JOURNAL OF NUMBER THEORY 9, 203–208 (1977)

An Example from Power Residues of the Critical Problem of Crapo and Rota

K. R. MATTHEWS

Department of Mathematics, University of Queensland, St. Lucia, Brisbane, Queensland, 4067 Australia

Communicated by H. Zassenhaus

Received June 13, 1975

A natural density arising from the author's recent work on a generalization of Artin's conjecture for primitive roots is shown to be essentially the characteristic polynomial of a geometric lattice, as defined by Crapo and Rota. Necessary and sufficient conditions are obtained for the vanishing of this density.

1. INTRODUCTION

Let p be a prime, $a_1,..., a_n$ be nonzero integers, and let P be the set of primes $q \equiv 1 \pmod p$ such that each of $a_1,..., a_n$ is a pth power nonresidue mod q. The natural density $d(p)$ of P is defined by

$$d(p) = \lim_{x\to\infty} (\pi(x))^{-1} \sum_{\substack{q\leqslant x\\ q\in P}} 1,$$

where $\pi(x)$ is the number of primes not exceeding x. In a recent paper of the author [2] the problem of finding necessary and sufficient conditions for $d(3)$ to vanish arose. The general problem of the vanishing of $d(p)$ turns out to be a critical problem as defined by Crapo and Rota [1, 16.1].

Clearly $d(p) = 0$ if one of $a_1,..., a_n$ is a perfect pth power, for then P is empty. However, the converse is not in general true. We shall find that certain pth power relations must hold between $a_1,..., a_n$ in order that $d(p)$ vanish.

2. A FORMULA FOR $d(p)$

The principle of inclusion–exclusion gives

$$\sum_{\substack{q\leqslant x\\ q\in P}} 1 = \sum_{\substack{q\leqslant x\\ q\equiv 1 (\mathrm{mod}\ p)}} 1 + \sum_{j=1}^{n} (-1)^j \sum_{1\leqslant i_1<\cdots<i_j\leqslant n} |\mathscr{S}_{i_1} \cap \cdots \cap \mathscr{S}_{i_j}|, \qquad (1)$$

ISSN 0022-314X

where $\mathscr{S}_i$ is the set of primes $q \leqslant x$, $q \equiv 1 \pmod{p}$ such that a_i is a pth power residue mod q. The prime ideal theorem (see [3, p. 162]) gives for $1 \leqslant i_1 < \cdots < i_j \leqslant n$,

$$\lim_{x\to\infty} (\pi(x))^{-1} \mid \mathscr{S}_{i_1} \cap \cdots \cap \mathscr{S}_{i_j} \mid = [\mathfrak{Q}(e^{2\pi i/p}, (a_{i_1})^{1/p}, \ldots, (a_{i_j})^{1/p}) : \mathfrak{Q}]^{-1}$$
$$= (p^j(p-1))^{-1}\, \tau(i_1, \ldots, i_j),$$

where $\tau(i_1, \ldots, i_j)$ is the number of j-tuples of integers $(\nu_1, \ldots, \nu_j)$, $1 \leqslant \nu_i \leqslant p$ such that

$$a_i^{\nu_1} \cdots a_{i_j}^{\nu_j} = b^p, \qquad b \text{ an integer.} \tag{2}$$

Also

$$\lim_{x\to\infty} (\pi(x))^{-1} \sum_{\substack{q \leqslant x \\ q \equiv 1 (\mathrm{mod}\ p)}} 1 = (p-1)^{-1} \tag{3}$$

by the prime number theorem for arithmetic progressions. Consequently from (1), (2), and (3) we have

$$d(p) = (p-1)^{-1} \left[1 + \sum_{j=1}^{n} (-1)^j p^{-j} \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} \tau(i_1, \ldots, i_j)\right]. \tag{4}$$

Similarly

$$(p-1)^{-k} \left[1 + \sum_{j=1}^{n} (-1)^j p^{-kj} \sum_{1 \leqslant i_1 \leqslant \cdots \leqslant i_j \leqslant n} \tau(i_1, \ldots, i_j)\right]$$

is the natural density of the k-tuples $(q_1, \ldots, q_k)$ of primes $q_j \equiv 1 \pmod{p}$ such that for all i, $1 \leqslant i \leqslant n$, there exists a j, $1 \leqslant j \leqslant k$, such that a_i is a pth power nonresidue mod q_j.

This formula can be transformed somewhat. Let $p_1, \ldots, p_t$ be the distinct primes which divide $a_1 a_2 \cdots a_n$ and let $\nu_{p_r}(a_s)$ be the exponent to which p_r divides a_s. Then (2) is equivalent to a vector equation in $V_t(\mathscr{F})$ ($\mathscr{F} = GF(p)$), namely,

$$\nu_1 C_{i_1} + \cdots + \nu_j C_{i_j} = 0,$$

where $C_1, \ldots, C_n$ are the columns of the $t \times n$ exponent matrix $C = [\nu_{p_r}(a_s)]$. Hence $\tau(i_1, \ldots, i_j)$ is the number of vectors in the null space of the matrix $[C_{i_1} \mid \cdots \mid C_{i_j}]$. Consequently

$$\tau(i_1, \ldots, i_j) = p^{j\text{-rank}[C_{i_1} \mid \cdots \mid C_{i_j}]}. \tag{5}$$

From (4) and (5) we obtain

$$d(p) = [p^t(p-1)]^{-1} \left[p^t + \sum_{j=1}^{n} (-1)^j \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} p^{t\text{-rank}[C_{i_1} \mid \cdots \mid C_{i_j}]}\right]. \tag{6}$$

It turns out that $p^t d(p)$ is the number of projective hyperplanes in $V_t(\mathscr{F})$ (i.e., sets of the form $\alpha_1 x_1 + \cdots + \alpha_t x_t = 0$, $\alpha_1, \ldots, \alpha_t$ not all zero) which do not pass through any of $C_1, \ldots, C_n$ (see Lemma 1).

3. The Critical Problem of Crapo and Rota

We may assume that $C_1, \ldots, C_n$ are each nonzero, for $C_i = 0$ is equivalent to a_i being a perfect pth power, and we know that $d(p) = 0$ in this case.

With Crapo and Rota we say that a sequence $L_1, \ldots, L_k$ of linear functionals on $V_t(\mathscr{F})$ distinguishes the set $S = \{C_1, \ldots, C_n\}$ if for each C_i, $1 \leqslant i \leqslant n$, there corresponds an L_j such that $L_j(C_i) \neq 0$. The minimum k for which such a sequence exists is called the critical exponent c of S. It is clear that $1 \leqslant c \leqslant t$.

Crapo and Rota use Möbius theory to prove the following result (see [1, 16.4]).

Lemma 1. *The number N_k of k sequences $L_1, \ldots, L_k$ of linear functionals on $V_t(\mathscr{F})$ which distinguish $S = \{C_1, \ldots, C_n\}$ is equal to $P(p^k)$, where $P(\lambda)$ is the polynomial defined by*

$$P(\lambda) = \lambda^t + \sum_{j=1}^{n} (-1)^j \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} \lambda^{t\text{-rank}[C_{i_1} | \cdots | C_{i_j}]} \tag{7}$$

($P(\lambda)$ is the characteristic polynomial of the geometric lattice spanned by $C_1, \ldots, C_n$.)

For the convenience of the reader we give a proof based on inclusion–exclusion.

Proof. For $1 \leqslant i_1 < \cdots < i_j \leqslant n$ *let $g(i_1, \ldots, i_j)$ be the number of linear functionals on $V_t(\mathscr{F})$ which vanish at each of $C_{i_1}, \ldots, C_{i_j}$*. Then

$$N_k = p^{tk} + \sum_{j=1}^{n} (-1)^j \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} g^k(i_1, \ldots, i_j) \tag{8}$$

by the principle of inclusion–exclusion.

However, $g(i_1, \ldots, i_j)$ is the number of elements in the quotient space $V_t(\mathscr{F})/B(i_1, \ldots, i_j)$, where $B(i_1, \ldots, i_j)$ is the column space of $[C_{i_1} | \cdots | C_{i_j}]$. Hence

$$g(i_1, \ldots, i_j) = p^{t\text{-rank}[C_{i_1} | \cdots | C_{i_j}]}. \tag{9}$$

From (8) and (9) it follows that $N_k = P(p^k)$.

COROLLARY 1. *If c is the critical exponent of $S = \{C_1, \ldots, C_n\}$, then*

$$P(p^k) = 0 \quad \text{for } k = 0, 1, \ldots, c-1,$$
$$P(p^k) > 0 \quad \text{for } k \geqslant c.$$

The Corollary shows that $d(p) = 0$ if and only if $c \geqslant 2$.

COROLLARY 2. *If rank $C = n$ then $c = 1$ and $d(p) > 0$.*

Proof. If rank $C = n$, then

$$P(\lambda) = \lambda^{t-n}(\lambda - 1)^n.$$

Hence $P(p)$ and so $d(p)$ are positive.

Remark. The condition rank $C = n$ means there is no nontrivial relation

$$a_1^{\nu_1} \cdots a_n^{\nu_n} = b^p, \qquad b \text{ an integer}, \quad 1 \leqslant \nu_i \leqslant p.$$

This is certainly true, for example, if $a_1, \ldots, a_n$ are pairwise relatively prime and none of $a_1, \ldots, a_n$ is a perfect pth power.

4. A NECESSARY AND SUFFICIENT CONDITION FOR $d(p) > 0$

By Corollary 2 we may assume that rank $C = r < n$. We also assume $a_1, \ldots, a_n$ have been relabeled if necessary so that $C_1, \ldots, C_r$ are linearly independent over $\mathscr{F}$.

Instead of the $P(p^k)$ k sequences of linear functionals on $V_t(\mathscr{F})$ which distinguish S, we consider the $p^{-k(t-\operatorname{rank} C)}P(p^k)$ k sequences of linear functionals on the column space of C, which distinguish S. Such linear functionals are given by the formula

$$L(\lambda_1 C_1 + \cdots + \lambda_r C_r) = \lambda_1 \alpha_1 + \cdots + \lambda_r \alpha_r, \tag{10}$$

where $\alpha_1, \ldots, \alpha_r \in \mathscr{F}$.

We also let

$$\begin{aligned} C_{r+1} &= \lambda_{1,1} C_1 + \cdots + \lambda_{1,r} C_r, \\ &\vdots \\ C_n &= \lambda_{n-r,1} C_1 + \cdots + \lambda_{n-r,r} C_r. \end{aligned} \tag{11}$$

(Equations (11) are equivalent to

$$a_{r+1} = a_1^{\lambda_{1,1}} \cdots a_r^{\lambda_{1,r}} b_1^{\,p}, \ldots, a_n = a_1^{\lambda_{n-r,1}} \cdots a_r^{\lambda_{n-r,r}} b_{n-r}^p,$$

where $b_1, \ldots, b_{n-r}$ are rational.)

The following equations should be noted:

$$L(C_i) = \begin{cases} \alpha_i & \text{for } \ 1 \leqslant i \leqslant r, \\ \lambda_{i-r,1}\alpha_1 + \cdots + \lambda_{i-r,r}\alpha_r & \text{for } \ r+1 \leqslant i \leqslant n, \end{cases}$$

where L is defined by (10). We then have the

THEOREM. *$d(p) = 0$ if and only if for every r-tuple $(\alpha_1, \ldots, \alpha_r)$ of nonzero elements of $\mathscr{F}$, we have*

$$\lambda_{j,1}\alpha_1 + \cdots + \lambda_{j,r}\alpha_r = 0$$

for some j, $1 \leqslant j \leqslant n - r$, j depending on $(\alpha_1, \ldots, \alpha_r)$. Here $\lambda_{j,k}$ are defined by (11).

Proof.

$d(p) = 0 \Leftrightarrow c \geqslant 2,$

$\Leftrightarrow$ one linear functional L does not suffice to distinguish S,

$\Leftrightarrow \forall L, \exists i, 1 \leqslant i \leqslant n$, such that $L(C_i) = 0$,

$\Leftrightarrow \forall L$ given by (10) with each of $\alpha_1, \ldots, \alpha_n$ nonzero, $\exists i, r + 1 \leqslant i \leqslant n$, such that $L(C_i) = 0$,

$\Leftrightarrow \forall(\alpha_1, \ldots, \alpha_r)$ with $\alpha_1, \ldots, \alpha_r$ nonzero, $\exists j, 1 \leqslant j \leqslant n - r$, such that $\lambda_{j,1}\alpha_1 + \cdots + \lambda_{j,r}\alpha_r = 0.$

EXAMPLE. Take $n = 4$, $r = 2$, $p = 3$ and assume that none of a_1, a_2, a_3, a_4 is a perfect cube. Then

$$C_3 = \lambda_{1,1}C_1 + \lambda_{1,2}C_2 \quad \text{and} \quad C_4 = \lambda_{2,1}C_1 + \lambda_{2,2}C_2 .$$

Hence by the Theorem, $d(3) = 0$ if and only if

$$\lambda_{1,1} + \lambda_{1,2} = 0 \quad \text{or} \quad \lambda_{2,1} + \lambda_{2,2} = 0$$

and

$$\lambda_{1,1} - \lambda_{1,2} = 0 \quad \text{or} \quad \lambda_{2,1} - \lambda_{2,2} = 0,$$

over $GF(3)$.

The only possible choices of systems are

$$\lambda_{1,1} + \lambda_{1,2} = 0 \quad \text{and} \quad \lambda_{2,1} - \lambda_{2,2} = 0$$

or

$$\lambda_{2,1} + \lambda_{2,2} = 0 \quad \text{and} \quad \lambda_{1,1} - \lambda_{1,2} = 0.$$

The first possibility corresponds to

$$a_3 = a_1^{2s} a_2^{s} b_1^{3} \quad \text{and} \quad a_4 = a_1^{t} a_2^{t} b_2^{3}, \tag{10}$$

b_1 and b_2 rational, s and t not divisible by 3, while the second possibility corresponds to interchanging a_3 and a_4 in (10).

References

1. H. H. Crapo and G. C. Rota, "On the Foundations of Combinatorial Theory: Combinatorial Geometries," M.I.T. Press, Cambridge, Mass., 1970.
2. K. R. Matthews, A generalisation of Artin's conjecture for primitive roots, *Acta Arith.* **29** (1976), 113–146.
3. A. Schinzel, A refinement of a theorem of Gerst on power residues, *Acta Arith.* **27** (1970), 161–168.