Conspectus materiae tomi XLIV, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	**Адрес редакции и книгообмена**

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-05691-6 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

A notion of density and essential components in GF$[p, x]$*

by

JOHN R. BURKE (Pullman, Wash.)

Introduction. In the early 1930's, L. G. Schnirelmann [2], [4] introduced a notion of density for subsets of $L_0 = \{0, 1, 2, \ldots\}$. If $A \subset L_0$, let $A(n) = |A \cap [1, n]|$. The Schnirelmann density of A is then defined to be $\sigma(A) = \inf_{n \geq 1} A(n)/n$. He was able to establish the following results:

THEOREM 1 (Schnirelmann). *If* $0 \in A \cap B$ *and* $\sigma(A)+\sigma(B) \geq 1$ *then* $A+B = L_0$.

THEOREM 2 (Schnirelmann). *If* $1 \in A$ *and* $0 \in B$ *then*

$$\sigma(A+B) \geq \sigma(A)+\sigma(B)-\sigma(A)\sigma(B).$$

It was Theorem 2 which led to the α-β conjecture, established by H. B. Mann [3] in 1944 and rightfully goes by Mann's Theorem today. In particular, if $0 < \sigma(A)$, $\sigma(B) < 1$ (the only situation for which Theorem 2 yields nontrivial results) and $0 \in B$ then $\sigma(A+B) > \sigma(A)$. A set B having the property that $\sigma(A+B) > \sigma(A)$ for every set A satisfying $0 < \sigma(A) < 1$, is called an essential component. Thus Theorem 2 states that if $0 \in B$ and $0 < \sigma(B)$, then B is an essential component.

Let p be a prime and let GF(p) be the Galois field of order p. Denote the polynomial ring over GF(p) by GF$[p, x]$. It is the intention in what follows to establish a density for GF$[p, x]$ similar to that of Schnirelmann's density for L_0. It will be shown that no analogue of Theorem 2 can exist yet there are some interesting essential components. We begin by establishing a density.

If $\mathscr{A} \subset$ GF$[p, x]$, let $\mathscr{A}(n) = \sum_{\substack{0 \leq \deg(a(x)) \leq n \\ a(x) \in \mathscr{A}}} 1$ where it is understood that $\deg(0) = -\infty$.

DEFINITION 1. The *density of a set* $\mathscr{A} \subset$ GF$[p, x]$ is given by

$$\tau(\mathscr{A}) = \inf_{n \geq 0} \frac{\mathscr{A}(n)}{p^{n+1}-1}.$$

* This is part of the author's Doctoral Dissertation and he would like to express his appreciation to his advisor, Prof. William Webb, for the guidance he has received.

It may be noted that the τ-density is somewhat weaker than that of Schnirelmann's, that is, the "intervals" over which the infimum is taken are coarser since they do not take into account the effect of adjoining or deleting each element, one at a time. One may, however, establish the following:

THEOREM 3. *If* $0\in\mathscr{A}\cap\mathscr{B}$ *and* $\tau(\mathscr{A})+\tau(\mathscr{B})\geqslant 1$, *then* $\mathscr{A}+\mathscr{B}=\mathrm{GF}[p,x]$.

Proof. It shall be shown, equivalently, that if $0\in\mathscr{A}\cap\mathscr{B}$ and $\mathscr{A}+\mathscr{B}\neq\mathrm{GF}[p,x]$, then $\tau(\mathscr{A})+\tau(\mathscr{B})<1$. Assume $\mathscr{A}+\mathscr{B}\neq\mathrm{GF}[p,x]$. Let $f(x)$ be a polynomial of least degree which is not in $\mathscr{A}+\mathscr{B}$, and let $\deg(f(x))=n$. Now, since $0\in\mathscr{A}$ and $f(x)\notin\mathscr{A}$, there must be at least $\tau(\mathscr{A})(p^{n+1}-1)+1$ nonzero polynomials, of degree less than or equal to n, of the form $f(x)-a(x)$, $a(x)\in\mathscr{A}$. There are also at least $\tau(\mathscr{B})(p^{n+1}-1)$ nonzero polynomials of degree n or less in $\mathscr{B}$. Since there are only $p^{n+1}-1$ nonzero polynomials of degree n or less, we have

$$(p^{n+1}-1)\geqslant\big(\tau(\mathscr{A})+\tau(\mathscr{B})\big)(p^{n+1}-1)+1.$$

Thus $\tau(\mathscr{A})+\tau(\mathscr{B})<1$ as claimed.

Thus it appears that the τ-density is a reasonable analogue of Schnirelmann's density. Before proceeding, we make precise the notion of essential component.

DEFINITION 2. A set $\mathscr{B}\subset\mathrm{GF}[p,x]$ is an *essential component* if $\tau(\mathscr{A}+\mathscr{B})>\tau(\mathscr{A})$ for any set $\mathscr{A}$ satisfying $0<\tau(\mathscr{A})<1$.

If the τ-density is an exact analogue to Schnirelmann's density, we should be able to obtain a result similar to Theorem 2. In particular, a set with positive density should be an essential component.

Let $p=2$ and consider $\mathscr{A}\subset\mathrm{GF}[p,x]$ such that $f(x)\in\mathscr{A}$ if and only if $f(x)$ has no linear term. Then $0\in\mathscr{A}$ and $0<\tau(\mathscr{A})=1/3<1$. But $\mathscr{A}$ is also a subgroup of $\mathrm{GF}[p,x]$ under addition hence $\mathscr{A}+\mathscr{A}=\mathscr{A}$ and consequently $\tau(\mathscr{A}+\mathscr{A})=\tau(\mathscr{A})$. Reflecting on this it is clear that any density allowing a subgroup to have positive density will not allow a theorem of the type of Theorem 2. Thus if we are to establish the existence of essential components, we must put some restrictions on our sets. In particular our restriction must eliminate subgroups.

DEFINITION 3. A set $\mathscr{B}\subset\mathrm{GF}[p,x]$ is a *basis of order* h if for any $f(x)\in\mathrm{GF}[p,x]$,

$$f(x)=\sum_{i=1}^{k}b_i(x),\quad k\leqslant h,\ b_i(x)\in\mathscr{B},\qquad \deg(b_i(x))\leqslant\deg(f(x)),\qquad 1\leqslant i\leqslant k.$$

Using the concept of a basis we can establish the following result. It is analogous to a result of Erdös [1] in 1936. It is interesting to note that in the integers, the theorem of Erdös yields only half as much growth as obtained in Theorem 4 although the Schnirelmann density appears to be much stronger than the τ-density, yielding results such as Theorem 2.

THEOREM 4. *Let* $\mathscr{A}$, $\mathscr{B}\subset\mathrm{GF}[p,x]$ *and assume* $\mathscr{B}$ *is a basis of order* h. *Then*

$$\tau(\mathscr{A}+\mathscr{B})\geqslant\tau(\mathscr{A})+\frac{1}{h}\tau(\mathscr{A})\big(1-\tau(\mathscr{A})\big).$$

Proof. Let $\bar{D}_n(f)$ denote the number of polynomials $a(x)\in\mathscr{A}$ such that $a(x)+f(x)\notin\mathscr{A}$, $\deg(a(x))\leqslant n$, and $\deg(f(x))\leqslant n$. Thus for any $b(x)\in\mathscr{B}$ it follows that

$$\bar{D}_n(b)\leqslant(\mathscr{A}+\mathscr{B})(n)-\mathscr{A}(n).$$

Next let

$$\bar{D}_n^*=\frac{1}{p^{n+1}-1}\sum_{0\leqslant\deg(f(x))\leqslant n}\bar{D}_n(f).$$

It is easily seen for $f(x)$, $f'(x)$ satisfying $\deg(f(x))$, $\deg(f'(x))\leqslant n$, that

$$\bar{D}_n(f+f')\leqslant\bar{D}_n(f)+\bar{D}_n(f').$$

As a consequence we have for any $f(x)$, $\deg(f(x))\leqslant n$,

$$\bar{D}_n(f)=\bar{D}_n\Big(\sum_{i=1}^{k}b_i\Big)\leqslant\sum\bar{D}_n(b_i)\leqslant h\big((\mathscr{A}+\mathscr{B})(n)-\mathscr{A}(n)\big)$$

so

$$\bar{D}_n^*=\frac{1}{p^{n+1}-1}\sum_{0\leqslant\deg(f(x))\leqslant n}\bar{D}_n(f)\leqslant\frac{1}{p^{n+1}-1}\sum_{0\leqslant\deg(f(x))\leqslant n}h\big((\mathscr{A}+\mathscr{B})(n)-\mathscr{A}(n)\big)$$
$$=h\big((\mathscr{A}+\mathscr{B})(n)-\mathscr{A}(n)\big).$$

Next, denote by $D_n(f)$ those elements $a(x)\in\mathscr{A}$ such that $a(x)+f(x)\in\mathscr{A}$, $\deg(a(x))\leqslant n$, and $\deg(f(x))\leqslant n$. Then for any $f(x)\in\mathrm{GF}[p,x]$, $\deg(f(x))\leqslant n$, we have $\bar{D}_n(f)+D_n(f)=\mathscr{A}(n)\geqslant\tau(\mathscr{A})(p^{n+1}-1)$ so that

$$(p^{n+1}-1)\bar{D}_n^*=\sum_{0\leqslant\deg(f(x))\leqslant n}\bar{D}_n(f)\geqslant\sum_{0\leqslant\deg(f(x))\leqslant n}\tau(\mathscr{A})(p^{n+1}-1)-\sum_{0\leqslant\deg(f(x))\leqslant n}D_n(f)$$
$$=\tau(\mathscr{A})(p^{n+1}-1)^2-\sum_{0\leqslant\deg(f(x))\leqslant n}D_n(f).$$

To bound $\sum_{0\leqslant\deg(f(x))\leqslant n}D_n(f)$ from above, note that it is equal to the number solutions to $a_i(x)+f(x)=a_j(x)$, which is the number of differences $a_i(x)-a_j(x)$, $i\neq j$. This in turn is not as large as $\mathscr{A}(n)^2$. Thus we have

$$(p^{n+1}-1)\bar{D}_n^*\geqslant\tau(\mathscr{A})(p^{n+1}-1)^2-\mathscr{A}(n)^2.$$

Putting the upper and lower bounds for $\bar{D}_n^*$ together yields

$$\frac{(\mathscr{A}+\mathscr{B})(n)}{p^{n+1}-1} \geqslant \frac{\mathscr{A}(n)}{p^{n+1}-1} + \frac{1}{h}\tau(\mathscr{A}) - \frac{\mathscr{A}(n)^2}{h(p^{n+1}-1)^2}.$$

It remains to show that $\dfrac{\mathscr{A}(n)}{p^{n+1}-1}$ may be replaced by $\tau(\mathscr{A})$. This follows immediately upon noting that $f(x) = x - x^2/h$, $h \geqslant 2$ is increasing on $[0, 1]$.

Now taking the infimum over all $n \geqslant 0$ gives the desired result.

Theorem 4 states that any basis is an essential component. Upon reviewing the proof, it appears that the condition of bounding the degrees of the summands in a basis may be needed because of the proof technique rather than having anything to do with an intrinsic fact of the problem. With this in mind we have

DEFINITION 4. A set $\mathscr{B} \subset \mathrm{GF}[p, x]$ is a *weak basis of order* h if for any $f(x) \in \mathrm{GF}[p, x]$

$$f(x) = \sum_{i=1}^{k} b_i(x), \qquad k \leqslant h,\ b_i(x) \in \mathscr{B}.$$

Let $p = 5$ and consider the following sets in $\mathrm{GF}[5, x]$.

$$\mathscr{A} = \{f(x)\colon \deg(f(x)) \geqslant 1, \text{ leading coef. is } 1 \text{ or } 3\} \cup \{1\},$$

$$\mathscr{B} = \{f(x)\colon \deg(f(x)) \geqslant 1; \text{ leading coef. is } 1 \text{ or } 3\} \cup \{0\}.$$

It is easily verified that $0 < \tau(\mathscr{A}) = 1/4 < 1$, $\mathscr{B}$ is a weak basis of order 3, and that $\tau(\mathscr{A}+\mathscr{B}) = \tau(\mathscr{A})$. There are, therefore, weak bases which are not essential components.

It should be observed that although every basis is an essential component, it gives the impression that the higher the order of the basis the less effect it has on the growth of the density of the sum set. In other words, the higher the order of the basis, the less it is an essential component. The remainder of this investigation will be devoted to the construction of a basis $\mathscr{B}$ of order h, for any $h \geqslant 2$, that will yield the best possible growth indicated by Theorem 4. That is

$$\tau(\mathscr{A}+\mathscr{B}) \geqslant \tau(\mathscr{A}) + \tfrac{1}{2}\tau(\mathscr{A})(1-\tau(\mathscr{A})).$$

The construction will parallel that given by Stöhr [5].

THEOREM 5. *Let h and k be positive integers with $h \geqslant 2$. There exists bases $\mathscr{B}_0, \ldots, \mathscr{B}_{k-1}$, each of order h such that*

(i) $\mathscr{L} = \sum_{i=0}^{k-1} \mathscr{B}_i$ *is a basis of order* h,

(ii) $\tau((h-1)\mathscr{L}) = 0$ *where* $(h-1)\mathscr{L} = \sum_{i=1}^{h-1} \mathscr{L}_i$.

Before beginning the proof, some notation is required. Let $g(x) \in \mathrm{GF}[p, x]$, $\deg(g(x)) \geqslant 1$ and let $J \subset \boldsymbol{L}_0$. Define the operator $\mathscr{G}_g$ by

$$\mathscr{G}_g(J) = \{\textstyle\sum_{\nu \in J}' a_\nu(x) g^\nu(x);\ \deg(a_\nu(x)) < \deg(g(x))\}$$

where $\sum'$ ranges over all finite sums with $\nu \in J$. The two properties of $\mathscr{G}_g$ to be utilized are

(i) $\mathscr{G}_g(\boldsymbol{L}_0) = \mathrm{GF}[p, x]$,

(ii) $\mathscr{G}_g(J \cup H) = \mathscr{G}_g(J) + \mathscr{G}_g(H)$ if $J \cap H = \emptyset$.

LEMMA 1. *If $\boldsymbol{L}_0$ is partitioned into h mutually disjoint sets $J^0, J^1, \ldots, J^{h-1}$, then*

$$\mathscr{B} = \bigcup_{i=0}^{h-1} \mathscr{G}_g(J^i) \text{ is a basis of order } h.$$

Proof. First note that $\mathrm{GF}[p, x] = \mathscr{G}_g(\boldsymbol{L}_0) = \mathscr{G}_g(\bigcup_{i=0}^{h-1} J^i) = \sum_{i=0}^{h-1} \mathscr{G}_g(J^i) \subset h\mathscr{B}$. Clearly any element $f(x) \in h\mathscr{B}$ can be written as a sum in which the summands have degree less than or equal to $\deg(f(x))$. Thus $\mathscr{B}$ is a basis of order at most h.

Let a_i be the least element in J^i and consider $f(x) = \sum_{i=0}^{h-1} g^{a_i}(x)$. Then $f(x) \notin (h-1)\mathscr{B}$ so the order of $\mathscr{B}$ is at least h.

For a basis as constructed in Lemma 1, let $\mathscr{J}^{(m)} = \bigcup_{\substack{i=0 \\ i \neq m}}^{h-1} \mathscr{G}_g(J^i)$.

$\mathscr{J}^{(m)}$ contains no polynomials whose $g(x)$-adic expansions have a power of $g(x)$ in J^m (there are more polynomials deleted, but for our purpose, these are the ones of interest).

LEMMA 2. *If $\mathscr{B}$ is a basis constructed by Lemma 1 and $\mathscr{J}^{(m)} = \bigcup_{\substack{i=0 \\ i \neq m}}^{h-1} \mathscr{G}_g(J^i)$ then*

$$(h-1)\mathscr{B} = \bigcup_{m=0}^{h-1} (h-1)\mathscr{J}^{(m)}.$$

Proof. Let $f(x) \in (h-1)\mathscr{B}$, then $f(x) = \sum_{i=0}^{h-2} b_i(x)$ where $b_i(x) \in \mathscr{G}_g(J^{m_i})$ for each i. Since there are at most $h-1$ distinct sets J^{m_i} involved, all of the $b_i(x)$ lie in some $\mathscr{J}^{(m)}$. Therefore $f(x) \in (h-1)\mathscr{J}^{(m)}$ for some m so that

$$(h-1)\mathscr{B} \subset \bigcup_{m=0}^{h-1} (h-1)\mathscr{J}^{(m)}.$$

Conversely, $\mathscr{J}^{(m)} \subset \mathscr{B}$ for each m so that $(h-1)\mathscr{J}^{(m)} \subset (h-1)\mathscr{B}$ for each m. Thus

$$\bigcup_{m=0}^{h-1} (h-1)\mathscr{J}^{(m)} \subset (h-1)\mathscr{B}.$$

For fixed integers $k \geqslant 1$ and $h \geqslant 2$, consider k different partitions of $\boldsymbol{L}_0$, each partition containing h equivalence classes. Denote them by $\{J_i^l\}_{l=0}^{h-1}$, $0 \leqslant i \leqslant k-1$. By Lemma 1 we can construct k bases,

$$\mathscr{B}_i = \bigcup_{l=0}^{h-1} \mathscr{G}_{il}(J_i^l), \qquad 0 \leqslant i \leqslant k-1.$$

Let $\mathscr{L} = \sum_{i=0}^{k-1} \mathscr{B}_i$. Then

$$(h-1)\mathscr{L} = (h-1)\Big(\sum_{i=0}^{k-1} \mathscr{B}_i\Big) = \sum_{i=0}^{k-1} (h-1)\mathscr{B}_i = \sum_{i=0}^{k-1} \bigcup_{m=0}^{h-1} (h-1)\mathscr{J}_i^{(m)}.$$

If $f(x) \in (h-1)\mathscr{L}$, then $f(x) = \sum_{i=0}^{k-1} b_i(x)$ where $b_i(x) \in \bigcup_{m=0}^{h-1} (h-1)\mathscr{J}_i^{(m)}$ so that $b_i(x) \in (h-1)\mathscr{J}_i^{(m)}$ for some m. Thus

$$(h-1)\mathscr{L} = \bigcup_{m_0=0}^{h-1} \bigcup_{m_1=0}^{h-1} \cdots \bigcup_{m_{k-1}=0}^{h-1} \sum_{i=0}^{k-1} (h-1)\mathscr{J}_i^{(m_i)}.$$

Fix a k-tuple $(m_0, \ldots, m_{k-1})$ and define $\mathscr{C} = \sum_{i=0}^{k-1} (h-1)\mathscr{J}_i^{(m_i)}$.

If there is a sequence $A \subset \bigcap_{i=0}^{k-1} J_i^{m_i}$, then for $a \in A$, $(g(x))^a$ does not appear in the $g(x)$-adic expansion of any element of $(h-1)\mathscr{J}_i^{(m_i)}$ so no term in $\mathscr{C}$ would have $(g(x))^a$ in its $g(x)$-adic expansion.

LEMMA 3. *Let h, k be positive integers with $h \geqslant 2$, then there exist k subdivisions of the set $\{0, 1, \ldots, h^k-1\}$ into h mutually disjoint sets $\{J_i^l\}_{l=0}^{h-1}$ such that for any k-tuple $(m_0, \ldots, m_{k-1})$, $0 \leqslant m_l \leqslant h-1$*

$$\bigcap_{i=0}^{h-1} J_l^{m_l} \neq \emptyset.$$

Proof. Let $J_l^l = \{m: 0 \leqslant m \leqslant h^k-1, m = \sum_{i=0}^{k-1} j_i h^i \text{ and } j_l = l\}$.

In applying Lemma 3, let J_i^l be the corresponding nonnegative residues mod(h^k). Thus the asymptotic density of $\bigcap_{i=0}^{h-1} J_i^{m_i}$ is $1/h^k > 0$.

Returning to the set $\mathscr{C}$, there are no polynomials in $\mathscr{C}$ whose $g(x)$-adic expansion contains any power of $g(x)$ which lie in some residue class mod(h^k). Thus

$$\tau(\mathscr{C}) \leqslant \lim_{n\to\infty} \frac{P^{n(h^k-1)}-1}{P^{nh^k}-1} = 0.$$

Each of the h^k k-tuples gives rise to a set of the form of $\mathscr{C}$ above. Thus

$$\tau((h-1)\mathscr{L}) \leqslant \lim_{n\to\infty} h^k \frac{P^{n(h^k-1)}-1}{P^{nh^k}-1} = 0.$$

This concludes the proof of Theorem 5. We are now ready for the main theorem.

THEOREM 6. *Given $h \geqslant 2$, there exists a basis $\mathscr{L}$ of order h such that*

(i) $\tau((h-1)\mathscr{L}) = 0$,

(ii) $\tau(\mathscr{A}+\mathscr{L}) \geqslant \tau(A) + \frac{1}{2}\tau(\mathscr{A})(1-\tau(\mathscr{A}))$.

Proof. Let $\varphi(\alpha) = \alpha + \frac{1}{h}(1-\alpha)\alpha$. If $\mathscr{A}$ is a sequence satisfying $\tau(\mathscr{A}) \geqslant \alpha > 0$ and $\mathscr{B}$ is a basis of order h then Theorem 4 implies $\tau(\mathscr{A}+\mathscr{B}) \geqslant \varphi(\alpha)$. Define $\varphi^{(0)}(\alpha) = \alpha$ and $\varphi^{(i+1)}(\alpha) = \varphi(\varphi^{(i)}(\alpha))$ for $i \geqslant 1$. If $\mathscr{L} = \sum_{i=0}^{k-1} \mathscr{B}_i$ is the basis in Theorem 5, then

$$\tau(\mathscr{A}+\mathscr{L}) = \tau(\mathscr{A}+\mathscr{B}_0+\mathscr{B}_1+\ldots+\mathscr{B}_{k-1}) \geqslant \varphi^{(k)}(\alpha).$$

To prove the theorem it suffices to show there exists $k = k(h)$ such that $\varphi^{(k)}(\alpha) \geqslant \alpha + \frac{1}{2}\alpha(1-\alpha)$. We shall show $k = h$ is a sufficient choice for k.

$$\varphi^{(h)}(\alpha) = \varphi^{(0)}(\alpha) + \sum_{i=0}^{h-1} (\varphi^{(i+1)}(\alpha) - \varphi^{(i)}(\alpha))$$

$$= \varphi^{(0)}(\alpha) + \frac{1}{h} \sum_{i=0}^{h-1} \varphi^{(i)}(\alpha)(1-\varphi^{(i)}(\alpha)).$$

If $\varphi^{(i)}(\alpha)(1-\varphi^{(i)}(\alpha)) > \frac{1}{2}\alpha(1-\alpha)$ for any i, $0 < i < h$ we are done since $\{\varphi^{(i)}(\alpha)\}_{i=0}^{\infty}$ is an increasing sequence bounded above by 1. Assume there is an i', $0 < i' < h$ such that $\varphi^{(i')}(\alpha) \leqslant \frac{1}{2}\alpha(1-\alpha)$. Then

$$\tfrac{1}{2}\alpha(1-\alpha) \leqslant \alpha(1-\alpha) - \varphi^{(i')}(\alpha)(1-\varphi^{(i')}(\alpha))$$

$$= (\varphi^{(i')}(\alpha) - \alpha)|\varphi^{(i')}(\alpha) + \alpha - 1|$$

$$\leqslant \varphi^{(i')}(\alpha) - \alpha \leqslant \varphi^{(h)}(\alpha) - \alpha.$$

Thus $\alpha + \frac{1}{2}\alpha(1-\alpha) \leqslant \varphi^{(h)}(\alpha)$ as claimed.

References

[1] P. Erdős, *On the arithmetical density of the sum of two sequences one of which forms a basis for the integers*, Acta Arith. 1 (1936), pp. 197–200.
[2] H. Halberstam and K. F. Roth, *Sequences*, Clarendon Press, Oxford 1966.
[3] H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. Math. (2) 43 (1942), pp. 523–527.
[4] L. G. Schnirelmann, *Über additive Eigenschaften von Zahlen*, Math. Ann. 107 (1933), pp. 649–690.
[5] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe*, J. Reine Angew Math. 194 (1955), pp. 111–140.

WASHINGTON STATE UNIVERSITY

Received on 15.4.1982
and in revised form on 4.3.1983 (1302)

ACTA ARITHMETICA
XLIV (1984)

Sommes de carrés de polynômes irréductibles dans $F_q[X]$

par

MIREILLE CAR (Marseille)

I. Introduction. Soit F_q le corps fini à q éléments, q étant un entier impair, et $F_q[X]$ l'anneau des polynômes à une variable sur le corps F_q. Certaines analogies entre les propriétés arithmétiques de l'anneau $F_q[X]$ et l'anneau Z des entiers relatifs ont été mises en évidence. En particulier, en ce qui concerne l'arithmétique additive les problèmes de Waring ([13]) et de Goldbach ([10]) ont été étudiés, et plus particulièrement, le problème de Waring pour les carrés ([3]–[9]). Il est démontré dans [7] que tout polynômes de $F_q[X]$ est somme de trois carrés sans que l'on ait une limitation des degrés des polynômes intervenant dans cette somme. Ceci conduit à introduire la définition suivante:

Si M est un polynôme de $F_q[X]$ de degré $2n$ ou $2n-1$, toute solution $(M_1, \ldots, M_k)$ de l'équation

$$M = M_1^2 + \ldots + M_k^2 \tag{E}$$

en polynômes $M_1, \ldots, M_k$ de degré au plus égal à n, est appelée *représentation restreinte de M en sommes de k carrés*. On a une estimation asymptotique du nombre $R_k(M)$ de ces représentations restreintes (cf. [1]), qui montre que, pour $k \geqslant 4$, tout polynôme de $F_q[X]$ de degré assez élevé admet une représentation restreinte en somme de k carrés, et que, pour $q \geqslant 53$, tout polynôme de $F_q[X]$ de degré assez élevé admet une représentation restreinte en somme de trois carrés. On peut aussi démontrer que pour $q \neq 3$, tout polynôme de $F_q[X]$ admet une représentation restreinte en somme de trois carrés, et que tout polynôme de $F_3[X]$ de degré différent de 3, admet une représentation restreinte en somme de trois carrés, [12].

On s'intéresse ici aux solutions $(P_1, \ldots, P_k)$ de l'équation (E) en polynômes irréductibles $P_1, \ldots, P_k$ satisfaisant aux mêmes conditions de degré, et au nombre $I_k(M)$ de représentations restreintes du polynôme M en somme de k carrés de polynômes irréductibles. On obtient, pour $k \geqslant 5$, une estimation asymptotique des nombres $I_k(M)$ qui montre que, pour $q \neq 3$, tout polynôme de $F_q[X]$ de degré assez élevé admet une représentation restreinte en somme de k carré de polynômes irréductibles, et que, pour