A QUESTION ON THE DISTRIBUTION OF POINTS ON A CURVE OVER A FINITE FIELD

by
Cristian Cobeli and Alexandru Zaharescu

Abstract. Let C be an affine curve in the affine space $A^r\left(\overline{F_p}\right)$ that is not contained in any hyperplane. We show that there exists a probability that measures the set of points $x \in C$ satisfying given size restrictions for the spacings between neighbor components.

2000 Mathematics Subject Classification. 11T99.

1. Introduction

It is generally known that the properties of points on a curve depend highly on their domain of definition. In particular, there is a big contrast between curves over R or C ,where continuity makes the law, and curves over a finite field, where statistical properties govern. This makes intuition in the second case to be mostly led by proportions and numbers. We start by looking at two recently proved results of this sort.

Given an integer $n \geq 2$, for any a relatively prime to $n, 1 \leq a \leq n-1$, let $\overline{a}$ be the inverse of a modulo n. This is the unique integer $n, 1 \leq \overline{a} \leq n-1$ that satisfies $a\overline{a} \equiv 1(1 \bmod n)$. For any real number $\delta \in (0,1]$ and integer $n \geq 2$, let *D(n)* denote the number of invertible residue classes (mod *n*) that are not more than δn further away from their inverse, that is

$$D(n) = \#\left\{a : 1 \leq a \leq n-1, (a,n) = 1, \left|a - \overline{a}\right| < \delta n\right\}$$

In [5] Wenpeng Zhang studied the behavior of $\left|a-\overline{a}\right|$ and he proved that for any $n \geq 2$ and any $0 < \delta \leq 1$ one has

$$D(n) = \delta(2-\delta)\varphi(n) + O\left(n^{1/2} d^2(n) \log^3 n\right) \qquad (1)$$

where $\varphi(n)$ is the Euler function and $d(n)$ denotes the number of divisors of *n*. As a conse-quence, we have $\lim_{n\to\infty} \frac{D(n)}{\varphi(n)} = \delta(2-\delta)$, for any $0 < \delta \leq 1$. At the same time, in [6] Zhiyong Zheng investigated the before-mentioned problem, with $\left(a, \overline{a}\right)$ replaced by a pair (x, y)sat-isfying a more general congruence. Precisely, let p be a prime number and let $f(x, y)$be a polynomial with integer coefficients of total degree $d \geq 2$, absolutely irreducible modulo p, and denote

$$D_f(p)=\#\{(x,y)\in Z^2 : 0\le x,y<p,\ f(x,y)\equiv 0(\mathrm{mod}\ p), |x-y<\delta p|\}$$

Then, it is proved in [6] that, for any $0\le\delta\le 1$, one has:

$$D_f(p)=\delta(2-\delta)p+O_d\left(p^{\frac{1}{2}}\log^2 p\right) \qquad (2)$$

This shows that the proportions of points $(x,y)\in(Z/pZ)^2$ with $f(x,y)\equiv 0(\mathrm{mod}\ p)$ and
$|x-y|<\delta p$ approaches $\delta(2-\delta)$, the same as in the case of the inverses. One should expect
this sort of result to be true in higher dimensions and this is the object of our investigation
in what follows.

2. Notations and Statement of Results

In this paper we study a similar question in the more general case of an affine curve *C* of degree *d* in a higher dimensional affine space $A^r\left(\overline{F_p}\right)$, where $\overline{F_p}$ denotes the algebraic closure of $F_p=Z/pZ$. It turns out that, as in the case of a plane curve treated by Zhiyong Zheng, the limiting distribution depends only on the dimension *r* of the space and not on the particular shape of the curve. In what follows we shall assume that *C* is absolutely irreducible, it is defined over F_p and it is not contained in any hyperplane. We consider the set

$$N_{r,p,C}=\{x=(x_1,\ldots,x_r)\in Z^r : 0\le x_1,\ldots,x_r<p,\ x(\mathrm{mod}\ p)\in C\}$$

For any $x\in N_{r,p,C}$ denote by $\tilde{x}=(\tilde{x}_1,\ldots\tilde{x}_{r-1})\in R^{r-1}$ the point whose coordinates are the normalized differences

$$\tilde{x}_i=\frac{x_{i+1}-x_i}{p} \text{ for } i=1,\ldots,r-1$$

In order to study the distribution in R^{r-1} of the set

$$\tilde{N}_{r,p,C}:=\{\tilde{x} : x\in N_{r,p,C}\},$$

we introduce the probability measure

$$\mu_{r,p,C}=\frac{1}{|N_{r,p,C}|}\sum_{x\in N_{r,p,C}}\delta_{\bar{x}}$$

where $\delta_{\tilde{x}}$ is a unit point delta mass at $\tilde{x}$. Another measure, maybe more natural in higher dimensions, has been introduced and studied in [2]. The measure $\mu_{r,p,C}$ defined above also leads to a generalization of the result of Zhiyong Zheng. The first question we pose is whether
for any given $r \geq 2$ there is a probability measure μ_{r-1} on R^{r-1} such that $\mu_{r,p,C}$ converges weakly to μ_{r-1} as $p \to \infty$ while d remains bounded and C is as above. Such a probability measure exists indeed, as follows from the next theorem. Moreover, we show that μ_{r-1} is absolutely continuous with respect to the Lebesgue measure and we provide an explicit formula for the density g_{r-1} of μ_{r-1}. In order to do this, we take a nice subset Ω of R^{r-1} , say is a bounded domain whose boundary is piecewise smooth, and study the behavior of $\mu_{r,p,C}(\Omega)$ as p gets large and C is a curve over F_p absolutely irreducible and not contained in
any hyperplane. Our main result is contained in the following theorem.

Theorem 1. Let $r \geq 2$, $d > 0$ be integers and let p be a prime. Let C be an irreducible algebraic curve in $A^r(\overline{F}_p)$ that is defined over F_p, assume that the degree of C is $\leq d$ and C
is not contained in any hyperplane of $A^r(\overline{F}_p)$. Then

$$\mu_{r,p,C}(\Omega) = \int \underset{\Omega}{\dots} \int g_{r-1}(t_1,\dots,t_{r-1})\, dt_1 \dots dt_{r-1} + O_{r,d,\Omega}\left(p^{-\frac{1}{2(r+1)}} \log^{\frac{r}{r+1}} p \right) \qquad (3)$$

in which

$$g_{r-1}(t_1,\dots,t_{r-1}) = \max\{0, \min\{1, 1-t_1, \dots, 1-(t_1+\dots+t_{r-1})\} + \min\{0, t_1, \dots, (t_1+\dots+t_{r-1})\}\} \qquad (4)$$

As a consequence we immediately obtain the stated result.

Corollary 1. Let $r \geq 2$, $d > 0$ be integers, and let $\{p_j\}_{j\geq 1}$ be an increasing sequence of
primes. Let $\{C_j\}_{j\geq 1}$ be a sequence of curves such that for each $j \geq 1$ the following conditions
hold: C_j is an irreducible algebraic curve in $A^r(\overline{F}_{p_j})$, C_j is defined over F_{p_j}, the degree of C_j is $\leq d$, and C_j is not contained in any hyperplane of $A^r(\overline{F}_{p_j})$. Then the sequence of probability measures $\{\mu_{r,p_j,C_j}\}_{j\geq 1}$ converges weakly to the probability measure μ_{r-1} with density g_{r-1} given by (4).

In the particular case when $r=2$ and $\Omega=(-\delta,\delta)$ with $0\le\delta\le1$, Theorem 1 says that if $p\to\infty$ and C is irreducible but it is not a straight line, then a point $(x,y)\in C$, with
$0\le x,y<p$ satisfies the inequality $|x-y|<\delta p$ with probability

$$\mu_1(\Omega)=\int_{-\delta}^{\delta} g_1(t)\,dt\,.$$

By (4) the density is given by

$$\begin{aligned} g_1(t) &= \max\left\{0,\ \min\{1,\ 1-t\}+\min\{0,\ t\}\right\} \\ &= \begin{cases} \max\{0,\ 1-t\}, & \text{if } t\ge 0, \\ \max\{0,\ 1+t\}, & \text{if } t<0, \end{cases} \\ &= \begin{cases} 1-|t|, & \text{if } |t|\le 1, \\ 0, & \text{else}, \end{cases} \end{aligned}$$

therefore

$$\mu_1(\Omega)=\int_{-\delta}^{\delta}(1-|t|)\,dt=2\delta-\delta^2.$$

which is in accord with the estimations (1) and (2) above.
Let us see our result in three dimensions also. Suppose $\Omega=(-\delta,\delta)\times(-\delta,\delta)$, where $0\le\delta\le1$. Then, by Theorem 1 we find that when $p\to\infty$, a point $(x,y,z)\in C$ with coordinates $0\le x,y,z<p$ is in the square section tube defined by $|x-y|<\delta p$, $|y-z|<\delta p$
with probability $\mu_2(\Omega)$. Moreover μ_2 has a density $g_2(u,v)$, and by (4) we know that this is

$$g_2(u,v)=\max\left\{0,\ \min\{1,\ 1-u,\ 1-u-v\}+\min\{0,\ u,\ u+v\}\right\}$$

A straightforward calculation shows that the support of $g_2(u,v)$ is the hexagon *ABCDEF*

with vertices: $A = (1, 0)$; $B = (0, 1)$; $C = (-1, 1)$; $D = (-1, 0)$; $E = (0, -1)$; $F = (1, -1)$,
and if we put $O = (0, 0)$, then

$$g_2(u,v) = \begin{cases} 1-u-v, & \text{if } (u,v) \in \triangle ABO, \\ 1-v, & \text{if } (u,v) \in \triangle BCO, \\ 1+u, & \text{if } (u,v) \in \triangle CDO, \\ 1+u+v, & \text{if } (u,v) \in \triangle DEO, \\ 1+v, & \text{if } (u,v) \in \triangle EFO, \\ 1-u, & \text{if } (u,v) \in \triangle FAO, \\ 0, & \text{otherwise.} \end{cases}$$

This yields

$$\mu_2(\Omega) = \iint\limits_{(-\delta,\delta)\times(-\delta,\delta)} g_2(u,v)\,dudv = \begin{cases} \frac{2}{3}\delta^2(-5\delta+6), & \text{if } 0 \le \delta \le \frac{1}{2}, \\ \frac{1}{3}(-2\delta^3+6\delta-1), & \text{if } \frac{1}{2} \le \delta \le 1. \end{cases}$$

If one compares the error terms from the estimations (1) or (2) with that from (3) one might argue that Theorem 1 is weaker in the case $r = 2$. This apparent weakness is due to the shape of the more general domain Ω for which Theorem 1 applies. In fact, as we will see at the end of the article, our method of proof is exible enough and can be adapted to get a smaller error term (of square root type) for finer domains. In particular one recovers (2) completely.

3. Proof of Theorem 1

The proof of Theorem 1 is similar to the proof of Theorem 1 from [2], with appropriate modifications due to the fact that we work here with a different measure. For the sake of completeness, the proof with all details is presented below.

3.1. Embedding of $N_{r,p,C}$ into a cylinder. We embed $N_{r,p,C}$ into the cylinder $R \times \Omega \subset R^r$ through the map $(x_1,...,x_r) \mapsto (y,t_1,...,t_r)$, in which

$$y = \frac{x_1}{p},\ t_1 = \frac{x_2 - x_1}{p}, \dots, t_{r-1} = \frac{x_r - x_{r-1}}{p}$$

Then the system of inequalities $0 \le x_1,...,x_r < p$ in the definition of $N_{r,p,C}$ is equivalent to the system of inequalities

$$0 \le y,\ y + t + 1,\ y + t_1 + t_2,\ \dots,\ y + t_1 + \cdots + t_{r-1} < 1\,. \tag{5}$$

An important role in what follows will be played by the set

$$\Omega^* := \{(y, t_1, \dots, t_r) \in \mathbb{R} \times \Omega:\ y,\, t_1, \dots, t_{r-1} \text{ satisfy } (5)\}$$

The basic idea is to view Ω^* in a net of cubes. Thus we split the region $p\Omega^*$ into cubes with edge equal to p/T, where *T* is a real parameter whose optimal value will be given later. Let *D (T)* be the union of such cubes that are included into $p\Omega^*$ and let *E(T)* be the union of those cubes that intersect $p\Omega^*$. Then we have

$$\mathcal{D}(T) \subseteq p\Omega^* \subseteq E(T)\,. \tag{6}$$

3.2. The problem in a cube.

Here we fix an arbitrary cube $J \subset R^r$ with edge p/T and estimate *N*(**J**), the number of points from $N_{r,p,C}$ that correspond to **J**, that is

$$N(\mathbf{J}) := \#\{\mathbf{x} \in \mathcal{N}_{r,p,\mathcal{C}}:\ (x_1, x_2 - x_1, \dots, x_r - x_{r-1}) \in \mathbf{J}\}\,.$$

Being a cube, **J** can be written as $\mathbf{J} = J_1 \times ... \times J_r$, which allows us to write

$$N(\mathbf{J}) = \sum_{\mathbf{x}\,(\mathrm{mod}\ \mathbf{p}) \in \mathcal{C}} \chi_{\mathcal{J}_1}(x_1)\chi_{\mathcal{J}_2}(x_2 - x_1)\cdots\chi_{\mathcal{J}_r}(x_r - x_{r-1})\,, \tag{7}$$

where $\chi_J(x)$ is the characteristic function of the interval J. We write $\chi_J(x)$ in a convenient form in terms of additive characters:

$$\chi_{\mathcal{J}}(x) = \sum_{y \in \mathcal{J}} \frac{1}{p} \sum_{k\,(\mathrm{mod}\ p)} e_p\big(k(x-y)\big)\,. \tag{8}$$

(We use Vinogradov's notation $e_p(x) = e^{\frac{2\pi i x}{p}}$.) Using (8) and changing the order of summa-
tion (7) becomes

$$N(\mathbf{J}) = \frac{1}{p^r} \sum_{k_1 \pmod p} \cdots \sum_{k_r \pmod p} \prod_{j=1}^{r} \left(\sum_{y_j \in \mathcal{J}_j} e_p(-k_j y_j) \right) S_{\mathbf{k}}(\mathbf{x}), \tag{9}$$

where k = $(k_1, \ldots, k_r)$,

$$\mathcal{L}_{\mathbf{k}}(\mathbf{x}) = (k_1 - k_2)x_1 + (k_2 - k_3)x_2 + \cdots + (k_{r-1} - k_r)x_{r-1} + k_r x_r \,,$$

and

$$S_{\mathbf{k}}(\mathbf{x}) = S_{\mathbf{k},p,r,\mathcal{C}}(\mathbf{x}) = \sum_{\mathbf{x} \pmod p \in \mathcal{C}} e_p\big(\mathcal{L}_{\mathbf{k}}(\mathbf{x})\big)\,.$$

Since $L_k(x)$ is a linear form and by hypothesis C is not contained in any hyperplane, it follows that $L_k(x)$ is constant along C if and only if k1 = ··· = kr = 0. We will see that the sum of the terms with k1 = ··· = kr = 0 add up to the main term in our estimation for N(J), while the remaining terms cancel each other into a lower order error term. These terms will be denoted by *M(**J**)* and *E(**J**)* respectively. Thus we have:

$$N(\mathbf{J}) = M(\mathbf{J}) + E(\mathbf{J})\,. \tag{10}$$

3.3. The Main Term. By definition we know that

$$\begin{aligned} M(\mathbf{J}) &= \frac{1}{p^r} \prod_{j=1}^{r} \Big(|\mathcal{J}_j| + O(1) \Big) \sum_{\mathbf{x} \pmod p \in \mathcal{C}} 1 \\ &= \frac{1}{p^r} \mathrm{Vol}(\mathbf{J}) |\mathcal{C}(\mathbf{F}_p)| \left(1 + O_r\left(\frac{T}{p}\right) \right). \end{aligned}$$

The Riemann Hypothesis for curves over finite fields (Weil [4]) gives:

$$|\mathcal{C}(\mathbf{F}_p)| = p + O_{r,d}(\sqrt{p}). \tag{11}$$

Then, assuming that $T \le \sqrt{p}$, we obtain

$$M(\mathbf{J}) = \frac{1}{p^r}\mathrm{Vol}(\mathbf{J})|\mathcal{C}(\mathbf{F}_p)|\left(1 + O_{r,d}\Big(\frac{1}{\sqrt{p}}\Big)\right). \tag{12}$$

3.4. The Error Term. We now estimate the remainder. This equals

$$E(\mathbf{J}) = \frac{1}{p^r}\sum_{\mathbf{k}\,(\mathrm{mod}\ p)}{}' \prod_{j=1}^{r}\left(\sum_{y_j\in\mathcal{J}_j} e_p\left(-k_j y_j\right)\right) S_{\mathbf{k}}(\mathbf{x})\,,$$

where the prime means that the terms with $k_1 = ... = k_r = 0$ are left out in the summation.
Since each of the factors of the product over j with 1 # j # r is a geometric progression, it can be estimated precisely. One has

$$\left|\sum_{y_j\in\mathcal{J}_j} e_p\left(-k_j y_j\right)\right| \le \min\left\{|\mathcal{J}_j|, \frac{2}{|1-e_p(k_j)|}\right\} \le \min\left\{|\mathcal{J}_j|, \frac{1}{\left|\sin\frac{\pi k_j}{p}\right|}\right\}$$
$$\le \min\left\{|\mathcal{J}_j|, \frac{1}{2\left\|\frac{k_j}{p}\right\|}\right\},$$

where $\|\cdot\|$ denotes the distance to the nearest integer. This gives immediately

$$|E(\mathbf{J})| \le \frac{1}{p^r}\sum_{\mathbf{k}\,(\mathrm{mod}\ p)}{}' \prod_{j=1}^{r}\left(\min\left\{p, \frac{p}{|k_j|}\right\}\right)|S_{\mathbf{k}}(\mathbf{x})|$$
$$\ll_r \sum_{\mathbf{k}\,(\mathrm{mod}\ p)}{}' \frac{1}{1+|k_1|}\cdots\frac{1}{1+|k_r|}|S_{\mathbf{k}}(\mathbf{x})|\,.$$

For each $\mathbf{k} \neq \mathbf{0}$ our hypotheses on C allow us to apply the Bombieri-Weil inequality (see [1,Theorem 6, p. 97]), which shows that $S_k(x) = O_{r,d}(p^{1/2})$. We derive

$$|E(\mathbf{J})| = O_{r,d}\left(p^{\frac{1}{2}}\log^r p\right). \tag{13}$$

3.5. Finishing the Proof. By combining (12) and (13) we obtain

$$N(\mathbf{J}) = \frac{\mathrm{Vol}(\mathbf{J})}{p^{r-1}} + O_{r,d}\left(p^{\frac{1}{2}} \log^r p\right) . \tag{14}$$

By the Lipschitz principle on the number of integer points in an r - dimensional domain (see Davenport [3]) it follows that $\mathrm{Vol}(E(T) \setminus D(T)) \ll_s T^{s-1}$. This shows that both D (T) and E(T) are unions of $T^r \mathrm{Vol}(\Omega^*) + O_{\Omega,r}(T^{r-1})$ cubes with edge equal to p/T since only $O_{\Omega,r}(T^{r-1})$ of them intersect E(Σ) \ D (T). Then, since

$$\mathrm{Vol}(\mathcal{D}(T)) = \mathrm{Vol}(p\Omega^*) + O_{r,\Omega}\left(T^{r-1}\mathrm{Vol}(\mathbf{J})\right)$$

and

$$\mathrm{Vol}(E(T)) = \mathrm{Vol}(p\Omega^*) + O_{r,\Omega}\left(T^{r-1}\mathrm{Vol}(\mathbf{J})\right) ,$$

by the definition and (6) we obtain

$$\begin{aligned}\#\left\{\mathbf{x} \in \mathcal{N}_{r,p,\mathcal{C}} :\ \tilde{\mathbf{x}} \in \Omega\right\} &= \frac{\mathrm{Vol}(p\Omega^*)}{p^{r-1}} + O_{r,d,\Omega}\left(T^r p^{\frac{1}{2}} \log^r p\right) + O_{r,\Omega}\left(T^{r-1}\frac{\mathrm{Vol}(\mathbf{J})}{p^{r-1}}\right) \\ &= p\mathrm{Vol}(\Omega^*) + O_{r,d,\Omega}\left(T^r p^{\frac{1}{2}} \log^r p\right) + O_{r,d,\Omega}\left(\frac{p}{T}\right) .\end{aligned} \tag{15}$$

We now turn to the probability

$$\mu_{r,p,\mathcal{C}}(\Omega) = \frac{\#\left\{\mathbf{x} \in \mathcal{N}_{r,p,\mathcal{C}} :\ \tilde{\mathbf{x}} \in \Omega\right\}}{|\mathcal{N}_{r,p,\mathcal{C}}|} .$$

By (11) it follows that $\left|N_{r,p,C}\right| = p + O_{r,d}(p^{1/2})$ Therefore, by (15) we find that

$$\mu_{r,p,\mathcal{C}}(\Omega) = \mathrm{Vol}(\Omega^*) + O_{r,d,\Omega}\left(T^r p^{-\frac{1}{2}} \log^r p\right) + O_{r,d,\Omega}\left(\frac{1}{T}\right) . \tag{16}$$

The optimal value of T that balances the big-O terms in (16) is $T = p^{\frac{1}{2(r+1)}} \log^{-\frac{r}{r+1}} p$. This gives

$$\mu_{r,p,\mathcal{C}}(\Omega) = \mathrm{Vol}(\Omega^*) + O_{r,d,\Omega}\left(p^{-\frac{1}{2(r+1)}} \log^{\frac{1}{r+1}} p\right).$$

The final touches of the proof require to explicitly compute $Vol(\Omega^*)$. By definition Ω^* is a
cylinder based on Ω and it is situated between two hypersurfaces. Thus

$$\Omega^* = \left\{(y, t_1, t_2, \ldots, t_{r-1}) \in \mathbb{R}^r : \ (t_1, \ldots, t_r) \in \Omega,\ h(t_1, \ldots, t_r) \le y \le H(t_1, \ldots, t_r)\right\},$$

say. This gives

$$\mathrm{Vol}(\Omega^*) = \int_{\Omega}\cdots\int \max\left\{0,\ H(t_1, \ldots, t_r) - h(t_1, \ldots, t_r)\right\} dt_1 \cdots dt_{r-1}.$$

Finally, by (5) we obtain

$$\begin{aligned} h(t_1, \ldots, t_r) &= \max\left\{0,\ -t_1,\ \ldots,\ -(t_1 + \cdots + t_{r-1})\right\} \\ &= \min\left\{0,\ t_1,\ \ldots,\ (t_1 + \cdots + t_{r-1})\right\} \end{aligned}$$

and

$$H(t_1, \ldots, t_r) = \min\left\{1,\ 1 - t_1,\ \ldots,\ 1 - (t_1 + \cdots + t_{r-1})\right\},$$

which concludes the proof of Theorem 1.

4. A better error term for finer Ω

One can see that the error term in the asymptotic formula from Theorem 1 in the case $r = 2$ is not as sharp as the bounds for the error terms in (1) or (2). This is due to the price paid to get a result valid for a more general region Ω. Our method of proof is exible enough to accommodate finer regions, which allows for an improvement in the error term.
This was also seen in [2] for the corresponding probability therein.
We can recover the estimate (2), with exactly the same bound for the error term, by using only that part in our proof which is concerned with cubes. To see this we write the set

$$\left\{(x, y) \in R^2 : 0 \le x, y < p, |x - y| < \delta p\right\}$$

as the union of two parallelograms and a square.
This are:

$$\left\{(x,y)\in\mathbb{R}^2:\ \ 0\le y<(1-\delta)p,\ 0\le x-y<\delta p\right\},$$

$$\left\{(y,x)\in\mathbb{R}^2:\ \ 0\le x<(1-\delta)p,\ 0<y-x<\delta p\right\},$$

$$\left\{(x,y)\in\mathbb{R}^2:\ \ (1-\delta)p\le x,y<p\right\}.$$

This splits accordingly the counting of points. Thus we have:

$$\#\left\{(x,y)\in\mathbb{Z}^2:\ \ 0\le x,y<p,\ (x,y)\pmod p\in\mathcal{C},\ |x-y|<\delta p\right\}=\Sigma_1+\Sigma_2+\Sigma_3,$$

where

$$\Sigma_1=\sum_{(x,y)\pmod p\in\mathcal{C}}\chi_{[0,(1-\delta)p)}(y)\chi_{[0,\delta p)}(x-y),$$

$$\Sigma_2=\sum_{(x,y)\pmod p\in\mathcal{C}}\chi_{[0,(1-\delta)p)}(x)\chi_{(0,\delta p)}(y-x)$$

and

$$\Sigma_3=\sum_{(x,y)\pmod p\in\mathcal{C}}\chi_{[(1-\delta)p,p)}(x)\chi_{[(1-\delta)p,p)}(y).$$

Here each of the sums $\Sigma_1,\Sigma_2,\Sigma_3$ may be treated in the same way we have estimated the points in the cubes **J**, and one obtains asymptotic results with square root upper bounds for the error terms as in (14). By combining these results, (2) follows.

We remark that a similar procedure works also in higher dimensional spaces whenever Ω can be split in a finite number of parallelepipeds.

References

[1] E. Bombieri, On exponential sums in finite fields, Amer. J. Math. 88 (1966) , 71–105.
[2] C. Cobeli and A. Zaharescu, On the distribution of the Fp - points on an affine curve in r dimensions,
Acta Arith. 99 (2001), no. 4, 321–329.
[3] H. Davenport, On a principle of Lipschitz, J. London Math. Soc. 26 (1951), 179–183.

[4] A. Weil, Sur les Courbes Alg´ebriques et les Vari´et´es qui s'en D´eduisent, Hermann. Paris 1948.
[5] W. Zhang, On the distribution of inverses modulo n, J. Number Theory 61 (1996), no. 2, 301–310.
[6] Z. Zheng, The distribution of Zeros of an Irreducible Curve over a Finite Field, J. Number Theory 59
(1996), no. 1, 106–118.

Authors:

Cristian Cobeli
Institute of Mathematics of the Romanian Academy
P.O. Box 1-764
70700 Bucharest, Romania
e-mail: ccobeli@stoilow.imar.ro

Alexandru Zaharescu
Institute of Mathematics of the Romanian Academy
P.O. Box 1-764
70700 Bucharest, Romania
and
Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street, Urbana, IL 61801, USA.
e-mail: zaharesc@math.uiuc.edu