which $(X, \mathcal{B}, \mu)$ is a probability space, and T is a measure-preserving transformation thereof. A set $R \subseteq \mathbf{N}$ is a *Poincaré set* if for any measure-preserving system $(X, \mathcal{B}, \mu, T)$ and $A \in \mathcal{B}$ with $\mu(A) > 0$ there exists some $n \in R$ with $\mu(T^{-n}A \cap A) > 0$ [Fu, Def.3.6]. An interesting question is which "natural" sets of integers are Poincaré sets. It turns out that, for $P \in \mathbf{Z}[x]$, the set $\{P(n) : n \in \mathbf{N}\}$ is a Poincaré set if and only if (1) has a root for each m. A consequence is that, if P is such and S is a set of integers of positive (upper Banach) density, then there exist $s_1, s_2 \in S,\ s_1 \neq s_2$, and $n \in \mathbf{N}$ such that $s_2 - s_1 = P(n)$. This result was first proved by Sárközy for the polynomial $P(x) = x^2$ [Sá1] (see also [Sá2] and [Sá3], where other polynomials

Received by the editors March 7, 1994 and, in revised form, November 28, 1994.
1991 *Mathematics Subject Classification.* Primary 11R09, 11R45; Secondary 11D61, 11U05.
Key words and phrases. Diophantine equations, congruences, effective number theory, Poincaré sets.

are dealt with). It does not seem to have been explicitly stated in the form above, but certainly follows from the results and the discussion in [Fu, Ch.3]. For more on this direction, see [Bo] (in particular, Theorem 6.6 there).

Another result involving polynomials that satisfy the property in question is due to Kamae and Mendes France [KM]. The well-known difference theorem of van der Corput states that, if $(x_n)_{n=1}^{\infty}$ is a sequence in $\mathbf{R}$ such that for every positive integer h the sequence $(x_{n+h} - x_n)_{n=1}^{\infty}$ is uniformly distributed modulo 1, then $(x_n)_{n=1}^{\infty}$ is also uniformly distributed modulo 1 (see, for example, [KN]). Kamae and Mendes France noted that there exist sets $H \subseteq \mathbf{N}$ such that it suffices to check the difference condition for each $h \in H$ to obtain the same conclusion. One of their examples of such a set H is the set of all values assumed by some integer polynomial satisfying our condition.

Obviously, (1) is solvable for each m if P has a linear monic factor $x - a$. The interest in the question stems from the fact that there are polynomials not having a linear factor, which still enjoy this property.

Example 1. The polynomial

$$P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 221)$$

has no integer (or rational) roots, but has a root modulo every integer (see [BS, p.3]).

It turns out that the question presented above is in fact decidable, and even in much more generality ([A], [FS]). In this paper we present a relatively simple answer to this question. We also find, given a polynomial $P(x) \in \mathbf{Z}[x]$, the density of the set of primes p for which (1) has a solution for $m = p$. (The fact that this set of primes has some Dirichlet density which is, moreover, a rational number, follows as a very special case from a result of Ax [A].)

We wish to express our gratitude to M. Boshernitzan for his comments and suggestions on this paper and to the referee for his helpful remarks.

2. The main results

Given $P(x) \in \mathbf{Z}[x]$, factorize it as a product of polynomials in $\mathbf{Z}[x]$, irreducible over $\mathbf{Q}$:

$$P(x) = h_1(x) \cdot \ldots \cdot h_\nu(x)\,.$$

(Here we assumed implicitly that the greatest common divisor of the coefficients of the polynomial $P(x) = a_n x^n + \cdots + a_0$ is 1 – otherwise the factorization is non-unique. Of course, this has no bearing on the paper, since for our results P may be replaced by $P/\gcd(a_0, a_1, \ldots, a_n)$, which is a polynomial that possesses the desired property.) To state our theorem we need a few notation. First, let L be the splitting field of P over $\mathbf{Q}$ and $G =$Gal $(L/\mathbf{Q})$ the Galois group of this extension. For $1 \le i \le \nu$, let θ_i be a fixed root of h_i, and put $K_i = \mathbf{Q}(\theta_i)$ and $H_i =$ Gal $(L/K_i) \le G$. Finally, set $U = \bigcup_{i=1}^{\nu} H_i \subseteq G$. We also need some constants. Write:

$$h_i(x) = \sum_{j=0}^{n_i} a_{ij} x^j\,.$$

Denote:

δ_i – the discriminant of h_i;
$\rho_i = a_{in_i}\delta_i = R(h_i, h_i')$ – the resultant of h_i and h_i' [vW, §35];
$\delta = \rho_1 \cdot \ldots \cdot \rho_\nu$;
$\delta = p_1^{\alpha_1} \cdot \ldots \cdot p_\mu^{\alpha_\mu}$ – the prime power factorization of δ;
$\Delta = p_1^{2\alpha_1+1} \cdot \ldots \cdot p_\mu^{2\alpha_\mu+1}$;
$D = \left(\prod_{i=1}^{\nu} \delta_i^{\frac{n_i-1}{n_i}}\right)^{n_1! \cdot \ldots \cdot n_\nu!}$.

Note that all these constants are integers, and are directly computable from the polynomials $h_1, h_2, \ldots, h_\nu$.

Theorem 1. *The following conditions are equivalent:*

(a) *P has a root* mod m *for every non-zero integer m;*
(b) *P has a root* mod Δ, *and*

$$\bigcup_{\sigma \in G} \sigma^{-1} U \sigma = G; \tag{2}$$

(c) *P has a root* mod Δ *and* mod p *for each prime $p \leq 2D^A$. (Here A is an effective absolute constant, to be defined later.)*

Remark 1. As follows from the results of Lagarias and Odlyzko [LO], under the Generalized Riemann Hypothesis (henceforward GRH), the term $2D^A$ in (c) may be replaced by $c_1 (\log D)^2$. Oesterlé [O] proved that one may take $c_1 = 70$. Bach [Ba] obtained further numerical results in this direction, but they are not general enough for the purposes of the present paper (see the discussion in [Ba], p.376).

Example 2. Condition (2) reveals that, for P to have the property under consideration without having rational roots, G has to be a union of proper subgroups thereof. The smallest group for which this occurs is the non-cyclic group of order 4. (Indeed, the condition is always fulfilled unless G is cyclic.) G is a union of three subgroups of order 2, so that P must be of degree 6 at least. This is the case in Example 1. With the group $G = S_3$ one can obtain a polynomial of degree 5 having the same properties:

$$P(x) = (x^3 - 19)(x^2 + x + 1).$$

In fact, in this case we have $L = \mathbf{Q}(\sqrt[3]{19}, i\sqrt{3}),\ G = S_3$ and:

$$\theta_1 = \sqrt[3]{19}, \quad \theta_2 = \frac{-1 + i\sqrt{3}}{2}.$$

The subgroup $H_1 = \mathrm{Gal}(L/\mathbf{Q}(\sqrt[3]{19}))$ is of order 2, and the union of its conjugates is the set of 4 elements of S_3 of orders 1 and 2. The subgroup $H_2 = \mathrm{Gal}(L/\mathbf{Q}(i\sqrt{3}))$ is of order 3. Thus condition (2) of Theorem 1 is satisfied. Now one calculates routinely

$$\delta_1 = 3^3 \cdot 19^2, \quad \delta_2 = 3,$$

so that

$$\delta = 3^4 \cdot 19^2, \quad \Delta = 3^9 \cdot 19^5.$$

It is easily verified that the congruence

$$x^2 + x + 1 \equiv 0 \pmod{19^5}$$

has a solution, and, with slightly more work, that the same holds for

$$x^3 - 19 \equiv 0 \pmod{3^9}.$$

Thus P is in fact an example as required.

Remark 2. It is easy to infer from Theorem 1 that there exists no polynomial of degree less than 5 without rational roots possesing the property in question. Thus the above example is minimal in this respect.

We mention in passing that, given a polynomial P satisfying the property under consideration, we can generate out of it many polynomials having the same property. In fact, solutions of (1), m being a high power of some fixed prime p, are all taken care of by one of the factors h_i of P. But then one may replace all other $h_j(x)$ by $h_j(px)$ (or $h_j(p^l x)$ with an arbitrary l).

Example 3. In Example 2, congruences modulo powers of 2 are taken care of by the first factor $x^3 - 19$, so in the second factor we may replace x by $4x$, say. Thus the polynomial $(x^3 - 19)(16x^2 + 4x + 1)$ is a non-monic polynomial possessing the property in question.

The *density* of a set T of primes is defined by

$$d(T) = \lim_{x \to \infty} \frac{\pi(x, T)}{\pi(x)},$$

where $\pi(x)$ is the number of all primes not exceeding x and $\pi(x, T) = |T \cap [1, x]|$ is the number of such primes belonging to T, provided that the limit exists. (Of course, in view of the Prime Number Theorem, one can replace the denominator on the right-hand side by $\frac{x}{\log x}$.)

We recall that there is also a weaker notion of density, namely that of the Dirichlet density. If the density of T exists, then so does the Dirichlet density, and the two densities coincide.

Theorem 2. *Given a polynomial $P \in \mathbf{Z}[x]$, the density of the set S of primes p for which the congruence $P(x) \equiv 0 \pmod{p}$ has a solution for $m = p$ is*

$$d(S) = \frac{\left|\bigcup_{\sigma \in G} \sigma^{-1} U \sigma\right|}{|G|}.$$

Remark 3. V. Schulze [Schu1, Schu2] proved that the density in Theorem 2 exists and is a rational number, and calculated it for some concrete polynomials. See also [A], [FS] and [L] for more general but less explicit results.

Remark 4. Theorems 1.3 and 1.4 of [LO] imply the following quantitative version of our Theorem 2:

$$|\pi(x, S) - d(S)\,\mathrm{Li}x| \leq d(S)\,\mathrm{Li}x^{\beta} + c_2\,|U|\,x \exp\left(-c_3 \sqrt{\frac{\log x}{|G|}}\right), \tag{3}$$

where $d(S)$ is as in Theorem 2,

$$\beta = \max\left(1 - \frac{1}{4\log D}, 1 - \frac{1}{c_4 D^{\frac{1}{|G|}}}\right),$$

and c_2, c_3, c_4 are effective absolute constants. Under GRH, the right-hand side of (3) may be replaced by

$$c_5\left(d(S)\sqrt{x}\,\log\left(Dx^{|G|}\right) + |U|\,\log D\right), \tag{3'}$$

c_5 being an effective absolute constant. This also follows from the results of [LO]. Oesterlé [O] obtained a version of (3′) including only explicit constants.

3. An upper bound for d_L

Lemma 1. *The absolute discriminant d_L of the field L divides D, and in particular $d_L \le D$.*

Proof. Fix i and write $n = n_i$, $a_j = a_{ij}$, $\theta = \theta_i$, $K = K_i$.

Let $\theta = \theta^{(1)}, \dots, \theta^{(n)}$ be the conjugates of θ over $\mathbf{Q}$. Consider the following basis of K over $\mathbf{Q}$:

$\omega_1 = 1;$
$\omega_2 = a_n\theta;$
$\omega_3 = a_n\theta^2 + a_{n-1}\theta;$
. . . . .
$\omega_n = a_n\theta^{n-1} + a_{n-1}\theta^{n-2} + \dots + a_2\theta.$

Since $\omega_1, \dots, \omega_n$ are algebraic integers (see [Schm, p.183] for an explanation), we have $d_K | d(\omega_1, \dots, \omega_n)$. But

$$d(\omega_1, \dots, \omega_n) = |\det[\omega_{kj}]|^2 = \delta_i,$$

where ω_{kj} is obtained from ω_k upon replacing θ by $\theta^{(j)}$. Thus, $d_K | \delta_i$.

Note that we have $d_{K^{(j)}} = d_K$ for any j, where $K^{(j)} = \mathbf{Q}(\theta^{(j)})$. Hence the discriminant $d_{K'}$ of the field $K' := K'_i = \mathbf{Q}(\theta^{(1)}, \dots, \theta^{(n-1)})$ divides

$$\prod_{j=1}^{n-1} (d_{K^{(j)}})^{[K':K^{(j)}]} = (d_K)^{(n-1)[K':K]} \big| \delta_i^{(n-1)(n-1)!}$$

Finally, the field L is the composite of $K'_1, \dots, K'_\nu$, hence

$$\mathrm{d}_L \mid \prod_{i=1}^{\nu} \left(d_{K'_i}\right)^{[L:K'_i]},$$

and the last product divides

$$\prod_{i=1}^{\nu} \left(\delta_i^{(n-1)(n-1)!}\right)^{n_1! \dots n_{i-1}! n_{i+1}! \dots n_\nu!} = D,$$

which proves the lemma.

4. Proof of Theorems 1 and 2

Let K be a subfield of L, $\mathfrak{P}$ a prime ideal of L unramified over K, $\mathfrak{p}$ the prime ideal of K below $\mathfrak{P}$, and $L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$ the corresponding completions. Since there are natural embeddings

$$\mathrm{Gal}\,(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \hookrightarrow \mathrm{Gal}\,(L/K) \hookrightarrow \mathrm{Gal}\,(L/\mathbf{Q}),$$

we may suppose further that

$$\mathrm{Gal}\,(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \leq \mathrm{Gal}\,(L/K) \leq \mathrm{Gal}\,(L/\mathbf{Q}).$$

Let R_L be the ring of integers of the field L. Recall that the *Frobenius symbol* $(\frac{L/K}{\mathfrak{P}}) \in \mathrm{Gal}\,(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is defined uniquely by the property

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N\mathfrak{p}} \mod \mathfrak{P}$$

for all $\alpha \in R_L$ [Na, §7.3.1], and that *Artin's symbol*

$$\left[\frac{L/K}{\mathfrak{p}}\right] = \left\{\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} : \sigma \in \mathrm{Gal}\,(L/K)\right\}$$

is the conjugacy class of $(\frac{L/K}{\mathfrak{P}})$ in $\mathrm{Gal}\,(L/K)$.

We need the following elementary property of Frobenius symbols. Let $\mathfrak{p}$ be unramified over $\mathbf{Q}$, and let $p \in \mathbf{Z}$ be the prime below $\mathfrak{p}$. Denote $f_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbf{Q}_p]$. We claim that

$$\left(\frac{L/K}{\mathfrak{P}}\right) = \left(\frac{L/\mathbf{Q}}{\mathfrak{P}}\right)^{f_{\mathfrak{p}}} \tag{4}$$

and

$$\left(\frac{L/\mathbf{Q}}{\mathfrak{P}}\right)^{m} \in \mathrm{Gal}\,(L/K) \iff f_{\mathfrak{p}}\,|m. \tag{5}$$

In fact, (4) is well known and follows immediately from the definition. To prove (5) note that $(\frac{L/\mathbf{Q}}{\mathfrak{P}})$ generates the cyclic group $\mathrm{Gal}\,(L_{\mathfrak{P}}\,/\,\mathbf{Q}_p)$, and that

$$\begin{aligned}&[\mathrm{Gal}\,(L_{\mathfrak{P}}\,/\,\mathbf{Q}_p) : \mathrm{Gal}\,(L/K) \cap \mathrm{Gal}\,(L_{\mathfrak{P}}\,/\,\mathbf{Q}_p)]\\ &= [\mathrm{Gal}\,(L_{\mathfrak{P}}\,/\,\mathbf{Q}_p) : \mathrm{Gal}\,(L_{\mathfrak{P}}\,/\,K_{\mathfrak{p}})] = [K_{\mathfrak{p}} : \mathbf{Q}_p] = f_{\mathfrak{p}}.\end{aligned}$$

We deduce both Theorems 1 and 2 from the following statement.

Lemma 2. *Let p be a prime not dividing δ. Then*

$$\left[\frac{L/\mathbf{Q}}{p}\right] \cap U \neq \emptyset \tag{6}$$

if and only if $P(x)$ has a root in $\mathbf{Q}_p$.

We mention that according to Lemma 1 it follows in particular that p is unramified in L.

Proof. Let $pR_L = \mathfrak{P}_1 \dots \mathfrak{P}_\tau$ be the decomposition of p in L. Then

$$\left[\frac{L/\mathbf{Q}}{p}\right] \; = \; \left\{ \left(\frac{L/\mathbf{Q}}{\mathfrak{P}_1}\right), \dots, \left(\frac{L/\mathbf{Q}}{\mathfrak{P}_\tau}\right) \right\}. \tag{7}$$

Hence (6) is equivalent to the following: for some i and j

$$\left(\frac{L/\mathbf{Q}}{\mathfrak{P}_j}\right) \; \in \; H_i. \tag{8}$$

Let $\mathfrak{p}$ be the prime ideal of K_i below $\mathfrak{P}_j$. Then (5) yields that (8) is equivalent to

$$[\,(K_i)_{\mathfrak{p}} \; : \; \mathbf{Q}_p] \; = \; 1,$$

which may happen if and only if $h_i(x)$ has a root in $\mathbf{Q}_p$. This proves the lemma.

Proof of Theorem 1. (b) $\Longrightarrow$ (a): Instead of (a) we shall prove the following equivalent statement:

(a$'$) *$P(x)$ has a root in $\mathbf{Q}_p$ for every prime p.*

So, fix a prime p. If it is does not divide δ, then $P(x)$ has a root in $\mathbf{Q}_p$ by (2) and Lemma 2. Now let p divide δ. Let $\lambda \in \mathbf{Z}$ be the root of $P(x) \bmod \Delta$. Then

$$|P(\lambda)|_p \; < \; |\delta|_p^2.$$

Hence for some i

$$|h_i(\lambda)|_p \; < \; |\rho_i|_p^2.$$

On the other hand, there exist polynomials $a(x)$, $b(x) \; \in \; \mathbf{Z}[x]$ such that

$$a(x)h_i(x) \; + \; b(x)h_i'(x) = \rho_i.$$

Hence $|h_i'(\lambda)|_p \; \geq \; |\rho_i|_p$, and we get

$$|h_i(\lambda)|_p \; < \; |h_i'(\lambda)|_p^2.$$

By Hensel's lemma [CF, Ch.2, App.C] $h_i(x)$ has a root in $\mathbf{Q}_p$. Hence $P(x)$ has a root in $\mathbf{Q}_p$, which completes the proof of (b) $\Longrightarrow$ (a$'$).

(a) $\Longrightarrow$ (c): Trivial.

(c) $\Longrightarrow$ (b): We have to prove that any conjugacy class C of the group G intersects U. As proved in [LMO, Theorem 1.1], there exists an effectively computable absolute constant A with the following property. For any conjugacy class C there exists a prime $p \in \mathbf{Z}$, satisfying the following conditions:

(i) p is unramified in L;

(ii) $\left[\dfrac{L\,/\,\mathbf{Q}}{p}\right] \; = \; C$;

(iii) $p \; \leq \; 2d_L^A$.

Fix such p, and prove that there exists $\lambda \in \mathbf{Z}$ such that

$$|P(\lambda)|_p \;<\; |\delta|_p^2. \tag{9}$$

When $p|\delta$, we take λ as a root of $P(x) \bmod \Delta$. So let p not divide δ. By Lemma 1, $p \le 2D^A$, whence $P(x)$ has a root $\lambda \bmod p$, and we get (9) since $|\delta|_p = 1$.

The same argument as above shows that the polynomial $P(x)$ has a root in $\mathbf{Q}_p$. Therefore $S \cap U \neq \emptyset$ by Lemma 2. This concludes the proof.

Proof of Theorem 2. Let C be a conjugacy class of G. Denote

$$T(C) \;=\; \left\{ p \,:\, \left[\frac{L/\mathbf{Q}}{p}\right] \;=\; C \right\}.$$

Applying Chebotarev density theorem in the form given in [LO] or [Schu3], we obtain $d(T(C)) \;=\frac{|C|}{|G|}$. Now by Lemma 2

$$d(S) \;=\; \sum_{C\cap U\neq\emptyset} d(T(C)) \;=\; \sum_{C\cap U\neq\emptyset}\frac{|C|}{|G|} \;=\; \frac{\left|\bigcup_{\sigma\in G}\sigma^{-1}U\sigma\right|}{|G|}\;.$$

The proof is complete.

References

[A] J. Ax, *Solving diophantine problems modulo every prime*, Ann. Math. **85** (1967), 161–183. MR **35:**126

[Ba] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), 355–380. MR **91m:**11096

[Bo] M. Boshernitzan, *On recurrence and spread in dynamical systems*, preprint.

[BH] D. Berend and J. E. Harmse, *On polynomial-factorial and similar diophantine equations*, preprint.

[BO] D. Berend and C. F. Osgood, *On the equation $P(x) = n!$ and a question of Erdős*, J. Number Theory **42** (1992), 189–193.

[BS] Z. I. Borevich and I. R. Shafarevich, *J. Number Theory*, Academic Press, New York, 1966.

[CF] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory (Proceedings of an Instructional Conference, University of Sussex, 1965),*, Academic Press and St Edmundsbury Press, Suffolk, 1990.

[EO] P. Erdős and R. Obláth, *Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ und $n! \pm m! = x^p$*, Acta Szeged **8** (1937), 241–255.

[FS] M. Fried and G. Sacerdote,, *Solving diophantine problems over all residue class fields of an algebraic number field and all finite fields*, Ann. Math. **104** (1976), 203–233. MR **58:**10722

[Fu] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton University Press, Princeton, New Jersey, 1981. MR **82j:**28010

[Gu] R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 1981. MR **83k:**10002

[KM] T. Kamae and M. Mendes France, *Van der Corput's difference theorem*, Israel J. of Math. **31** (1978), 335–342. MR **80a:**10070

[KN] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974. MR **54:**7415

[L] J.C. Lagarias, *Sets of primes determined by systems of polynomial congruences*, Illinois J. of Math. **24** (1983), 224–239. MR **85f:**11081

[LMO] J.C. Lagarias, H.L. Montgomery and A.M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), 271–296. MR **81b:**12013

[LO] J.C. Lagarias and A.M. Odlyzko, *Effective Versions of the Chebotarev density theorem*, Algebraic Number Fields, (Proceedings of a Symposium held at University of Durham, 1975) (A. Fröhlich, ed.), Academic Press, London, 1977, pp. 409–464. MR **56:**5506

[N] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer-Verlag, and PWN–Polish Scientific Publishers, Warsaw, 1990. MR **91h:**11107

[O] J. Osterlé,, *Versions effectives du théorème de Chebotarev sous l'hypothése de Riemann généralisé,*, Soc. Math. France Astérisque **61** (1979), 165–167.

[Sá1] A. Sárközy, *On difference sets of sequences of integers,* I, Acta Math. Acad. Sci. Hung. **31** (1978), 125–149. MR **57:**5942

[Sá2] ———, *On difference sets of sequences of integers,* II, Ann. Univ. Sci. Budapest Eötvös Sect. Math. **21** (1978), 45–53. MR **80j:**10062a

[Sá3] ———, *On difference sets of sequences of integers,* III, Acta Math. Acad. Sci. Hung. **31** (1978), 355-386. MR **80j:**10062b

[Schm] W. Schmidt, *Construction and Estimates of Bases in Function Fields*, J. Number Theory **39** (1991), 181–224. MR **93b:**11079

[Schu1] V. Schulze, *Die Primteilerdichte von ganzzahligen Polynomen,* I, J. Reine Angew. Math. **253**, 175–185. MR **45:**8640

[Schu2] ———, *Die Primteilerdichte von ganzzahligen Polynomen,* II, J. Reine Angew. Math. **256** (1972), 153–162. MR **47:**178

[Schu3] ———, *Die Primteilerdichte von ganzzahligen Polynomen,* III, J. Reine Angew. Math. **273** (1975), 144–145. MR **51:**5559

[vW] B.L. van der Waerden, *Algebra* I, Springer, 1971.

Department of Mathematics and Computer Science, Ben-Gurion University, Beer Sheva 84105, Israel

E-mail address: berend@black.bgu.ac.il

Department of Mathematics and Computer Science, Ben-Gurion University, Beer Sheva 84105, Israel and Université Bordeaux 2, Mathématiques Stochastiques, BP26, F-33076 Bordeaux Cedex, France

Current address: Max Planck Institute for Mathematics, Gottfried Claren Str. 26, 53225 Bonn, Germany

E-mail address: yuri@cfgauss.uni-math.gwdg.de