JOURNAL OF NUMBER THEORY **65**, 101–104 (1997)
ARTICLE NO. NT972135

One-Dimensional Crystals and Quadratic Residues

Fernando Chamizo and Antonio Córdoba

Departamento de Matemáticas, Facultad de Ciencias, Universidad Autónoma de Madrid, 28049 Madrid, Spain

Communicated by A. Granville

Received March 21, 1996; revised December 18, 1996

The main problem in crystallography is recovering the electronic density from the diffraction peak intensities. The one-dimensional model leads to recover a discrete Fourier series in $\mathbb{Z}_n$ with integral coefficients from its absolute value, which has arithmetical implications. In this paper we prove that the constant absolute value of Gaussian sums determines them among a class of exponential sums. This implies that if diffraction peak intensities are constant except for one of them, then, modulo translations, we obtain a quadratic residue molecule. © 1997 Academic Press

1. INTRODUCTION

The spatial configurations of crystallized molecules are usually obtained via x-ray diffraction data. As was first suggested by M. von Laue, when the intensities of the diffracted rays are registered on a flat screen, high peaks appear in a discrete set, revealing the symmetries of the crystal. The standard interpretation assigns diffraction peak intensities to absolute values of the Fourier transform $\hat{\rho}$ of the electron density ρ. The phase problem asks for the reconstruction of ρ from the knowledge of $|\hat{\rho}|$. In certain interesting cases this leads naturally to problems of factorization in suitable rings of polynomials (see [6]). For example, if we have a density $\rho = \sum \delta_{n_j}$ where δ_{n_j} denotes Dirac's delta function placed at the integer n_j, then $|\hat{\rho}|$ determines (modulo translations or reflections) ρ if the polynomial $\sum x^{n_j}$ is irreducible in $\mathbb{Z}[x]$. This leads to the study of irreducible polynomials with 0, 1 coefficients. In [4] the conjecture that most of these polynomials are irreducible is stated and some other related results are quoted. On the other hand, in general, if the polynomial $\sum x^{n_j}$ is not irreducible there is a lack of uniqueness, showing that in general terms the phase problem is not well posed (the first practical example of nonuniqueness was considered in 1930 by Pauling and Shappell [5] who were studying crystals of bixbyite). A rather interesting question is which kind of "chemical,"

0022-314X/97 $25.00

"geometric," or "arithmetic," information about ρ is relevant to ensure the reconstruction (see [3] and [6]).

A plausible model for the electronic density of one-dimensional (periodic) crystals is given by infinite sums of Dirac's delta functions (cf. [2])

$$\rho = \sum_{j=1}^{N} b_j \sum_{n=-\infty}^{\infty} \delta_{x_j+n},$$

where $b_j \in \mathbb{Z}^+$ are positive integers and $0 \leqslant x_j < 1$.

In this context, the phase problem seeks to locate the positions $\{x_j\}$ (modulo translations or reflections $x'_j = 1 - x_j$) knowing the absolute values

$$F(v) = \left| \sum_{j=1}^{N} b_j e^{2\pi i x_j v} \right|, \qquad v \in \mathbb{Z}.$$

The result presented in this paper consists of a new observation about Gaussian sums, i.e., roughly speaking, they are determined by their absolute value among a class of exponential sums. In this way we obtain a nontrivial case in which the phase problem can be solved.

Notation. Throughout this paper we shall write $e(x)$ as an abbreviation of $e^{2\pi i x}$, and (n/p), p prime, will denote the usual Legendre symbol (i.e., $+1$ if n is a quadratic residue and -1 if n is a quadratic nonresidue modulo p).

2. STATEMENT AND PROOF OF THE RESULT

Our result reads as follows:

THEOREM 2.1. *Let $0 = x_1 < x_2 < \cdots < x_N < 1$ be real numbers and assume that there exists a prime number p such that the sum*

$$S(m) = \sum_{j=1}^{N} b_j e(m x_j), \qquad b_j \in \mathbb{Z}^+,$$

is of constant modulus $|S(m)| = \Gamma$ if p is not a divisor of m and $|S(m)| = \sum b_j$ otherwise. Then $p x_j \in \mathbb{Z}$, $1 \leqslant j \leqslant N$, and either

$$S(m) = AT(m) + Be\left(\frac{mk}{p}\right) G(m) \qquad or \qquad S(m) = AT(m) + Be\left(\frac{mk}{p}\right),$$

where $A, B, k \in \mathbb{Z}$ *and*

$$T(m) = \sum_{n=0}^{p-1} e\left(\frac{mn}{p}\right), \qquad G(m) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e\left(\frac{mn}{p}\right).$$

The proof will be based on the following lemma.

LEMMA 2.2. *If all the algebraic conjugates of* $x \in \mathbb{Q}(\zeta)$, $\zeta = e(1/p)$, *are complex numbers of equal modulus, then either*

$$x = B\zeta^k \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^n \qquad or \qquad x = B\zeta^k,$$

for some $B \in \mathbb{Q}$, $k \in \mathbb{Z}$.

Proof. Let σ be a generator of the Galois group of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Using the hypothesis of the lemma we can write $\sigma(x)/x = e(\alpha)$, for some $\alpha \in \mathbb{Q}$ (if $\alpha \notin \mathbb{Q}$ then $e(\alpha)$ is not an algebraic number [1]), i.e., $\sigma(x)/x = \zeta_b^a$, where $\zeta_b = e(1/b)$, $a, b \in \mathbb{Z}^+$, $(a, b) = 1$.

Taking a^* such that $a^* a \equiv 1 \bmod (b)$ we get that $\zeta_b = (\zeta_b^a)^{a^*} \in \mathbb{Q}(\zeta)$. We have two cases:

(i) If $p \mid b$, then $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta_b)] = \phi(p)/\phi(b)$ yields $b = p$ or $b = 2p$.

(ii) If $p \nmid b$, then $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta, \zeta_b) = \mathbb{Q}(\zeta_{pb})$ yields $pb = p$ or $pb = 2p$.

Therefore we have that $b = 1, 2, p, 2p$ and $\zeta_b^a = \pm \zeta^l$ for some integer l, $0 \leqslant l \leqslant p-1$.

Let us assume that $\sigma(\zeta) = \zeta^g$, and take k such that $(g-1)\,k \equiv l \bmod p$, then since $\sigma(x)/x = \pm \zeta^l$, we get

$$\frac{\sigma(\zeta^{-k}x)}{\zeta^{-k}x} = \pm 1, \qquad \frac{\sigma^2(\zeta^{-k}x)}{\sigma(\zeta^{-k}x)} = \pm 1.$$

Therefore $\sigma^2(\zeta^{-k}x) = \zeta^{-k}x$.

The subfield invariant under σ^2 is

$$M = \{a(\sigma^2(\zeta) + \sigma^4(\zeta) + \cdots + \sigma^{p-1}(\zeta)) + b(\sigma(\zeta) + \sigma^3(\zeta) + \cdots + \sigma^{p-2}(\zeta));\ a, b \in \mathbb{Q}\},$$

hence

$$\zeta^{-k}x = a \sum_{n \in \mathscr{R}} \zeta^n + b \sum_{n \in \mathscr{N}} \zeta^n, \qquad a, b \in \mathbb{Q},$$

where $\mathscr{R}$ and $\mathscr{N}$ denote, respectively, the set of quadratic and nonquadratic residues mod p.

If $\sigma(\zeta^{-k}x)=\zeta^{-k}x$, $\zeta^{-k}x \in \mathbb{Q}$. If $\sigma(\zeta^{-k}x)=-\zeta^{-k}x$, then we have $b=-a$ and that $\zeta^{-k}x$ is a rational multiple of a Gauss sum. ∎

Proof of the Theorem. The identity $|S(p)|=\sum b_j$ implies $e(px_1)=e(px_2)=\cdots=e(px_N)$ and since we have fixed $x_1=0$ then we must have $x_r=n_r/p$ for some integers n_r, $0\leqslant n_r<p$. Therefore $x=S(1)$ is in the hypothesis of the lemma and we get either

$$S(1)=Be\left(\frac{k}{p}\right)G(1) \qquad \text{or} \qquad S(1)=Be\left(\frac{k}{p}\right).$$

For m prime with p we obtain by conjugation in $\mathbb{Q}(\zeta)$ either

$$S(m)=Be\left(\frac{mk}{p}\right)G(m) \qquad \text{or} \qquad S(m)=Be\left(\frac{mk}{p}\right).$$

Finally, let us observe that $T(m)$ vanishes if and only if $p\nmid m$. Therefore there exists $A\in\mathbb{Q}$ such that either

$$S(m)=AT(m)+Be\left(\frac{mk}{p}\right)G(m) \qquad \text{or} \qquad S(m)=AT(m)+Be\left(\frac{mk}{p}\right),$$

for every $m\in\mathbb{Z}$.

Identifying coefficients, we deduce easily that A and B are integers. ∎

REFERENCES

1. A. Baker, "Transcendental Number Theory," Cambridge Univ. Press, Cambridge, 1975.
2. C. Giacovazzo, The diffraction of x-rays by crystals, *in* "Fundamentals of Crystallography," International Union of Crystallography, Oxford Univ. Press, Oxford, 1995.
3. A. Grübaum and C. Moore, The use of higher-order invariants in the determination of generalized Patterson cyclotomic sets, *Acta Crystallogr. A* **51** (1995), 310–323.
4. A. M. Odlyzko and B. Poonen, Zeros of polynomials with 0, 1 coefficients, *Enseign. Math.* **39** (1993), 317–348.
5. L. Pauling and M. D. Shappell, The crystal structure of bixbyite and the C-modification of the sesquioxides, *Z. Kristallogr.* **75** (1930), 128–142.
6. J. Rosenblatt, Phase retrieval, *Commun. Math. Phys.* **95** (1984), 317–343.