Journal of Number Theory **77**, 200–208 (1999)
Article ID jnth.1999.2378, available online at http://www.idealibrary.com on IDEAL®

Notes on a Problem of H. Cohn

András Biró

Mathematical Institute of the Hungarian Academy of Sciences, Reáltanoda u. 13-15, 1053 Budapest, Hungary
E-mail: biroand@math-inst.hu

Communicated by Alan C. Woods

Received April 14, 1998

We prove some partial results concerning the following problem: *Assume that F is a finite field, a_i is a complex number for each $i \in F$ such that $a_0 = 0$, $a_1 = 1$, $|a_i| = 1$ for all $i \in F \setminus \{0\}$, and $\sum_{i \in F} a_{i+j}\bar{a}_i = -1$ for all $i \in F \setminus \{0\}$. Does it follow that the function $i \to a_i$ is a multiplicative character of F?* We prove (in the case $|F| = p$, p is a prime) on the one hand that there is only a finite number of complex solutions; on the other hand we solve completely a mod p version of the problem. The proofs are mainly elementary, except for applying a theorem of Chevalley from algebraic geometry.

1. INTRODUCTION

The problem mentioned in the abstract was posed by Harvey Cohn. This is Problem 39 in the book of Montgomery ([M, p. 202]; note that there is a misprint there). It is easy to see that characters satisfy these conditions indeed.

Consider the following modified problem.

Assume that F is a finite field, a_i is a complex number for each $i \in F$ such that $a_0 = 0$, $a_1 = 1$, $a_i \neq 0$ for all $i \in F \setminus \{0\}$, and for every $j \in F \setminus \{0\}$ we have

$$\sum_{i \in F \setminus \{0\}} \frac{a_{i+j}}{a_i} = -1.$$

Does it follow that the function $i \to a_i$ is a multiplicative character of F?

These modified conditions are equivalent with the old ones if $|a_i| = 1$ for all $i \in F \setminus \{0\}$. So if the new conditions imply that $i \to a_i$ is a character, then the answer to the question of Cohn is affirmative. However, it may happen that there are numbers a_i satisfying the new conditions, but $|a_i| \neq 1$ for some $i = F \setminus \{0,1\}$.

0022-314X/99 $30.00

In this paper we consider this modified problem, but only in the case when $F = F_p$ for some prime p, where F_p is the field with $|F_p| = p$. (This is because our key lemma, Lemma 2 (similarly to Lemma 1) does not work in the prime power case.) We cannot find all the solutions, but we prove that the modified problem has only finitely many solutions (this implies of course that Cohn's problem also has only finitely many solutions). On the other hand, in characteristic p (instead of the complex, i.e., characteristic 0 case) we solve completely the modified problem, and the solutions in this case are indeed the "characters," i.e., the multiplicative functions on F_p with values in F_p.

More precisely, we prove the following two theorems.

THEOREM 1. *Let p be a prime, let F_p be the field with $|F_p| = p$. There is only a finite number of p-tulpes $(a_i : i \in F_p)$ of complex numbers such that $a_0 = 0$, $a_1 = 1$, $a_i \neq 0$ for $i \neq 0$, and*

$$\sum_{i \in F_p \setminus \{0\}} \frac{a_{i+j}}{a_i} = -1$$

for every $j \in F_p \setminus \{0\}$.

THEOREM 2. *Let p be a prime, let F_p be the field with $|F_p| = p$, and $F \supseteq F_p$ any field of characteristic p. Assume that there is given an $a_i \in F$ for every $i \in F_p$ such that $a_0 = 0$, $a_1 = 1$, $a_i \neq 0$ for $i \neq 0$, and*

$$\sum_{i \in F_p \setminus \{0\}} \frac{a_{i+j}}{a_i} = 1$$

for every $j \in F_p \setminus \{0\}$. Then $a_i = i^A$ for every $i \in F_p$ with some $1 \leqslant A \leqslant p-2$.

We mention the following easy consequence of Theorem 2.

COROLLARY. *Assume that the complex numbers $(a_i : i \in F_p)$ satisfy the conditions of Theorem* 1, and $a_i = \pm 1$ *for every $i \neq 0$. Then we have $a_i = (i/p)$ (Legendre symbol) for every $i \in F_p$.*

To prove this reduce the integers $a_i \bmod p$, then Theorem 2 gives $a_i \equiv (i/p) \pmod p$, and this implies the Corollary.

In Section 2 we prove some lemmas needed for both theorems. Then first we prove Theorem 2 (because its proof is shorter) and finally we prove Theorem 1. The proof of Theorem 2 is completely elementary, while the proof of Theorem 1 uses some algebraic geometry. Note that the proof of Theorem 1 in Section 4 gives the additional information that if $(a_i : i \in F_p)$ is a solution then every a_i $(i \neq 0)$ is an algebraic number relatively prime to p.

2. SOME LEMMAS

Let p be a prime, F_p the field with $|F_p| = p$, and $F \supseteq F_p$ an arbitrary field. Let V be the set of the F-valued functions on F_p, this is a p-dimensional vector space over F. A basis of V is given by the functions f_A (here $A = (0, 1, ..., p-1)$ with the definition

$$f_A(i) = i^A \qquad \text{for every} \quad i \in F_p.$$

(We put $i^0 = 1$ for every $i \in F_p$, i.e., f_0 is identically 1.) This is a basis indeed, since a not identically 0 polynomial over F of degree at most $p-1$ can not have p distinct roots. Let the linear transformation T on V be given by

$$(Tf)(i) = f(i+1) \qquad \text{for} \quad f \in V, \qquad i \in F_p.$$

Define the subspaces V_B of V for $B = 0, 1, ..., p$ by

$$V_B = \langle f_A : 0 \leqslant A < B \rangle.$$

So $V_0 = \{0\}$, $V_p = V$, $V_0 < V_1 < \cdots < V_p$, and the dimension of V_B is B.

LEMMA 1. *If* $1 < B \leqslant p$, $f \in V_B \setminus V_{B-1}$, *then* $Tf - f \in V_{B-1} \setminus V_{B-2}$.

Proof. This is clear, since

$$f(i) = c_{B-1} i^{B+1} + \sum_{0 \leqslant A < B-1} c_A i^A$$

for $i \in F_p$ with $c_0, c_1, ..., c_{B-1} \in F$, $c_{B-1} \neq 0$. Then we have

$$(Tf - f)(i) = f(i+1) - f(i) = c_{B-1}(B-1) i^{B-2} + \cdots,$$

and $0 < B - 1 < p$.

LEMMA 2. *If* W *is a* T*-invariant subspace of* V, *then* $W = V_B$ *for some* $0 \leqslant B \leqslant p$.

Proof. Let $0 \leqslant B \leqslant p$ be the least integer such that $W \subseteq V_B$. If $B = 0$, then $W = V_0$ and we are done. If $B > 0$, then $W \cap (V_B \setminus V_{B-1}) \neq \varnothing$. Since W is T-invariant, we can apply repeatedly Lemma 1 getting $g_0, g_1, ..., g_{B-1} \in W$ such that $g_{B-1} \in V_B \setminus V_{B-1}$, $g_{B-2} \in V_{B-1} \setminus V_{B-2}$, ..., $g_0 \in V_1 \setminus V_0$, and these vectors generate V_B, so $W = V_B$.

We introduce an "inner product" on V. Let

$$(f, g) = \sum_{i \in F_p} f(i)\, g(i).$$

This is a bilinear form on $V \times V$ with values in F. If W is a subspace of V, set

$$W^{\perp} = \{f \in V : (f, g) = 0 \text{ for } g \in W\}.$$

LEMMA 3. *If $0 \leqslant B \leqslant p$, then $V_B^{\perp} = V_{p-B}$.*

Proof. Clearly $V_B^{\perp}$ is T-invariant and then it follows from Lemma 2 and the easily proved fact that if the dimension of $W \leqslant V$ is B, then $W^{\perp}$ is a $(p-B)$-dimensional subspace.

3. PROOF OF THEOREM 2

With the notations of Section 2 our Theorem 2 reads as follows (taking $f(i) = a_i$).

LEMMA 4. *Let $f \in V$ be such that $f(0) = 0$, $f(1) \neq 1$, and $f(i) \neq 0$ for $i \in F_p \setminus \{0\}$. Let $g \in V$ be defined by $g(0) = 0$ and $g(i) = 1/f(i)$ for $i \in F_p \setminus \{0\}$. Assume that for every $j \in F_p$ we have*

$$\sum_{i \in F_p} f(i+j)\, g(i) = -1.$$

Then $f = f_A$ with some $1 \leqslant A \leqslant p-2$.

Remark. Observe that the condition for $j = 0$ is automatically satisfied, for $p - 1 = -1$ in the field F.

Proof. Let $0 \leqslant B \leqslant p$ be the least integer such that $f \in V_B$. Since $f \neq 0$, so $B \geqslant 1$, and

$$f = c_{B-1} f_{B-1} + \sum_{0 \leqslant A < B-1} c_A f_A$$

with some $c_{B-1} \neq 0$, $c_0, \ldots, c_{B-1} \in F$. We have $B > 1$, because $f(0) = 0$. Let $h = (1/c_{B-1}) f_{p-B}$. Then, since $(f_{B-1}, f_{p-B}) = -1$, by Lemma 1 and Lemma 3 $(T^j f, h) = -1$ for every $j \geqslant 0$. This means that $g - h \in V_B^{\perp} = V_{p-B}$, hence

$$g = \frac{1}{c_{B-1}} f_{p-B} + \sum_{0 \leqslant A < p-B} d_A f_A$$

with $d_A \in F$ for $0 \leqslant A < p - B$. We can see that $B < p$, as $g(0) = 0$. So $1 < B < p$. Let $P_f, P_g \in F[x]$ with

$$P_f(x) = c_{B-1} x^{B-1} + \sum_{0 \leqslant A < B-1} c_A x^A,$$

and

$$P_g(x) = \frac{1}{c_{B-1}} x^{p-B} + \sum_{0 \leqslant A < p-B} d_A x^A.$$

Then $P_f(i) = f(i)$, $P_g(i) = g(i)$ for every $i \in F_p$. Hence $(P_f P_g)(i) = f(i)\, g(i) = i^{p-1}$ for every $i \in F_p$, and on the other hand $\deg(P_f P_g) = p - 1$. This means that the polynomials $P_f(x)\, P_g(x)$ and x^{p-1} are of degree at most $p - 1$, and they take the same value at p distinct elements (at the elements of F_p). So $P_f(x)\, P_g(x) = x^{p-1}$, i.e., $P_f(x)$ divides x^{p-1}, and we obtain

$$f(i) = c_{B-1} i^{B-1}$$

for every $i \in F_p$. Since $f(1) = 1$, we must have $c_{B-1} = 1$, and then $f = f_A$ with $A = B - 1$, where $1 \leqslant A \leqslant p - 2$, because $1 < B < p$.

4. PROOF OF THEOREM 1

The proof consists of two parts. In the first part we prove (see Lemma 5) that if a solution consists of algebraic numbers (of course after proving Theorem 1 we will know that this is true for every solution), then it consists of numbers relatively prime to p. This result is not surprising, because we expect that the solutions are characters, hence they consist of roots of unity. Lemma 5 is the only arithmetic information we need: in the second part of the proof we derive Theorem 1 from Lemma 5 using some general algebraic geometry.

LEMMA 5. *Let K be an algebraic number field, let R be the ring of integers in K, and P a prime ideal of R such that $P \cap Z = pZ$. Let $a_i, b_i \in K$ for $i \in F_p$ such that $a_0 = 0$, $a_1 = 1$, and $a_i b_i = 1$ for $i \in F_p \setminus \{0\}$. Assume that for every $j \in F_p \setminus \{0\}$ we have*

$$\sum_{i \in F_p} a_{i+j} b_i = -1.$$

Then $v_P(a_i)=0$ *for every* $i\in F_p\setminus\{0\}$. (*Here for elements* $\alpha\in K\setminus\{0\}$ *we denote by* $v_P(\alpha)$ *the exponent of* α *with respect to* P, *i.e.*, $v_P(\alpha)$ *is the integer such that*

$$\alpha R = P^{v_P(\alpha)}Q_1Q_2^{-1},$$

where Q_1 *and* Q_2 *are ideals of* R *prime to* P. *We put* $v_P(0)=\infty$.)

Remark. In our application we will have $b_0=0$, but we do not need it here.

Proof. Assume that the function $i\to v_P(a_i)$ is not constant on $F_p\setminus\{0\}$. (Otherwise we are done, because $v_P(a_1)=v_P(1)=0$.) Let

$$m_1=\min_{i\in F_p} v_P(a_i), \qquad m_2=\min_{i\in F_P} v_P(b_i),$$

and

$$H_1=\{i\in F_P : v_P(a_i)=m_1\}, \qquad H_2=\{i\in F_P : v_P(b_i)=m_2\}.$$

By our assumptions $m_1\leqslant 0$, $m_2\leqslant 0$, $m_1+m_2<0$, since $v_P(a_1)=v_P(b_1)=v_P(1)=0$, $v_P(a_i)+v_P(b_i)=0$ for $i\in F_P\setminus\{0\}$, and $i\to v_P(a_i)$ is not constant on $F_p\setminus\{0\}$.

We have $H_1\cap H_2=\varnothing$, since $0\notin H_1$ (because $a_0=0$, $a_1=1$), and if $i\neq 0$, $i\in H_1\cap H_2$, then by $a_ib_i=1$ we would have $m_1+m_2=0$, which is a contradiction.

It is clear that for $i_1i_2\in F_p$ one has

$$v_P(a_{i_1}b_{i_2})\geqslant m_1+m_2,$$

and equality holds if and only if $i_1\in H_1$, $i_2\in H_2$. On the other hand, for any $j\in F_p$ the relation

$$v_P\left(\sum_{i\in F_p} a_{i+j}b_i\right)=0$$

holds, because for $j\neq 0$ the inner sum is -1, for $j=0$ it is $p-1$.

Now let $\pi\in P\setminus P^2$. We obtain from the above facts for every fixed $j\in F_p$ that

$$v_P\left(\sum_{i+j\in H_1,\, i\in H2} \frac{a_{i+j}}{\pi^{m_1}}\frac{b_i}{\pi^{m_2}}\right)>0$$

(using also $m_1+m_2<0$).

Let $F = R/P$, this is an extension field of F_p. The natural homomorphism $q: R \to F$ uniquely extends to a homomorpism $q: \hat{R} \to F$, where

$$\hat{R} = \{\alpha \in K : v_P(\alpha) \geqslant 0\}.$$

Define the functions $f: F_p \to F$ and $g: F_p \to F$ in the following way. For $i \in F_p$ we set $f(i) = q(a_i/\pi^{m_1})$, $g(i) = q(b_i/\pi^{m_2})$. We obtain from the above considerations that

$$\sum_{i \in F_p} f(i+j)\, g(i) = 0$$

for every $j \in F_p$, and obviously the support of f is H_1, the support of g is H_2, and $H_1 \neq \emptyset$, $H_2 \neq \emptyset$. This constradicts Lemma 6 below, so the present lemma will be proved if we prove Lemma 6.

LEMMA 6. *Let $f: F_p \to F$ and $g: F_p \to F$ be given functions, and $H_1, H_2 \subseteq F_p$ such that $H_1 \cap H_2 = \emptyset$, and $f(i) = 0$ for $i \in F_p \backslash H_1$, $g(i) = 0$ for $i \in F_p \backslash H_2$. Assume further that for all $j \in F_p$ we have*

$$\sum_{i \in F_p} f(i+j)\, g(i) = 0.$$

Then at least one of the functions f and g is identically 0.

Proof. Let $0 \leqslant B \leqslant p$ be the least integer such that $f \in V_B$. We can assume that $B \geqslant 1$, since $B = 0$ means that f is identically 0. Since we have $(T^j f, g) = 0$ or every $j \geqslant 0$ by our conditions, so $g \in V_B^{\perp} = V_{p-B}$. We can assume that $B \leqslant p-1$, since $B = p$ means that g is identically 0.

So there are polynomials $P_f, P_g \in F[x]$ with $\deg P_f \leqslant B-1$, $\deg P_g \leqslant (p-B)-1$, and

$$P_f(i) = f(i), \qquad P_g(i) = g(i)$$

for every $i \in F_p$. But $f(i)\, g(i) = 0$ for every $i \in F_p$, since $H_1 \cap H_2 = \emptyset$. So the degree of the polynomial $P_f\, P_g$ is at most $p-2$, but it has p distinct roots, which means that $P_f\, P_g = 0 \in F[x]$. This implies that $P_f = 0$ or $P_g = 0$, which proves the lemma.

We will use the following result from algebraic geometry.

LEMMA 7. *Let $P_i(x_1, x_2, ..., x_n)$, $Q_j(x_1, x_2, ..., x_n) \in C[x_1, x_2, ..., x_n]$ be given n-variable complex polynomials $(1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s)$, and let X be the subset of C^n where the polynomials P_i vanish but the Q_j do not, i.e.,*

$$X = \{(a_1, a_2, ..., a_n) \in C^n : P_i(a_1, a_2, ..., a_n) = 0, \qquad Q_j(a_1, a_2, ..., a_n) \neq 0\}.$$

Let $1 \leqslant k \leqslant n$ be fixed and denote by p_k the projection of C^n on the kth coordinate axis, so $p_k((a_1, a_2, ..., a_n)) = a_k$. Then either $p_k(X)$ or $C \backslash p_k(X)$ is finite.

Proof. This is a special case of a theorem of Chevalley, a form of which states that the image of a constructible subset by a morphism of affine algebraic varieties is again constructible. A constructible subset is a finite union of locally closed subsets, where locally closed means the intersection of an open and a closed subset (with respect to the Zariski topology). Now, our X is locally closed in the affine n-space, projection is a morphism, and a locally closed subset of the affine line is either finite or its complement is finite, so our statement follows. For a proof of the theorem of Chevalley see, e.g., [H, Sect. 4.4].

We also need an easy consequence of this.

LEMMA 8. *The notations are the same as in Lemma 7, but this time we assume that the coefficients of the polynomials P_i and Q_j are algebraic numbers. Assume that X is nonempty. Then X has a point with all of its coordinates algebraic.*

Proof. We prove it by induction on n. If $|X| < \infty$, then obviously every coordinate of every point of X is algebraic, so we may assume that $|X| = \infty$. Then there is a $1 \leqslant k \leqslant n$ such that $|p_k(X)| = \infty$, by symmetry we can put $k = n$, and by Lemma 7 we have that $|C \backslash p_n(X)| < \infty$. So there is an algebraic α with $\alpha \in p_n(X)$. This proves the statement for $n = 1$, and for $n > 1$ the set Y of $(n-1)$-tuples $(a_1, a_2, ..., a_{n-1})$ with $(a_1, a_2, ..., a_{n-1}, \alpha) \in X$ is nonempty, and then applying the inductive hypothesis for this Y the lemma is proved.

Proof of Theorem 1. It follows from Lemma 5 that if the a_i are algebraic numbers and $(a_i : i \in F_p)$ satisfies the conditions of Theorem 1, then for each $i \neq 0, 1$ one has $a_i \notin pZ$, where Z is the set of rational integers (taking $b_0 = 0$, $b_i = 1/a_i$ for $i \in F_p \backslash \{0\}$, and letting P be any prime ideal above p of $K = Q(a_2, a_3, ..., a_{p-1})$). We prove that if we would have infinitely many solutions, then we could find a solution such that each a_i is algebraic and $a_i \in pZ$ for some $i \neq 0, 1$, and this will prove the theorem.

Let X be the set of p-tuples $(a_i : i \in F_p)$ satisfying the conditions listed in the assertion of the theorem. If $|X| = \infty$, then we can find an $i_0 \neq 0, 1$ such that $|p_{i_0}(X)| = \infty$. Then, by Lemma 7, $C \backslash p_{i_0}(X)$ is finite, so we can find an integer $n_0 \in Z$ such that $pn_0 \in p_{i_0}(X)$. Let X_0 be the set of points in X with $a_{i_0} = pn_0$. Then X_0 is nonempty, so applying Lemma 8 the proof is finished.

REFERENCES

[H] J. E. Humphreys, "Linear Algebraic Groups," Springer-Verlag, Berlin/Heidelberg/New York, 1975.

[M] H. L. Montgomery, "Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis," Amer. Math. Soc., Providence, 1994.