Canad. J. Math. Vol. **55** (2), 2003 pp. 432–448

Pair Correlation of Squares in p-Adic Fields

Alexandru Zaharescu

Abstract. Let p be an odd prime number, K a p-adic field of degree r over $\mathbf{Q}_p$, O the ring of integers in K, $B = \{\beta_1, \dots, \beta_r\}$ an integral basis of K over $\mathbf{Q}_p$, u a unit in O and consider sets of the form $\mathcal{N} = \{n_1\beta_1 + \cdots + n_r\beta_r : 1 \le n_j \le N_j, 1 \le j \le r\}$. We show under certain growth conditions that the pair correlation of $\{uz^2 : z \in \mathcal{N}\}$ becomes Poissonian.

1 Introduction

In a p-adic field the squares are distributed very regularly in many respects. Our aim here is to describe a p-adic context in which squares show signs of Poisson behavior. Given a sequence $\{\theta_n\} \subset [0, 1)$, the nearest neighbor spacing distribution is defined by ordering the first N elements of the sequence: $\theta_{1,N} \le \theta_{2,N} \le \cdots \le \theta_{N,N}$, and then defining the normalized spacings to be

$$\delta_n^{(N)} := N(\theta_{n+1,N} - \theta_{n,N}).$$

The asymptotic distribution function of $\{\delta_n^{(N)}\}_{n=1}^N$ is level spacing distribution $P_1(s)$, that is for each interval $[a, b]$ we require that

$$\lim_N \frac{1}{N} \#\{n < N : \delta_n^{(N)} \in [a, b]\} = \int_a^b P_1(s)\, ds.$$

In the Poisson model of a sequence generated by uncorrelated levels, $P_1(s) = e^{-s}$. Moreover in that model one knows the behavior of all other local spacing statistics. For a fixed real number α, the problem of the distribution of local spacings between the members of the sequence $\alpha n^2 (\mathrm{mod}\ 1)$ has been investigated in [7]. The standard approach to the analysis of the consecutive spacing measures is via m-level correlations, for any $m \ge 2$. One of the main results in [7] gives conditions on the diophantine approximations to α which ensure that along a subsequence all the m-level correlations of $\alpha n^2 (\mathrm{mod}\ 1)$ become Poissonian. It is also shown in [7] that there are irrational numbers α for which the 5-level correlations diverge to infinity. The source of this phenomenon is large square factors in the denominators of the convergents to the continued fraction of α. The extreme case when these denominators are powers of a fixed prime number p can be interpreted in a p-adic context. In this paper we are concerned with such a case. Since we know that in this situation higher correlations diverge, we will only consider the pair correlation problem ($m = 2$). The pair

Received by the editors November 13, 2001; revised May 28, 2002.
AMS subject classification: 11S99, 11K06.

correlation function measures the density of differences between pairs of elements of a given sequence. Thus for a sequence $(x_n)_{n\in\mathbf{N}}$ uniformly distributed in $[0,1]$, the pair correlation function $R_2(x)$ is given, if it exists, by

$$\lim_{N\to\infty}\frac{1}{N}\#\Big\{1\le n_1\ne n_2\le N : x_{n_1}-x_{n_2}\in\frac{1}{N}I\Big\}=\int_I R_2(x)\,dx \tag{1}$$

for any interval $I\subset\mathbf{R}$. In the Poissonian model the pair correlation function $R_2(x)$ is identically equal to 1. It was proved in [6] that, given a polynomial f of degree ≥ 2 with integer coefficients, the pair correlation of the sequence $\alpha f(n)(\mathrm{mod}\ 1)$ is Poissonian, for almost all $\alpha\in\mathbf{R}$. In particular, for almost all $\alpha\in\mathbf{R}$ the pair correlation of $\alpha n^2(\mathrm{mod}\ 1)$ is Poissonian. One also knows (see [1]) that for any irrational number α there is a sequence of "windows" $[M+1,M+N]$, with N as large as $M^{1/5}$, along which the pair correlation of $\alpha n^2(\mathrm{mod}\ 1)$ becomes Poissonian. In order to understand for fixed α the distribution of $\alpha n^2(\mathrm{mod}\ 1)$, approximations of α by rationals $\frac{b}{q}$ have been considered in [7]. This leads to the problem of studying the distribution of finite sequences of the form $bn^2(\mathrm{mod}\ q)$, $1\le n\le N$, with $(b,q)=1$, where $q\to\infty$ and N grows with q. The case q prime is investigated in [7] in the context of general m-level correlations, and the case q almost square free is discussed in [9]. In [5], [4] the distribution of squares modulo q is shown to be Poissonian as $q\to\infty$ provided the number of distinct prime factors of q goes to infinity. In the present paper we let q be a power of a fixed prime number p. Then the pair correlation of the complete sequence $bn^2(\mathrm{mod}\ q)$ is not Poissonian. However, for N in the range $q^{\frac{3}{4}+\delta}<N<q^{1-\delta}$ for some fixed $\delta>0$, the pair correlation of the sequence $bn^2(\mathrm{mod}\ q)$, $1\le n\le N$ becomes Poissonian as $q\to\infty$. In other words, with δ, q, b and N as above, for any interval $I\subset\mathbf{R}$ one has

$$\lim_{q\to\infty}\frac{1}{N}\#\Big\{1\le n_1\ne n_2\le N : bn_1^2-bn_2^2\equiv h(\mathrm{mod}\ q), h\in\frac{q}{N}I\Big\}=\mathrm{length}(I). \tag{2}$$

This result holds for general q and it was known to the authors of [7], although it was not inserted in the final version of [7]. In what follows we let q be a power of p, interpret (2) in the field $\mathbf{Q}_p$ of p-adic numbers and then prove an extension of that result in the context of a general p-adic field K.

2 Statement of Main Result

We start with a prime number p and an extension K of $\mathbf{Q}_p$ of degree r. In order to simplify the presentation we assume in the following that $p\ne 2$. Denote as usually by $\mathbf{Z}_p$ the ring of integers in $\mathbf{Q}_p$. Choose a large natural number s and set $q=p^s$. The number b which appears on the left side of (2) can be replaced by any p-adic unit. Also, the conditions $bn_1^2-bn_2^2\equiv h(\mathrm{mod}\ q)$, $h\in\frac{q}{N}I$ may be written in the form

$$bn_1^2-bn_2^2\in I_{q,N} \tag{3}$$

where

$$I_{q,N}=\Big(\frac{q}{N}I\cap\mathbf{Z}\Big)+q\mathbf{Z}_p. \tag{4}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

Here we used simultaneously the canonical injections of $\mathbf{Z}$ in $\mathbf{R}$ and in $\mathbf{Z}_p$. Note that for fixed I, if $N, q \to \infty$ such that $\frac{q}{N} \to \infty$ then one has

$$\#\Big(\frac{q}{N}I \cap \mathbf{Z}\Big) \sim \frac{q}{N}\,\mathrm{length}(I).$$

Note also that for N larger than the length of I the sets $n + q\mathbf{Z}_p$, with $n \in \frac{q}{N}I \cap \mathbf{Z}$, are disjoint balls in $\mathbf{Z}_p$. Therefore, if we denote by $\mu_{\mathbf{Z}_p}$ the Haar measure on $\mathbf{Z}_p$, normalized by $\mu_{\mathbf{Z}_p}(\mathbf{Z}_p) = 1$, then one has

$$\mu_{\mathbf{Z}_p}(I_{q,N}) \sim \frac{\mathrm{length}(I)}{N}. \tag{5}$$

Relations (3), (4) and (5) point to the following interpretation of the problem. We have a sequence bn^2, $1 \le n \le N$ in $\mathbf{Z}_p$ and we look for pairs of elements in this sequence for which their difference belongs to a certain set $I_{q,N}$ of measure $\sim \frac{\mathrm{length}(I)}{N}$. This is analogous to the pair correlation problem for sequences in $[0,1]$, stated in (1). We now return to our p-adic field K and view the pair correlation problem as an r-dimensional extension of the previous case. Denote by O the ring of integers in K and fix an integral basis $B = \{\beta_1, \dots, \beta_r\}$ of K over $\mathbf{Q}_p$. Choose s large and set $q = p^s$ as before. Next, choose positive integers $N_1, \dots, N_r \le q$ and consider the set

$$\mathcal{N} = \{n_1\beta_1 + \cdots + n_r\beta_r : 1 \le n_j \le N_j, 1 \le j \le r\}. \tag{6}$$

Denote $N = N_1 \cdots N_r$. Choose a unit $u \in O$, and consider the finite sequence uz^2, $z \in \mathcal{N}$. In order to find analogs of (3), (4) and (5) in this more general context, let us fix a box $I = I_1 \times \cdots \times I_r \subset \mathbf{R}^r$. The dilate factor q/N from (4) needs to be replaced by $q/N^{1/r}$. We take all the integer points $h = (h_1, \dots, h_r)$ from $(q/N^{1/r})I$ and then send them to O through the map $(h_1, \dots, h_r) \mapsto h_1\beta_1 + \cdots + h_r\beta_r = h \cdot \beta$, where we set $\beta = (\beta_1, \dots, \beta_r)$. Thus we consider the set

$$I_{q,N} = \Big\{h \cdot \beta : h \in \frac{q}{N^{1/r}}I \cap \mathbf{Z}^r\Big\} + qO. \tag{7}$$

Again the Haar measure of $I_{q,N}$ and the Lebesgue measure of I are connected by the asymptotic relation

$$\mu_O(I_{q,N}) \sim \frac{\mathrm{Vol}(I)}{N} \tag{8}$$

as $q, N \to \infty$ such that $q/N^{1/r} \to \infty$. Here the Haar measure μ_O is normalized by $\mu_O(O) = 1$. Then the basic quantity to be investigated in the pair correlation problem for the sequence uz^2, $z \in \mathcal{N}$ is

$$R^{(2)}(K, B, u, I, q, \mathcal{N}) := \frac{1}{N}\#\{z_1 \ne z_2 \in \mathcal{N} : uz_1^2 - uz_2^2 \in I_{q,N}\}. \tag{9}$$

The question is whether, by analogy with (2), one has

$$R^{(2)}(K, B, u, I, q, \mathcal{N}) \to \mathrm{Vol}(I)$$

as $q \to \infty$. For simplicity in what follows we will only consider boxes I which do not contain the origin. Then we may drop the condition $z_1 \ne z_2$ on the right side of (9). Our main result is the following

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

Theorem 1 *Let p be an odd prime number, $\frac{1}{8} > \delta > 0$, K a p-adic field of degree r over $\mathbf{Q}_p$, O the ring of integers in K, B an integral basis of K over $\mathbf{Q}_p$, u a unit in O and $0 \notin I$ a box in $\mathbf{R}^r$. Then as $q, N_1, \ldots, N_r \to \infty$, $q = p^s$, s integer, such that $q^\delta \leq N_1, \ldots, N_r \leq q$ and $N := N_1 \cdots N_r \in [q^{\frac{3r}{4}+\delta}, q^{r-\delta}]$ one has*

$$R^{(2)}(K, B, u, I, q, \mathcal{N}) \to \mathrm{Vol}(I). \tag{10}$$

3 The Case of the Complete Sequence $(\mathrm{mod}\ q)$

In this section we consider the sequence $uz^2, z \in \mathcal{N}$ in the particular case when $N_1 = \cdots = N_r = q$. Then $\mathcal{N}$ consists of a complete set of representatives in O modulo the ideal qO. For any $a \in O$ denote

$$c(K, q, a) = \#\{z_1, z_2 \in \mathcal{N} : uz_1^2 - uz_2^2 \in a + qO\}.$$

Note that $c(K, q, a)$ does not depend on the choice of the integral basis B. If we set $A = O/qO$ then $c(K, q, a)$ equals the number of solutions $(x_1, x_2) \in A \times A$ of the equation

$$ux_1^2 - ux_2^2 = a. \tag{11}$$

Here u is invertible in A. We make a change of variables $x_1 + x_2 = y_1, x_1 - x_2 = y_2$. Then (recall that p is odd) $c(K, q, a)$ equals the number of solutions $(y_1, y_2) \in A \times A$ of the equation

$$y_1 y_2 = au^{-1}. \tag{12}$$

Assume first that a is invertible in A. This forces both y_1 and y_2 to be invertible in A. Conversely, for any invertible element $y_1 \in A$ there is a unique $y_2 \in A$ satisfying (12). It follows in this case that $c(K, q, a)$ equals the number of invertible elements of A. These are the elements of A which do not vanish in the residue field of K, call it k. Say $\#(k) = p^f$. Then

$$c(K, q, a) = \left(1 - \frac{1}{p^f}\right) \#A = p^{rs} - p^{rs-f}. \tag{13}$$

Denote by e the ramification index of K over $\mathbf{Q}_p$ and let π be a uniformizer of K. Then $r = fe$, $pO = \pi^e O$ and $qO = \pi^{se} O$. Let now $a \in O \setminus qO$. Write a in the form $a = \pi^m a'$ where a' is a unit in O. If (y_1, y_2) is a solution of (12), $y_1 = \pi^{m_1} y_1'$, $y_2 = \pi^{m_2} y_2'$ with y_1', y_2' invertible in A, then

$$m_1 + m_2 = m \tag{14}$$

and

$$y_1' y_2' = a' u^{-1} (\mathrm{mod}\ q\pi^{-m} A). \tag{15}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

Conversely, if $y_1, y_2 \in A$ are such that (14) and (15) hold true, then (y_1, y_2) is a solution of (12). Let us count the solutions to (12) for a fixed pair (m_1, m_2) satisfying (14). We treat (15) as an equality in the ring $A/q\pi^{-m}A$. As before, the number of solutions of (15) in $A/q\pi^{-m}A$ equals the number of invertible elements in $A/q\pi^{-m}A$, which in turn equals

$$\Big(1 - \frac{1}{p^f}\Big)\#(A/q\pi^{-m}A) = \Big(1 - \frac{1}{p^f}\Big)p^{f(se-m)} = p^{rs-fm} - p^{rs-f(m+1)}.$$

Now by the equality $y_1 = \pi^{m_1}y_1'$, y_1' is well defined in $A/q\pi^{-m_1}A$, therefore there are exactly

$$\frac{\#(A/q\pi^{-m_1}A)}{\#(A/q\pi^{-m}A)} = \frac{p^{f(se-m_1)}}{p^{f(se-m)}} = p^{fm_2}$$

values of y_1' which have the same image in $A/q\pi^{-m}A$. Similarly, there are p^{fm_1} values of y_2' which have the same image in $A/q\pi^{-m}A$. It follows that each of the above $p^{rs-fm} - p^{rs-f(m+1)}$ solutions in $A/q\pi^{-m}A$ corresponds to p^{fm} solutions $(y_1, y_2) \in A \times A$. This gives $p^{rs} - p^{rs-f}$ solutions to (12) for each fixed pair (m_1, m_2). There are $m+1$ pairs (m_1, m_2) satisfying (14). We obtain the following generalization of (13).

Lemma 1 *For any $0 \le m < se$ and any $a \in \pi^m O \setminus \pi^{m+1}O$ one has*

$$c(K, q, a) = (m+1)(p^{sr} - p^{sr-f}). \tag{16}$$

4 Characters

Any element $t \in O$ can be written uniquely in the form $t = t_1\beta_1 + \cdots + t_r\beta_r$ with $t_1, \ldots, t_r \in \mathbf{Z}_p$, and $t \in qO$ if and only if $t_1, \ldots, t_r \in q\mathbf{Z}_p$. Since $\mathbf{Z}_p/q\mathbf{Z}_p$ is canonically isomorphic to $\mathbf{Z}/q\mathbf{Z}$, we get a natural map $H\colon A \to (\mathbf{Z}/q\mathbf{Z})^r$ given by $H(t) = \big(t_1 (\mathrm{mod}\, q), \ldots, t_r (\mathrm{mod}\, q)\big)$. Note that H is an isomorphism of abelian groups. One may then use H in order to describe the characters of the group $(A, +)$. We choose a vector $v = (v_1, \ldots, v_r) \in (\mathbf{Z}/q\mathbf{Z})^r$ such that if we let $t = \pi^{se-1}$ the dot product $H(t) \cdot v = t_1v_1 + \cdots + t_rv_r$ is not zero in $\mathbf{Z}/q\mathbf{Z}$. Clearly there are such vectors v since $t = \pi^{se-1} \neq 0$ in A so not all the components $t_1, \ldots, t_r$ are zero in $\mathbf{Z}/q\mathbf{Z}$. The vector v depends on the basis B, and will be fixed in what follows. Consider the map $\psi\colon A \to \mathbf{C}$ given by $\psi(t) = e_q\big(H(t) \cdot v\big)$, where $e_q : \mathbf{Z}/q\mathbf{Z} \to \mathbf{C}$ is defined by $e_q(n) = \exp(\frac{2\pi i n}{q})$. Note that

$$\psi(t + w) = \psi(t)\psi(w),$$

that is, ψ is a character of the group $(A, +)$. In particular we have $\psi(0) = 1$ and $\psi(-t) = \psi(t)^{-1} = \overline{\psi(t)}$. For any $w \in A$ define a map $\psi_w\colon A \to \mathbf{C}$ by $\psi_w(t) = \psi(wt)$. Clearly ψ_w is a character of A for each $w \in A$. Moreover one has $\psi_1 = \psi$ and $\psi_{w+z} = \psi_w\psi_z$ for any $w, z \in A$. We claim that distinct elements w', w'' of A produce distinct characters. Indeed, if $w' \neq w''$ and $\psi_{w'} = \psi_{w''}$ then if we set $w = w' - w''$, ψ_w will be the trivial character: $\psi_w(t) = 1$ for all $t \in A$. Now the point is that any

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

nonzero element of A is a divisor of π^{se-1} in A. Thus if we choose $t \in A$ such that $wt = \pi^{se-1}$ we will have

$$\psi_w(t) = \psi(wt) = \psi(\pi^{se-1}) = e_q\big(H(\pi^{se-1}) \cdot v\big) \neq 1$$

since $H(\pi^{se-1}) \cdot v \neq 0$ in $\mathbf{Z}/q\mathbf{Z}$ by our choice of v. This proves the claim. It follows that ψ_w, $w \in A$ are all the characters of A. As a consequence one has the orthogonality relation

$$\frac{1}{\#(A)} \sum_{w \in A} \psi_w(t) = \frac{1}{\#(A)} \sum_{w \in A} \psi(wt) = \begin{cases} 1, & \text{if } t = 0 \\ 0, & \text{else.} \end{cases} \tag{17}$$

Next, we claim that for any $0 \leq m \leq se$ and any $t \in A$ one has

$$\sum_{z \in \pi^m A} \psi(tz) = \begin{cases} p^{sr-fm}, & \text{if } t \in \pi^{se-m}A \\ 0, & \text{else.} \end{cases} \tag{18}$$

Indeed, if $t \in \pi^{se-m}A$ then $tz = 0$ for any $z \in \pi^m A$ and the left side of (18) equals $\#(\pi^m A) = p^{sr-fm}$. Assume now that $t \notin \pi^{se-m}A$. Then $\pi^m t \neq 0$. By applying (17) to $\pi^m t$ one obtains

$$\sum_{w \in A} \psi(w\pi^m t) = 0. \tag{19}$$

Note that for any $z \in \pi^m A$ we have the same number of elements $w \in A$ for which $z = \pi^m w$. For, if $z = \pi^m w_1 = \pi^m w_2$ then $\pi^m(w_1 - w_2) = 0$, so $w_1 - w_2 \in \pi^{se-m}A$. Conversely, if $z = \pi^m w_1$ and $w_1 - w_2 \in \pi^{se-m}A$ then $z = \pi^m w_2$. It follows that for each $z \in \pi^m A$ the set $\{w \in A : \pi^m w = z\}$ coincides with one of the cosets of A modulo the ideal $\pi^{se-m}A$, so all these sets have the same number of elements, equal to $\#(\pi^{se-m}A) = p^{mf}$. We conclude that the left side of (19) equals the left side of (18) multiplied by p^{mf}, and this proves the claim.

5 Kloosterman Sums

In order to study the distribution of sequences of the form $bn^2 (\mathrm{mod}\ p)$, $1 \leq n \leq N$ for large prime numbers p, exponential sums of linear forms along certain curves $(\mathrm{mod}\ p)$ are considered in [7]. In the pair correlation problem, the curves are given by equations of the form $bx_1^2 - bx_2^2 = \text{constant}$. The change of variables $x_1 + x_2 = y_1$, $x_1 - x_2 = y_2$ transforms the above exponential sums into Kloosterman sums. Here we try to follow the same argument, so at this point we bring into play Kloosterman sums in our context. Notations are as in the previous sections. We associate to any $a, b \in A$ the Kloosterman sum

$$\mathrm{Kl}(a, b, q) = \sum_{x \in A^\times} \psi(ax + bx^{-1}) \tag{20}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

where $A^\times = A \setminus \pi A$ is the group of invertible elements in A. Thus $\#(A^\times) = \#(A)(1 - p^{-f}) = p^{sr} - p^{sr-f}$. Note that when $K = \mathbf{Q}_p$, $B = \{1\}$, the sums $\mathrm{Kl}(a, b, q)$ coincide with the classical Kloosterman sums (mod q). In that case one has (see [8], [3])

$$\mathrm{Kl}(a, b, q) \ll q^{\frac{1}{2}}(a, b, q)^{\frac{1}{2}}, \tag{21}$$

where (a, b, q) denotes the greatest common divisor of the numbers a, b and q. Returning to the case of a general K, we set $s_1 = [\frac{s+1}{2}]$, where $[\cdot]$ denotes the integer part function. Let us fix a set $\mathcal{L}$ of representatives in A modulo the ideal $p^{s_1}A$. Next, we take any element $x \in A$ and write it uniquely in the form

$$x = y + z, \quad y \in \mathcal{L},\ z \in p^{s_1}A. \tag{22}$$

In the argument that follows, y and z are assumed to be functions of x, given by (22). Clearly $x \in A \setminus \pi A$ if and only if $y \in A \setminus \pi A$. Denote $\mathcal{L}^\times = \mathcal{L} \cap A^\times$. Then, as x runs over $A^\times$, y and z will run independently over $\mathcal{L}^\times$ and respectively $p^{s_1}A$. Therefore

$$\mathrm{Kl}(a, b, q) = \sum_{y \in \mathcal{L}^\times} \sum_{z \in p^{s_1}A} \psi\big(ay + az + b(y + z)^{-1}\big). \tag{23}$$

Now $z^2 = 0$ by our choice of s_1. It follows that $(1 - y^{-1}z)(1 + y^{-1}z) = 1$ and hence $(y + z)^{-1} = y^{-1}(1 + y^{-1}z)^{-1} = y^{-1}(1 - y^{-1}z) = y^{-1} - y^{-2}z$ for any $y \in \mathcal{L}^\times$ and $z \in p^{s_1}A$. Inserting this in (23) one obtains

$$\begin{aligned} \mathrm{Kl}(a, b, q) &= \sum_{y \in \mathcal{L}^\times} \sum_{z \in p^{s_1}A} \psi(ay + az + by^{-1} - by^{-2}z) \\ &= \sum_{y \in \mathcal{L}^\times} \psi(ay + by^{-1}) \sum_{z \in p^{s_1}A} \psi\big((a - by^{-2})z\big). \end{aligned} \tag{24}$$

Here the inner sum is zero unless $a - by^{-2} \in p^{s-s_1}A$ when it equals $p^{(s-s_1)r}$ by (18). Thus

$$\mathrm{Kl}(a, b, q) = p^{(s-s_1)r} \sum_{\substack{y \in \mathcal{L}^\times \\ a - by^{-2} \in p^{s-s_1}A}} \psi(ay + by^{-1}). \tag{25}$$

This further implies

$$|\mathrm{Kl}(a, b, q)| \le p^{(s-s_1)r} \#(\mathcal{U}_{a,b,q}) \tag{26}$$

where

$$\mathcal{U}_{a,b,q} := \{y \in \mathcal{L}^\times : a - by^{-2} \in p^{s-s_1}A\} = \{y \in \mathcal{L}^\times : ay^2 - b \in p^{s-s_1}A\}.$$

Let us assume first that at least one of a, b is not divisible by p. Fix $y_0 \in \mathcal{U}_{a,b,q}$. For any $y \in \mathcal{U}_{a,b,q}$ one has $a(y^2 - y_0^2) \in p^{s-s_1}A$ and $by^{-2}y_0^{-2}(y^2 - y_0^2) = b(y_0^{-2} - y^{-2}) \in$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

$p^{s-s_1}A$. It follows that $y^2 - y_0^2 \in p^{s-s_1-1}A$, which in turn implies $y - y_0 \in p^{s-s_1-1}A$ or $y + y_0 \in p^{s-s_1-1}A$. Thus $\mathcal{U}_{a,b,q}$ is contained in the union of the sets $y_0 + p^{s-s_1-1}A$ and $-y_0 + p^{s-s_1-1}A$. By the definition of $\mathcal{L}$ we know that the elements of $\mathcal{U}_{a,b,q}$ have distinct images in $A/p^{s_1}A$. We conclude that

$$\#(\mathcal{U}_{a,b,q}) \leq 2\#(p^{s-s_1-1}A/p^{s_1}A) = 2p^{(2s_1+1-s)r}.$$

Employing this in (26) one obtains

$$|\operatorname{Kl}(a,b,q)| \leq 2p^{(s_1+1)r} \leq 2p^{\frac{(s+3)r}{2}}. \tag{27}$$

Let now a, b be arbitrary elements of A. There is no cancellation in the sum from the right side of (20) if $a = b = 0$. Assume at least one of a, b is not zero, and let l be the largest positive integer for which p^l divides both a and b. Choose $a_1, b_1 \in A$ such that $a = p^l a_1$ and $b = p^l b_1$. Each invertible element of $O/p^{s-l}O$ is the image of exactly p^{lr} elements of $A^\times$ and

$$\operatorname{Kl}(a,b,q) = p^{lr}\operatorname{Kl}(a_1,b_1,p^{s-l}). \tag{28}$$

Here at least one of a_1, b_1 is not divisible by p, so one may apply (27) to $\operatorname{Kl}(a_1, b_1, p^{s-l})$:

$$\operatorname{Kl}(a_1,b_1,p^{s-l}) \leq 2p^{\frac{(s-l+3)r}{2}}. \tag{29}$$

We have proved the following

Lemma 2 *Let $a, b \in A$ and let l be the largest positive integer $\leq s$ for which $a, b \in p^l A$. Then*

$$\operatorname{Kl}(a,b,q) \leq 2p^{\frac{(s+l+3)r}{2}}.$$

Let now $a, b, c \in A$, $c \neq 0$ and consider the sum

$$T(a,b,c,q) = \sum_{\substack{x_1,x_2 \in A \\ x_1x_2=c}} \psi(ax_1 + bx_2). \tag{30}$$

Let m_a, m_b, m_c be the largest integers $\leq se$ for which π^{m_a} divides a, π^{m_b} divides b and π^{m_c} divides c. We put (30) in the form

$$T(a,b,c,q) = \sum_{m_1+m_2=m_c} \sum_{\substack{x_1 \in \pi^{m_1}A \setminus \pi^{m_1+1}A \\ x_2 \in \pi^{m_2}A \setminus \pi^{m_2+1}A \\ x_1x_2=c}} \psi(ax_1 + bx_2). \tag{31}$$

For any $x_1 \in \pi^{m_1}A \setminus \pi^{m_1+1}A$ there are exactly p^{fm_1} elements $y_1 \in A^\times$ for which $x_1 = \pi^{m_1}y_1$. Similarly, given $x_2 \in \pi^{m_2}A \setminus \pi^{m_2+1}A$, there are p^{fm_2} elements $y_2 \in A^\times$ such that $x_2 = \pi^{m_2}y_2$. Therefore

$$T(a,b,c,q) = \frac{1}{p^{fm_c}} \sum_{m_1+m_2=m_c} \sum_{\substack{y_1,y_2 \in A^\times \\ \pi^{m_c}y_1y_2=c}} \psi(a\pi^{m_1}y_1 + b\pi^{m_2}y_2). \tag{32}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

If we choose $c' \in A^\times$ such that $c = \pi^{m_c} c'$ then the condition $\pi^{m_c} y_1 y_2 = c$ can be written as $y_2 = c' y_1^{-1} + z$, with $z \in \pi^{se-m_c} A$, hence

$$T(a,b,c,q) = \frac{1}{p^{fm_c}} \sum_{m_1+m_2=m_c} \sum_{y_1 \in A^\times} \sum_{z \in \pi^{se-m_c} A} \psi\big(a\pi^{m_1} y_1 + b\pi^{m_2}(c' y_1^{-1} + z)\big).$$

We infer from (18) that

$$\sum_{z \in \pi^{se-m_c} A} \psi(b\pi^{m_2} z) = \begin{cases} p^{fm_c}, & \text{if } b\pi^{m_2} \in \pi^{m_c} A \\ 0, & \text{else.} \end{cases} \tag{33}$$

The condition $b\pi^{m_2} \in \pi^{m_c} A$ is equivalent to $m_b \geq m_1$. On combining the last two relations we see that

$$\begin{aligned} T(a,b,c,q) &= \sum_{\substack{m_1+m_2=m_c \\ m_1 \leq m_b}} \sum_{y_1 \in A^\times} \psi(a\pi^{m_1} y_1 + b\pi^{m_2} c' y_1^{-1}) \\ &= \sum_{\substack{m_1+m_2=m_c \\ m_1 \leq m_b}} \mathrm{Kl}(a\pi^{m_1}, b\pi^{m_2} c', q). \end{aligned} \tag{34}$$

From Lemma 2 we derive

$$|T(a,b,c,q)| \leq 2 \sum_{\substack{m_1+m_2=m_c \\ m_1 \leq m_b}} p^{\frac{(s+l(m_1,m_2)+3)r}{2}} \tag{35}$$

where $l(m_1,m_2)$ is the largest integer $\leq s$ for which $a\pi^{m_1}, b\pi^{m_2} \in p^{l(m_1,m_2)}A$. The condition $a\pi^{m_1} \in p^{l(m_1,m_2)}A$ gives $el(m_1,m_2) \leq m_a + m_1 \leq m_a + m_c$. Similarly, $b\pi^{m_2} \in p^{l(m_1,m_2)}A$ implies $el(m_1,m_2) \leq m_b + m_2 \leq m_b + m_c$. Therefore $rl(m_1,m_2) = fel(m_1,m_2) \leq f(m_c + \min\{m_a, m_b\})$, and from (35) we derive

$$|T(a,b,c,q)| \leq 2sep^{\frac{(s+3)r+f(m_c+\min\{m_a,m_b\})}{2}}. \tag{36}$$

Recalling that $r = fe$, we have the following result.

Lemma 3 *Let $a, b, c \in A$ and let l, m be the largest integers $\leq s$ for which $a, b \in p^l A$ and $c \in p^m A$. Then*

$$|T(a,b,c,q)| \leq 2rsp^{\frac{(s+l+m+5)r}{2}}. \tag{37}$$

6 Proof of Theorem 1. Preliminaries

Let p, δ, K, O, B, u and I be as in the statement of the theorem. Choose a large number $q = p^s$ and positive integers $q^\delta \leq N_1, \ldots, N_r \leq q$ such that $N := N_1 \cdots N_r \in$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

$[q^{\frac{3r}{4}+\delta}, q^{r-\delta}]$, and consider the sequence $uz^2, z \in \mathcal{N}$ with $\mathcal{N}$ given by (6). For any $a \in O$ denote

$$\nu(a) = \#\{z_1, z_2 \in \mathcal{N} : uz_1^2 - uz_2^2 - a \in qO\}. \tag{38}$$

Then (9), (7) and (38) give

$$R^{(2)}(K, B, u, I, q, N) = \frac{1}{N} \sum_{h \in \frac{q}{N^{1/r}} I \cap \mathbf{Z}^r} \nu(h \cdot \beta). \tag{39}$$

Since $N_1, \ldots, N_r \leq q$, the set $\mathcal{N}$ injects in A via the canonical projection $O \to O/qO = A$. In (38) we view $\mathcal{N}$, u and a as lying inside A (note that $\nu(a) = \nu(a')$ if $a, a' \in O$ have the same image in A) and write (38) in the form

$$\nu(a) = \#\{z_1, z_2 \in \mathcal{N} \subseteq A : uz_1^2 - uz_2^2 = a\}. \tag{40}$$

Denote by J the image in A of the the set $\{h \cdot \beta : h \in \frac{q}{N^{1/r}} I \cap \mathbf{Z}^r\}$. Then (39) may be rewritten as

$$R^{(2)}(K, B, u, I, q, N) = \frac{1}{N} \sum_{a \in J} \nu(a). \tag{41}$$

For any $a \in A$ define a function g_a on $A \times A$ by

$$g_a(x_1, x_2) = \begin{cases} 1, & \text{if } ux_1^2 - ux_2^2 = a \\ 0, & \text{else} \end{cases} \tag{42}$$

so that

$$\nu(a) = \sum_{z_1, z_2 \in \mathcal{N}} g_a(z_1, z_2). \tag{43}$$

For $a, y_1, y_2 \in A$ consider the sum

$$S(a, y_1, y_2) = \frac{1}{\#(A)^2} \sum_{w_1, w_2 \in A} g_a(w_1, w_2) \psi(-y_1 w_1 - y_2 w_2). \tag{44}$$

Let us compute

$$\begin{aligned} &\sum_{y_1, y_2 \in A} S(a, y_1, y_2) \sum_{z_1, z_2 \in \mathcal{N}} \psi(y_1 z_1 + y_2 z_2) \\ &= \frac{1}{\#(A)^2} \sum_{z_1, z_2 \in \mathcal{N}} \sum_{y_1, y_2 \in A} \psi(y_1 z_1 + y_2 z_2) \sum_{w_1, w_2 \in A} g_a(w_1, w_2) \psi(-y_1 w_1 - y_2 w_2) \\ &= \frac{1}{\#(A)^2} \sum_{z_1, z_2 \in \mathcal{N}} \sum_{w_1, w_2 \in A} g_a(w_1, w_2) \sum_{y_1, y_2 \in A} \psi\big(y_1(z_1 - w_1) + y_2(z_2 - w_2)\big). \end{aligned} \tag{45}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

Here the inner sum vanishes unless $z_1 = w_1$ and $z_2 = w_2$ when it equals $\#(A)^2$ by (17). Thus

$$\sum_{y_1,y_2\in A} S(a,y_1,y_2) \sum_{z_1,z_2\in\mathcal{N}} \psi(y_1z_1+y_2z_2) = \sum_{z_1,z_2\in\mathcal{N}} g_a(z_1,z_2) = \nu(a) \tag{46}$$

by (43). Using (46) in (41) one obtains

$$R^{(2)}(K,B,u,I,q,N) = \frac{1}{N}\sum_{a\in J}\sum_{y_1,y_2\in A} S(a,y_1,y_2) \sum_{z_1,z_2\in\mathcal{N}} \psi(y_1z_1+y_2z_2).$$

We now change the order of summation, then separate out the contribution of $(y_1,y_2) = (0,0)$:

$$R^{(2)}(K,B,u,I,q,N) = \mathcal{M} + \mathcal{E} \tag{47}$$

where the main term $\mathcal{M}$ equals

$$\mathcal{M} = \frac{1}{N}\sum_{a\in J} S(a,0,0) \sum_{z_1,z_2\in\mathcal{N}} \psi(0) = N\sum_{a\in J} S(a,0,0), \tag{48}$$

and the remainder $\mathcal{E}$ is given by

$$\mathcal{E} = \frac{1}{N}\sum_{(0,0)\neq(y_1,y_2)}\sum_{z_1,z_2\in\mathcal{N}} \psi(y_1z_1+y_2z_2)\sum_{a\in J} S(a,y_1,y_2). \tag{49}$$

7 The Main Term

In this section we show that

$$\mathcal{M} \to \mathrm{Vol}(I) \tag{50}$$

as $q, N_1, \dots, N_r \to \infty$ subject to the conditions from the statement of Theorem 1. From (44) and (42) it follows that

$$\begin{aligned} S(a,0,0) &= \frac{1}{\#(A)^2}\sum_{w_1,w_2\in A} g_a(w_1,w_2) \\ &= \frac{1}{\#(A)^2}\#\{(w_1,w_2)\in A\times A : uw_1^2 - uw_2^2 = a\} \\ &= \frac{1}{\#(A)^2}c(K,q,a) = p^{-2sr}c(K,q,a). \end{aligned} \tag{51}$$

Therefore

$$\mathcal{M} = Np^{-2sr}\sum_{a\in J} c(K,q,a). \tag{52}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

We now apply Lemma 1, which gives

$$\begin{aligned}(53)\qquad \mathcal{M} &= Np^{-2sr}\sum_{0\le m<se}\ \sum_{a\in J\cap(\pi^m A\setminus\pi^{m+1}A)}(m+1)(p^{sr}-p^{sr-f})\\ &= Np^{-2sr}(p^{sr}-p^{sr-f})\sum_{0\le m<se}(m+1)\big(\#(J\cap\pi^m A)-\#(J\cap\pi^{m+1}A)\big)\\ &= Np^{-sr}(1-p^{-f})\sum_{m\ge 0}\#(J\cap\pi^m A).\end{aligned}$$

Here $\#(J\cap\pi^m A)=0$ as soon as $m>\frac{se}{4}$. Indeed, any element $t\in J$ is of the form $t=t_1\beta_1+\cdots+t_r\beta_r$ with $t_1,\dots,t_r\in\mathbf{Z}$, $(t_1,\dots,t_r)\neq(0,\dots,0)$ and $|t_1|,\dots,|t_r|\ll\frac{q}{N^{1/r}}\le q^{\frac14-\frac{\delta}{r}}=p^{\frac{s}{4}-\frac{\delta s}{r}}$, so t can not be divisible by π^m if $m>\frac{se}{4}$. We now fix an m and estimate $\#(J\cap\pi^m A)$. Assume first that m is a multiple of e, say $m=em_1$. Let $h\in\frac{q}{N^{1/r}}I\cap\mathbf{Z}^r$, $h=(h_1,\dots,h_r)$. Since B is an integral basis, p^{m_1} divides $h\cdot\beta$ if and only if p^{m_1} divides each of the integers $h_1,\dots,h_r$. We deduce that

$$(54)\qquad \#(J\cap\pi^m A)=\#\Big(\frac{q}{N^{1/r}}I\cap p^{m_1}\mathbf{Z}^r\Big).$$

The right side of (54) coincides with the number of integer points in the box $\frac{q}{N^{1/r}p^{m_1}}I$. By the Lipschitz principle (see Davenport [2]) it follows that

$$\begin{aligned}(55)\quad \#(J\cap\pi^m A)=\#(J\cap p^{m_1}A)&=\mathrm{Vol}\Big(\frac{q}{N^{1/r}p^{m_1}}I\Big)+O_{r,I}\Big(\Big(1+\frac{q}{N^{1/r}p^{m_1}}\Big)^{r-1}\Big)\\ &=\frac{q^r}{Np^{rm_1}}\mathrm{Vol}(I)+O_{r,I}\Big(1+q^{r-1}N^{\frac{1-r}{r}}p^{(1-r)m_1}\Big).\end{aligned}$$

Note that the main term on the right side of (55) equals $\frac{q^r}{Np^{fm}}\mathrm{Vol}(I)$. We now extend this estimate to the case of a general m. Write $m=em_1+l$ with $0\le l<e$. If $h\in\frac{q}{N^{1/r}}I\cap\mathbf{Z}^r$, $h=(h_1,\dots,h_r)$, then π^m divides $h\cdot\beta$ if and only if $h_j=p^{m_1}t_j$, $1\le j\le r$ with $t_1,\dots,t_r\in\mathbf{Z}$ and $t_1\beta_1+\cdots+t_r\beta_r$ divisible by π^l. Thus

$$(56)\qquad \#(J\cap\pi^m A)=\#\Big\{t\in\frac{q}{N^{1/r}p^{m_1}}I\cap\mathbf{Z}^r:\pi^l\text{ divides }t\cdot\beta\Big\}.$$

We break the box $\frac{q}{N^{1/r}p^{m_1}}I$ into cubes of side p of the form $y+pU$, $y\in p\mathbf{Z}^r$, where $U=\{0\le x_1,\dots,x_r<1\}$ is the unit cube in $\mathbf{R}^r$. Note that as t runs over the set of integer points in such a cube $y+pU$, $t\cdot\beta$ runs over a set of representatives in O for O/pO. In the ring O/pO there are exactly $\#(\pi^l O/pO)=p^{f(e-l)}=p^{r-fl}$ elements which are divisible by π^l. Thus for any cube $y+pU$ as above one has

$$(57)\qquad \#\{t\in\mathbf{Z}^r\cap(y+pU):\pi^l\text{ divides }t\cdot\beta\}=p^{r-fl}.$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

Now the number of cubes $y + pU$, $y \in p\mathbf{Z}^r$ which are entirely contained in the box $\frac{q}{N^{1/r}p^{m_1}}I$ equals

$$\text{Vol}\Big(\frac{q}{N^{1/r}p^{m_1+1}}I\Big) + O_{r,I}\Big(\Big(1+\frac{q}{N^{1/r}p^{m_1+1}}\Big)^{r-1}\Big) \tag{58}$$
$$= \frac{q^r}{Np^{r(m_1+1)}}\,\text{Vol}(I) + O_{r,I}(1 + q^{r-1}N^{\frac{1-r}{r}}p^{(1-r)(m_1+1)}).$$

Also, the number of boundary cubes, that is the number of cubes $y + pU$, $y \in p\mathbf{Z}^r$ which have a nonempty intersection with the box $\frac{q}{N^{1/r}p^{m_1}}I$ but are not contained in it, is $O_{r,I}\big((1 + qN^{-1/r}p^{-(m_1+1)})^{r-1}\big)$. It follows that the number of integer points from the box $\frac{q}{N^{1/r}p^{m_1}}I$ which belong to boundary cubes is $O_{r,I}(p^r + q^{r-1}N^{\frac{1-r}{r}}p^{r+(1-r)(m_1+1)})$. Using this, together with (57) and (58) in (56) we derive

$$\#(J \cap \pi^m A) = p^{r-fl}\Big(\frac{q^r}{Np^{r(m_1+1)}}\,\text{Vol}(I) + O_{r,I}(1 + q^{r-1}N^{\frac{1-r}{r}}p^{(1-r)(m_1+1)})\Big) \tag{59}$$
$$+ O_{r,I}(p^r + q^{r-1}N^{\frac{1-r}{r}}p^{r+(1-r)(m_1+1)})$$
$$= \frac{q^r}{Np^{fm}}\,\text{Vol}(I) + O_{r,I}(p^r + q^{r-1}N^{\frac{1-r}{r}}p^{r+\frac{(1-r)m}{e}}).$$

From (59) we get (recall that $\#(J \cap \pi^m A) = 0$ for $m > \frac{se}{4}$)

$$\sum_{m\geq 0}\#(J \cap \pi^m A) = \frac{q^r}{N(1-p^{-f})}\,\text{Vol}(I) + O_{r,I}(sp^r + sp^r q^{r-1}N^{\frac{1-r}{r}}) \tag{60}$$
$$= \frac{p^{sr}}{N(1-p^{-f})}\,\text{Vol}(I) + O_{r,I}(sp^r q^{r-1}N^{\frac{1-r}{r}}).$$

On combining (60) with (53) and the inequality $N \leq q^{r-\delta}$ we finally obtain

$$\mathcal{M} = \text{Vol}(I) + O_{r,I}(sp^r q^{-1}N^{\frac{1}{r}}) = \text{Vol}(I) + O_{r,I}(sp^{r-\frac{\delta s}{r}}) \tag{61}$$

which proves (50).

8 The Remainder

In order to complete the proof of Theorem 1 it remains to show that

$$\mathcal{E} \to 0 \tag{62}$$

as $q, N_1, \ldots, N_r \to \infty$ satisfying the conditions of the theorem. For any $y \in A$ we set

$$F(y) = \sum_{z\in\mathcal{N}}\psi(zy). \tag{63}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

Then (49) may be written as

$$\mathcal{E} = \frac{1}{N} \sum_{(0,0)\neq(y_1,y_2)} F(y_1)F(y_2) \sum_{a\in J} S(a, y_1, y_2). \tag{64}$$

Next, we bound $F(y_1)$, $F(y_2)$ and $S(a, y_1, y_2)$. Taking into account (63), (6) and the definition of ψ, we see that

$$\begin{aligned} F(y) &= \sum_{1\le n_1\le N_1} \cdots \sum_{1\le n_r\le N_r} \psi(n_1\beta_1 y + \cdots + n_r\beta_r y) \\ &= \prod_{1\le j\le r} \sum_{1\le n_j\le N_j} \psi(n_j\beta_j y) = \prod_{1\le j\le r} \sum_{1\le n_j\le N_j} e_q\big(n_j H(\beta_j y)\cdot v\big). \end{aligned} \tag{65}$$

The last sums from (65) are geometric progressions and can be estimated accurately. For any $j \in \{1, \dots, r\}$ and $y \in A$ let us denote by $L_j(y)$ the unique integer number in the interval $[-\frac{q-1}{2}, \frac{q-1}{2}]$ whose image in $\mathbf{Z}/q\mathbf{Z}$ coincides with $H(\beta_j y)\cdot v$. Then one has

$$\Big|\sum_{1\le n_j\le N_j} e_q\big(n_j H(\beta_j y)\cdot v\big)\Big| = \Big|\sum_{1\le n_j\le N_j} \exp\Big(\frac{2\pi i n_j L_j(y)}{q}\Big)\Big| \tag{66}$$

$$\begin{aligned} &\le \min\left\{N_j, \frac{2}{|1-\exp(\frac{2\pi i L_j(y)}{q})|}\right\} \\ &\le \min\left\{N_j, \frac{1}{|\sin\frac{\pi L_j(y)}{q}|}\right\} \\ &\le \min\left\{N_j, \frac{q}{|L_j(y)|}\right\}. \end{aligned} \tag{67}$$

As a result

$$|F(y)| \le \prod_{1\le j\le r} \min\left\{N_j, \frac{q}{|L_j(y)|}\right\} \tag{68}$$

for any $y \in A$. We now bound $S(a, y_1, y_2)$. By (44) and (42) we know that

$$S(a, y_1, y_2) = p^{-2sr} \sum_{\substack{w_1,w_2\in A \\ w_1^2-w_2^2=au^{-1}}} \psi(-y_1w_1 - y_2w_2). \tag{69}$$

Here we change the variables to $w_1 = -x_1 - x_2$, $w_2 = x_2 - x_1$ and get

$$\begin{aligned} S(a, y_1, y_2) &= p^{-2sr} \sum_{\substack{x_1,x_2\in A \\ x_1x_2=a(4u)^{-1}}} \psi\big(x_1(y_1+y_2) + x_2(y_1-y_2)\big) \\ &= p^{-2sr} T\big(y_1+y_2, y_1-y_2, a(4u)^{-1}\big). \end{aligned} \tag{70}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

Let l, m be the largest integers $\leq s$ for which $y_1, y_2 \in p^l A$ and $a \in p^m A$. Note that l is also the largest integer $\leq s$ for which $y_1 + y_2, y_1 - y_2 \in p^l A$. Then Lemma 3 implies

$$|S(a, y_1, y_2)| \leq 2rsp^{\frac{(-3s+l+m+5)r}{2}}. \tag{71}$$

We now bound the inner sum on the right side of (64). Let m_0 be the largest integer for which $J \cap p^{m_0} A$ is nonempty. Then

$$\Big|\sum_{a\in J} S(a, y_1, y_2)\Big| \leq \sum_{0\leq m\leq m_0} \sum_{a\in J\cap(p^m A\setminus p^{m+1}A)} |S(a, y_1, y_2)|. \tag{72}$$

Choose $c_I > 0$ such that I is contained in the cube $[-c_I, c_I]^r$. Then if we select an element $t \in J \cap p^{m_0} A$, $t = t_1\beta_1 + \cdots + t_r\beta_r$ then $|t_1|, \ldots, |t_r| \leq \frac{c_I q}{N^{1/r}}$, and $t_1, \ldots, t_r$ are integers divisible by p^{m_0}, not all zero. It follows that $p^{m_0} \leq \frac{c_I q}{N^{1/r}}$. This, together with (55) show that for any $m \in \{0, 1, \ldots, m_0\}$ one has

(73)

$$\begin{aligned}\#\big(J \cap (p^m A \setminus p^{m+1}A)\big) &\leq \#(J \cap p^m A)\\ &= \frac{q^r}{Np^{rm}}\,\mathrm{Vol}(I) + O_{r,I}(1 + q^{r-1}N^{\frac{1-r}{r}}p^{(1-r)m}) \ll_{r,I} \frac{q^r}{Np^{rm}}.\end{aligned}$$

Using (71) and (73) in (72) we derive

$$\begin{aligned}\Big|\sum_{a\in J} S(a, y_1, y_2)\Big| &\leq \sum_{0\leq m\leq m_0} 2rsp^{\frac{(-3s+l_{y_1,y_2}+m+5)r}{2}} \#(J \cap p^m A)\\ &\ll_{r,I} \frac{sp^{\frac{(-3s+l_{y_1,y_2}+5)r}{2}} q^r}{N} \sum_{0\leq m\leq m_0} p^{-\frac{rm}{2}} \ll \frac{sp^{\frac{(-s+l_{y_1,y_2}+5)r}{2}}}{N}\end{aligned} \tag{74}$$

where l_{y_1,y_2} is the largest integer $\leq s$ for which $y_1, y_2 \in p^{l_{y_1,y_2}} A$. Employing (74) in (64) one obtains

$$|\mathcal{E}| \ll_{r,I} \frac{sp^{\frac{(-s+5)r}{2}}}{N^2} \sum_{(0,0)\neq(y_1,y_2)} |F(y_1)F(y_2)| p^{\frac{rl_{y_1,y_2}}{2}}. \tag{75}$$

We now insert (68) in (75) and get

(76)

$$|\mathcal{E}| \ll_{r,I} \frac{sp^{\frac{(-s+5)r}{2}}}{N^2} \sum_{(0,0)\neq(y_1,y_2)} p^{\frac{rl_{y_1,y_2}}{2}} \prod_{1\leq j\leq r} \min\Big\{N_j, \frac{p^s}{|L_j(y_1)|}\Big\} \min\Big\{N_j, \frac{p^s}{|L_j(y_2)|}\Big\}$$

Let us remark that the map from A to $\{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}^r$ given by $y \mapsto \big(L_1(y), \ldots, L_r(y)\big)$ is one-to-one. Indeed, if $y', y'' \in A$ are such that $L_j(y') = L_j(y'')$ for any j, then if we set $y = y' - y''$, we have $L_j(y) = 0$, $1 \leq j \leq r$. In

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

other words, one has $H(\beta_j y)\cdot \nu = 0$ in $\mathbf{Z}/q\mathbf{Z}$ for any j. Then any linear combination $w = n_1\beta_1 + \cdots + n_r\beta_r$ with $n_1, \ldots, n_r \in \mathbf{Z}$ satisfies $H(wy)\cdot\nu = 0$. These linear combinations cover the entire ring A. If $y \neq 0$ then there exists $w \in A$ such that $wy = \pi^{se-1}$ and we get a contradiction since $H(\pi^{se-1})\cdot\nu \neq 0$ in $\mathbf{Z}/q\mathbf{Z}$. Hence the above map is one-to-one. Let now $l_1, \ldots, l_{2r} \in \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$, not all zero. Then there is a unique pair $(0,0) \neq (y_1, y_2) \in A \times A$ for which $L_j(y_1) = l_j$, $L_j(y_2) = l_{r+j}$, $1 \leq j \leq r$. Let p^m be the greatest common divisor of $q, l_1, \ldots, l_{2r}$. Then not all the numbers $p^{s-m-1}l_1, \ldots, p^{s-m-1}l_{2r}$ are divisible by q. It follows that at least one of $p^{s-m-1}y_1, p^{s-m-1}y_2$ is not zero in A. This means that at least one of y_1, y_2 does not lie in $p^{m+1}A$. Thus $l_{y_1,y_2} \leq m$, and hence the factor $p^{\frac{rl_{y_1,y_2}}{2}}$ on the right side of (76) is bounded by $p^{\frac{rm}{2}}$. We deduce that

$$|\mathcal{E}| \ll_{r,I} \frac{sp^{\frac{(-s+5)r}{2}}}{N^2} \sum_{0\leq m<s} \sum_{\substack{|l_1|,\ldots,|l_{2r}|\leq \frac{q-1}{2} \\ (q,l_1,\ldots,l_{2r})=p^m}} p^{\frac{rm}{2}} \prod_{1\leq j\leq 2r} \min\{N_j, \frac{p^s}{|l_j|}\} \tag{77}$$

where we set $N_{j+r} := N_j$ for $1 \leq j \leq r$. For any $l_1, \ldots, l_{2r} \in \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$ denote $\mathcal{C}(l_1, \ldots, l_{2r}) = \{1 \leq j \leq 2r : l_j \neq 0\}$. We take each nonempty subset $\mathcal{C}$ of $\{1, \ldots, 2r\}$ and collect all those terms from the right side of (77) for which $\mathcal{C}(l_1, \ldots, l_{2r}) = \mathcal{C}$. We derive

$$|\mathcal{E}| \ll_{r,I} \frac{sp^{\frac{(-s+5)r}{2}}}{N^2} \sum_{0\leq m<s} \sum_{\Phi\neq\mathcal{C}\subseteq\{1,\ldots,2r\}} \sum_{\substack{0<|l_j|\leq\frac{q-1}{2}, j\in\mathcal{C} \\ p^m|l_j}} \frac{p^{\frac{rm}{2}+s\#(\mathcal{C})}\prod_{j\notin\mathcal{C}} N_j}{\prod_{j\in\mathcal{C}}|l_j|}$$

If we write $l_j = p^m l_j'$ for $j \in \mathcal{C}$ and note that

$$\sum_{l_j', j\in\mathcal{C}} \frac{1}{|l_j'|} \ll_r (\log q)^{\#(\mathcal{C})} \leq \log^{2r} q = s^{2r}\log^{2r} p,$$

and $p^{5r/2} = O(1)$, then we see that

$$\begin{aligned} |\mathcal{E}| &\ll_{r,I,p} \frac{s^{2r+1}p^{-\frac{sr}{2}}}{N^2} \sum_{0\leq m<s} \sum_{\Phi\neq\mathcal{C}\subseteq\{1,\ldots,2r\}} p^{\frac{rm}{2}+(s-m)\#(\mathcal{C})} \prod_{j\notin\mathcal{C}} N_j \\ &= \frac{s^{2r+1}p^{-\frac{sr}{2}}}{N^2} \sum_{\Phi\neq\mathcal{C}\subseteq\{1,\ldots,2r\}} p^{s\#(\mathcal{C})} \prod_{j\notin\mathcal{C}} N_j \sum_{0\leq m<s} p^{(\frac{r}{2}-\#(\mathcal{C}))m}. \end{aligned} \tag{78}$$

Here the inner sum is bounded by $s\max\{1, p^{(\frac{r}{2}-\#(\mathcal{C}))s}\}$, hence

$$\begin{aligned} |\mathcal{E}| &\ll_{r,I,p} \frac{s^{2r+2}p^{-\frac{sr}{2}}}{N^2} \sum_{\Phi\neq\mathcal{C}\subseteq\{1,\ldots,2r\}} \max\{p^{s\#(\mathcal{C})}, p^{\frac{rs}{2}}\} \prod_{j\notin\mathcal{C}} N_j \\ &= s^{2r+2} \sum_{\Phi\neq\mathcal{C}\subseteq\{1,\ldots,2r\}} \frac{p^{s\max\{\#(\mathcal{C})-\frac{r}{2},0\}}}{\prod_{j\in\mathcal{C}} N_j}. \end{aligned} \tag{79}$$

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press

Since $\prod_{j\in\mathcal{C}} N_j \geq q^{\delta} = p^{s\delta}$ for any $\Phi \neq \mathcal{C}$, it follows that the contribution on the right side of (79) of those $\mathcal{C}$ with $\#(\mathcal{C}) \leq \frac{r}{2}$ is $\ll s^{2r+2}/p^{s\delta}$. For any $\frac{r}{2} < l \leq 2r$ denote $\tilde{N}_l = \min\{\prod_{j\in\mathcal{C}} N_j : \mathcal{C} \subseteq \{1,\dots,2r\}, \#(\mathcal{C}) = l\}$. Then

$$|\mathcal{E}| \ll_{r,I,p} \frac{s^{2r+2}}{p^{s\delta}} + s^{2r+2} \max_{\frac{r}{2}<l\leq 2r} \frac{p^{s(l-\frac{r}{2})}}{\tilde{N}_l}. \tag{80}$$

For any $\mathcal{C}$ one has

$$\prod_{j\in\mathcal{C}} N_j = \frac{N^2}{\prod_{j\notin\mathcal{C}} N_j} \geq \frac{N^2}{\prod_{j\notin\mathcal{C}} p^s} = N^2 p^{s(\#(\mathcal{C})-2r)}$$

and so

$$\tilde{N}_l \geq N^2 p^{s(l-2r)} \tag{81}$$

for any l. On combining (80) with (81) we conclude that

$$|\mathcal{E}| \ll_{r,I,p} \frac{s^{2r+2}}{p^{s\delta}} + s^{2r+2} \max_{\frac{r}{2}<l\leq 2r} \frac{p^{s(l-\frac{r}{2})}}{N^2 p^{s(l-2r)}} = \frac{s^{2r+2}}{p^{s\delta}} + \frac{s^{2r+2} p^{\frac{3rs}{2}}}{N^2}. \tag{82}$$

Now (62) follows since $N \geq q^{\frac{3r}{4}+\delta}$, which completes the proof of Theorem 1.

References

[1] F. Boca and A. Zaharescu, *Pair correlation of values of rational functions* (mod p). Duke Math. J. (2) **105**(2000), 267–307.

[2] H. Davenport, *On a principle of Lipschitz*. J. London Math. Soc. **26**(1951), 179–183. Corrigendum: On a principle of Lipschitz, J. London Math. Soc. **39**(1964), 580.

[3] T. Estermann, *On Kloosterman's sum*. Mathematika **8**(1961), 83–86.

[4] P. Kurlberg, *The distribution of spacings between quadratic residues. II*. Israel J. Math. (A) **120**(2000), 205–224.

[5] P. Kurlberg and Z. Rudnick, *The distribution of spacings between quadratic residues*. Duke Math. J. **100**(1999), 211–242.

[6] Z. Rudnick and P. Sarnak, *The pair correlation function of fractional parts of polynomials*. Comm. Math. Phys. (1) **194**(1998), 61–70.

[7] Z. Rudnick, P. Sarnak and A. Zaharescu, *The distribution of spacings between the fractional parts of* $n^2\alpha$. Invent. Math. (1) **145**(2001), 37–57.

[8] S. Salié, *Über die Kloostermanschen Summen* $S(u, v, q)$. Math. Z. **34**(1931), 91–109.

[9] A. Zaharescu, *Correlation of fractional parts of* $n^2\alpha$. to appear in Forum Math.

Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, Illinois 61801
USA.
e-mail: zaharesc@math.uiuc.edu

https://doi.org/10.4153/CJM-2003-019-6 Published online by Cambridge University Press