ACTA ARITHMETICA
XCIX.4 (2001)

On the distribution of the $\mathbf{F}_p$-points on an affine curve in r dimensions

by

Cristian Cobeli (Bucureşti) and
Alexandru Zaharescu (Bucureşti and Urbana, IL)

1. Introduction and statement of results. Let p be a prime number, $\overline{\mathbf{F}}_p$ the algebraic closure of $\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}$ and let $\mathcal{C}$ be an irreducible curve of degree d in an affine space $\mathbb{A}^r(\overline{\mathbf{F}}_p)$. We assume in the following that $\mathcal{C}$ is not contained in any hyperplane and that it is defined over $\mathbf{F}_p$. Our object in this paper is to study the distribution of the set $\mathcal{C}(\mathbf{F}_p)$ of $\mathbf{F}_p$-points on $\mathcal{C}$. We are interested in obtaining asymptotic results as p goes to infinity, while r is fixed, d is bounded and $\mathcal{C}$ is as above. In particular we would like to understand the distribution of distances between the coordinates of a point $\mathbf{x} = (x_1, \dots, x_r) \in \mathbf{F}_p^r$ which moves along the curve. Our original motivation for investigating these distances came from the problem of the distribution of $|a - \overline{a}|$, where $a, \overline{a}$ run over the set $\{1, \dots, p-1\}$ such that $a\overline{a} \equiv 1 \pmod p$. This problem was solved by Wenpeng Zhang [4] who proved that for any integer $n \geq 2$ and any $0 < \delta \leq 1$,

$$(1) \quad |\{a : \ 1 \leq a \leq n-1, \ (a,n) = 1, \ |a - \overline{a}| < \delta n\}| = \delta(2-\delta)\varphi(n) + O(n^{1/2} d^2(n) \log^3 n),$$

where $\varphi(n)$ is the Euler function and $d(n)$ denotes the number of divisors of n. In [5] Zhiyong Zheng investigated the same problem, with $(a, \overline{a})$ replaced by a pair (x, y) satisfying 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. Then it is proved in [5] that for any $0 < \delta \leq 1$,

$$(2) \quad |\{(x,y) \in \mathbb{Z}^2 : 0 \leq x, y < p, \ f(x,y) \equiv 0 \pmod p, \ |x - y| < \delta p\}| = \delta(2-\delta)p + O_d(p^{1/2} \log^2 p).$$

2000 *Mathematics Subject Classification*: Primary 11T99.

Returning to our context, we fix an $r \geq 2$, then choose a large prime number p and a curve $\mathcal{C}$ in $\mathbb{A}^r(\overline{\mathbf{F}}_p)$ as before. We view $\mathcal{C}(\mathbf{F}_p)$ as sitting in the torus $\mathbb{T}^r = \mathbb{R}^r/\mathbb{Z}^r$. Precisely, one has a natural injection $\mathbf{F}_p \to \mathbb{T} = \mathbb{R}/\mathbb{Z}$ defined as follows. Given $x \in \mathbf{F}_p$, choose a representative m of x in $\mathbb{Z}$ and then project $m/p \in \mathbb{R}$ to its image $t = t(x)$ in $\mathbb{T}$. Note that $t(x)$ does not depend on the choice of m. Then $\mathbf{F}_p^r$ injects in $\mathbb{T}^r$, a point $\mathbf{x} = (x_1, \dots, x_r) \in \mathbf{F}_p^r$ being sent to $t(\mathbf{x}) = (t(x_1), \dots, t(x_r)) \in \mathbb{T}^r$. To study the distribution of $\mathcal{C}(\mathbf{F}_p)$ in $\mathbb{T}^r$, consider the probability measure $\mu_{r,p,\mathcal{C}}$ on $\mathbb{T}^r$ defined by

$$\mu_{r,p,\mathcal{C}} = \frac{1}{|\mathcal{C}(\mathbf{F}_p)|} \sum_{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)} \delta_{t(\mathbf{x})},$$

where $\delta_{t(\mathbf{x})}$ is a unit point delta mass at $t(\mathbf{x})$. The first question one would ask about these measures is whether they converge to a certain measure on $\mathbb{T}^r$ as $p \to \infty$ and $\mathcal{C}$ is as before, say of bounded degree d. The answer is that they weakly converge to the (normalized) Haar measure μ on $\mathbb{T}^r$. Next, we would like to know how fast $\mu_{r,p,\mathcal{C}}(\Omega)$ approaches $\mu(\Omega)$ for a given nice domain Ω in $\mathbb{T}^r$, so that one could produce quantitative results for any large prime number p. We prove the following

THEOREM 1. *Let $r \geq 2$ be an integer and Ω a domain in $\mathbb{T}^r$ with piecewise smooth boundary. Then for any prime p and any irreducible curve $\mathcal{C}$ of degree d in $\mathbb{A}^r(\overline{\mathbf{F}}_p)$, defined over $\mathbf{F}_p$ and not contained in any hyperplane,*

$$\mu_{r,p,\mathcal{C}}(\Omega) = \mu(\Omega) + O_{r,d,\Omega}(p^{-1/(2(r+1))} \log^{r/(r+1)} p).$$

Next, we look at the distances between the coordinates $x_1, \dots, x_r$ of a point $\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)$. Consider the concrete problem of finding, for a given $\boldsymbol{\delta} = (\delta_1, \dots, \delta_{r-1}) \in \mathbb{R}^{r-1}$ with $0 < \delta_1, \dots, \delta_{r-1} \leq 1$, the proportion $\varrho_{r,p,\mathcal{C},\boldsymbol{\delta}}$ of points $\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)$ for which

$$|t(x_1) - t(x_r)| \leq \delta_1, \quad |t(x_2) - t(x_r)| \leq \delta_2, \ \dots, \ |t(x_{r-1}) - t(x_r)| \leq \delta_{r-1}.$$

The map from $\mathbb{R}^r$ to $\mathbb{R}^{r-1}$ given by $(y_1, \dots, y_r) \mapsto (y_1 - y_r, \dots, y_{r-1} - y_r)$ sends $\mathbb{Z}^r$ to $\mathbb{Z}^{r-1}$, and so it induces a map, call it ψ, from $\mathbb{T}^r$ to $\mathbb{T}^{r-1}$. Note that ψ is additive and it preserves the Haar measure:

$$\mu(U) = \mu(\psi^{-1}(U)) \tag{3}$$

for any open subset U of $\mathbb{T}^{r-1}$, where we denoted by μ the Haar measure on both $\mathbb{T}^r$ and $\mathbb{T}^{r-1}$. Let $U_{\boldsymbol{\delta}}$ be the image in $\mathbb{T}^{r-1}$ of the box $[-\delta_1, \delta_1] \times \dots \times [-\delta_{r-1}, \delta_{r-1}] \subset \mathbb{R}^{r-1}$. Assume $0 < \delta_1, \dots, \delta_{r-1} \leq 1/2$, then $\mu(U_{\boldsymbol{\delta}}) = 2^{r-1}\delta_1 \dots \delta_{r-1}$. By the definition of $\mu_{r,p,\mathcal{C}}$, ψ and $\varrho_{r,p,\mathcal{C},\boldsymbol{\delta}}$ one sees that

$$\varrho_{r,p,\mathcal{C},\boldsymbol{\delta}} = \mu_{r,p,\mathcal{C}}(\psi^{-1}(U_{\boldsymbol{\delta}})). \tag{4}$$

Using (4), (3) and Theorem 1 with $\Omega = \psi^{-1}(U_{\boldsymbol{\delta}})$ we obtain

$$\varrho_{r,p,\mathcal{C},\boldsymbol{\delta}} = 2^{r-1}\delta_1 \dots \delta_{r-1} + O_{r,d,\boldsymbol{\delta}}(p^{-1/(2(r+1))} \log^{r/(r+1)} p). \tag{5}$$

A more accurate version of (5) is stated in Corollary 1 from Section 4 below. In case $r = 2$, $\delta_1 = \delta$, from (5) one derives

$$\varrho_{r,p,\mathcal{C},\boldsymbol{\delta}} \sim 2\delta \quad \text{as } p \to \infty.$$

The reader noticed that this is different from the asymptotic result which follows from (2). The reason for this comes from the way the distance was defined: in (5) the distances are computed on the torus $\mathbb{T}$ while in (2) the set $\mathcal{C}(\mathbf{F}_p)$ is injected in a Euclidean space. Precisely, the points $(x, y) \in \mathbb{Z}^2$, $0 \le x, y < p$, $(x, y) \pmod p \in \mathcal{C}$ for which $|x-y-p| < \delta p$ or $|x-y+p| < \delta p$ do contribute to $\varrho_{r,p,\mathcal{C},\boldsymbol{\delta}}$, and they account for the difference δ^2 in the two asymptotic results. Actually one can recover a result of type (2) from Theorem 1 above, as follows. Fix a point $\mathbf{u} \in \mathbb{T}^r$ and choose a representative $\mathbf{v} = (v_1, \dots, v_r)$ of $\mathbf{u}$ in $\mathbb{R}^r$. Any $\mathbf{t} = (t_1, \dots, t_r) \in \mathbb{T}^r$ has a unique representative $(v_1 + y_1, \dots, v_r + y_r) \in \mathbb{R}^r$ with $0 \le y_1, \dots, y_r < 1$. We define the distances between the components of $\mathbf{t}$ *with respect to* $\mathbf{v}$, by

$$|t_i - t_j|_{\mathbf{v}} = |y_i - y_j|, \quad 1 \le i, j \le r.$$

These distances depend on $\mathbf{u}$ but not on the choice of $\mathbf{v}$, so we denote them by $|t_i - t_j|_{\mathbf{u}}$. Given a point $\mathbf{t} \in \mathbb{T}^r$ and two of its components $t_i, t_j \in \mathbb{T}$, there are two arcs in $\mathbb{T}$ which join the points t_i and t_j. For any $\mathbf{u} \in \mathbb{T}^r$ the distance $|t_i - t_j|_{\mathbf{u}}$ equals the length of one of these two arcs. Thus in some sense working with distances with respect to a fixed point $\mathbf{u} \in \mathbb{T}^r$ gives us a coherent way of choosing between the above two arcs associated to any pair (t_i, t_j), as $\mathbf{t}$ runs over $\mathbb{T}^r$. We now consider for a given $\mathbf{u} \in \mathbb{T}^r$ and a given $\boldsymbol{\delta} = (\delta_1, \dots, \delta_{r-1}) \in \mathbb{R}^{r-1}$ with $0 < \delta_1, \dots, \delta_{r-1} \le 1$, the proportion $\eta_{r,p,\mathcal{C},\mathbf{u},\boldsymbol{\delta}}$ of points $\mathbf{x} = (x_1, \dots, x_r) \in \mathcal{C}(\mathbf{F}_p)$ for which

$$|t(x_1) - t(x_r)|_{\mathbf{u}} \le \delta_1, \quad \dots, \quad |t(x_{r-1}) - t(x_r)|_{\mathbf{u}} \le \delta_{r-1}.$$

We remark that $\eta_{r,p,\mathcal{C},\mathbf{u},\boldsymbol{\delta}}$ does depend on $\mathbf{u}$. However, the fact that changing $\mathbf{u}$, that is, changing the lifting of $\mathbb{T}^r$ in $\mathbb{R}^r$ does not affect the Haar measure which is invariant under translations, together with the fact that $\mu_{r,p,\mathcal{C}}$ approaches the Haar measure as $p \to \infty$, make $\eta_{r,p,\mathcal{C},\mathbf{u},\boldsymbol{\delta}}$ converge to a limit which is independent of $\mathbf{u}$. To state our result, we introduce the following function $h : [0,1] \times [0,1] \to [0,1]$. For $0 \le z < 1/2$ we define

$$h(y,z) = \begin{cases} y + z & \text{if } 0 \le y < z, \\ 2z & \text{if } z \le y < 1 - z, \\ 1 - y + z & \text{if } 1 - z \le y \le 1. \end{cases}$$

For $1/2 \le z \le 1$ we let

$$h(y,z) = \begin{cases} y + z & \text{if } 0 \le y < 1 - z, \\ 1 & \text{if } 1 - z \le y < z, \\ 1 - y + z & \text{if } z \le y \le 1. \end{cases}$$

Next, for any $0 < \delta_1, \dots, \delta_{r-1} \le 1$ we set

$$c(\delta_1, \dots, \delta_{r-1}) = \int_0^1 \prod_{j=1}^{r-1} h(y, \delta_j)\, dy.$$

Then we prove the following result.

THEOREM 2. *Let $r \ge 2$ be an integer, $\mathbf{u} \in \mathbb{T}^r$, $\boldsymbol{\delta} = (\delta_1, \dots, \delta_{r-1}) \in \mathbb{R}^{r-1}$ with $0 < \delta_1, \dots, \delta_{r-1} \le 1$, p a prime number and $\mathcal{C}$ an irreducible curve of degree d in $\mathbb{A}^r(\overline{\mathbf{F}}_p)$, defined over $\mathbf{F}_p$ and not contained in any hyperplane. Then*

$$\eta_{r,p,\mathcal{C},\mathbf{u},\boldsymbol{\delta}} = c(\delta_1, \dots, \delta_{r-1}) + O_{r,d,\mathbf{u},\boldsymbol{\delta}}(p^{-1/(2(r+1))} \log^{r/(r+1)} p).$$

In particular, when $r = 2$ one has

$$c(\delta) = \int_0^1 h(y, \delta)\, dy = 2\delta - \delta^2$$

which agrees with (2).

Acknowledgements. The authors are grateful to Andrew Granville for suggesting the problem which led to Theorem 1 above. They are also grateful to the referee whose suggestions improved the presentation of the paper.

2. Proof of Theorem 1. Let $r, p, \mathcal{C}$ and Ω be as in the statement of the theorem. We split the torus $\mathbb{T}^r$ in little cubes with edge length $1/T$, where T is a positive integer. As we shall see later, the optimal choice for T in this proof is $T = [p^{1/(2(r+1))} \log^{-r/(r+1)} p]$. For each such cube $\mathbf{J}$ one has $\mu(\mathbf{J}) = T^{-r}$. We denote by $\mathcal{D}(T)$ the union of those cubes contained in Ω and by $E(T)$ the union of those cubes which have a nonempty intersection with Ω. Therefore

$$\mathcal{D}(T) \subseteq \Omega \subseteq E(T). \tag{6}$$

Now fix an arbitrary such cube $\mathbf{J}$ and estimate the number $N(\mathbf{J})$ of points $\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)$ for which $t(\mathbf{x}) \in \mathbf{J}$. Since $\mathbf{J}$ is a cube, there are subsets $J_1, \dots, J_r$ of $\mathbf{F}_p$ of the form $J_j = \{a_j + 1, a_j + 2, \dots, a_j + b_j\}$, $1 \le j \le r$, such that a point $\mathbf{x} \in \mathbf{F}_p^r$ lies in $J_1 \times \dots \times J_r$ if and only if $t(\mathbf{x}) \in \mathbf{J}$. The number of elements of J_j is

$$\#(J_j) = p/T + O(1), \quad 1 \le j \le r.$$

One has

$$N(\mathbf{J}) = \sum_{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)} \chi_{\mathcal{J}_1}(x_1) \dots \chi_{\mathcal{J}_r}(x_r), \tag{7}$$

where $\chi_{\mathcal{J}}(x)$ is the characteristic function of the interval $\mathcal{J}$. An analytic expression for $\chi_{\mathcal{J}}(x)$ with $x \in \mathbf{F}_p$ is given by

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

where $e_p(x) = e^{2\pi i x/p}$. Using (8) in (7) and changing the order of summation, we obtain

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

where $\mathbf{k} = (k_1, \dots, k_r)$ and

$$S_{\mathbf{k}}(\mathbf{x}) = S_{\mathbf{k},p,r,\mathcal{C}}(\mathbf{x}) = \sum_{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)} e_p(k_1 x_1 + \dots + k_r x_r).$$

Since by hypothesis $\mathcal{C}$ is not contained in any hyperplane it follows that the linear form $k_1 x_1 + \dots + k_r x_r$ is constant along $\mathcal{C}$ if and only if $k_1 = \dots = k_r = 0$. This suggests separating the sum of the terms with $k_1 = \dots = k_r = 0$ and we will see that they give the main contribution in (9). It equals

$$M = \frac{1}{p^r} \Big(\prod_{j=1}^{r} |\mathcal{J}_j| \Big) \sum_{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)} 1 = \frac{|\mathcal{C}(\mathbf{F}_p)|}{T^r} \left(1 + O_r\left(\frac{T}{p} \right) \right). \tag{10}$$

By the Riemann Hypothesis for curves over finite fields (Weil [3]) we know that

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

In what follows we assume that $T \le \sqrt{p}$. Then we have

$$M = \frac{p}{T^r} \left(1 + O_{r,d}\left(\frac{1}{\sqrt{p}} \right) \right). \tag{12}$$

The remainder is

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

where the prime means that the terms with $k_1 = \dots = k_r = 0$ are excluded from the summation. Each of the factors of the product over j $(1 \le j \le r)$ is a geometric progression and can be estimated accurately. Indeed, we have

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

$$\le \min \left\{ |\mathcal{J}_j|, \frac{1}{2\left\| \frac{k_j}{p} \right\|} \right\},$$

where $\|\cdot\|$ denotes the distance to the nearest integer. For each $\mathbf{k} \neq \mathbf{0}$ our hypotheses on $\mathcal{C}$ allow us to apply the Bombieri–Weil inequality (see [1, Theorem 6]), which gives $S_{\mathbf{k}}(\mathbf{x}) = O_{r,d}(p^{1/2})$. Assuming, as we can, that in the summation over $\mathbf{k}$ in the definition of E one has $|k_j| \leq (p-1)/2$ for $1 \leq j \leq r$, we obtain

$$|E| \leq \frac{1}{p^r} \sideset{}{'}\sum_{\mathbf{k} \,(\mathrm{mod}\, p)} \prod_{j=1}^{r} \left(\min\left\{ \frac{p}{T}, \frac{p}{|k_j|} \right\} \right) |S_{\mathbf{k}}(\mathbf{x})|$$
$$\ll_r \sideset{}{'}\sum_{\mathbf{k} \,(\mathrm{mod}\, p)} \frac{1}{T+|k_1|} \cdots \frac{1}{T+|k_r|} |S_{\mathbf{k}}(\mathbf{x})|.$$

Consequently we deduce

$$|E| = O_{r,d}(p^{1/2} \log^r p). \tag{13}$$

By putting together (12) and (13) we obtain the required estimation for a cube:

$$N(\mathbf{J}) = p/T^r + O_{r,d}(p^{1/2} \log^r p). \tag{14}$$

We know by the Lipschitz principle on the number of integer points in an r-dimensional domain (see Davenport [2]), applied in this case via our lifting of $\mathbb{T}^r$ in $\mathbb{R}^r$, that

$$\mu(E(T) \setminus \mathcal{D}(T)) = O_{r,\Omega}(1/T).$$

That is, both $\mathcal{D}(T)$ and $E(T)$ are unions of $T^r\mu(\Omega) + O_{\Omega,r}(T^{r-1})$ cubes with edge equal to $1/T$. Using (14) for all these cubes one obtains

$$\begin{aligned} &|\{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p) : t(\mathbf{x}) \in \mathcal{D}(T)\}| \\ &\qquad = (p/T^r + O_{r,d}(p^{1/2} \log^r p))(T^r\mu(\Omega) + O_{\Omega,r}(T^{r-1})) \\ &\qquad = p\mu(\Omega) + O_{r,d,\Omega}(T^r p^{1/2} \log^r p) + O_{\Omega,r}(p/T) \end{aligned}$$

and similarly

$$|\{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p) : t(\mathbf{x}) \in E(T)\}| = p\mu(\Omega) + O_{r,d,\Omega}(T^r p^{1/2} \log^r p) + O_{\Omega,r}(p/T).$$

Therefore

$$|\{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p) : t(\mathbf{x}) \in \Omega\}| = p\mu(\Omega) + O_{r,d,\Omega}(T^r p^{1/2} \log^r p) + O_{\Omega,r}(p/T). \tag{15}$$

Since

$$\mu_{r,p,\mathcal{C}}(\Omega) = \frac{|\{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p) : t(\mathbf{x}) \in \Omega\}|}{|\mathcal{C}(\mathbf{F}_p)|},$$

from (15) and (11) it follows that

$$\mu_{r,p,\mathcal{C}}(\Omega) = \mu(\Omega) + O_{r,d,\Omega}(T^r p^{-1/2} \log^r p) + O_{r,d,\Omega}(1/T). \tag{16}$$

We now choose

$$T = [p^{1/(2(r+1))} \log^{-r/(r+1)} p],$$

which gives

$$\mu_{r,p,\mathcal{C}}(\Omega) = \mu(\Omega) + O_{r,d,\Omega}(p^{-1/(2(r+1))}\log^{r/(r+1)} p)$$

and this completes the proof of Theorem 1.

3. Proof of Theorem 2. Let $r, p, \mathcal{C}, \mathbf{u}$ and $\boldsymbol{\delta}$ be as in the statement of the theorem. Choose a representative $\mathbf{v} = (v_1, \dots, v_r)$ of $\mathbf{u}$ in $\mathbb{R}^r$. Inside the box

$$B = \{(v_1 + y_1, \dots, v_r + y_r) : 0 \le y_1, \dots, y_r < 1\}$$

consider the region

$$A = \{(v_1 + y_1, \dots, v_r + y_r) \in B : |y_j - y_r| \le \delta_j,\ 1 \le j \le r-1\}.$$

Let Ω be the image of A in $\mathbb{T}^r$. The canonical map from A to Ω is one-to-one and we have

$$\mathrm{Vol}(A) = \mu(\Omega). \tag{17}$$

By the definition of $\eta_{r,p,\mathcal{C},\mathbf{u},\boldsymbol{\delta}}$ we see that

$$\eta_{r,p,\mathcal{C},\mathbf{u},\boldsymbol{\delta}} = \frac{|\{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p) : t(\mathbf{x}) \in \Omega\}|}{|\mathcal{C}(\mathbf{F}_p)|} = \mu_{r,p,\mathcal{C}}(\Omega).$$

From Theorem 1 and (17) we deduce

$$\eta_{r,p,\mathcal{C},\mathbf{u},\boldsymbol{\delta}} = \mathrm{Vol}(A) + O_{r,d,\mathbf{u},\boldsymbol{\delta}}(p^{-1/(2(r+1))}\log^{r/(r+1)} p).$$

It remains to compute $\mathrm{Vol}(A)$. Set

$$z_j = \max\{0, y_r - \delta_j\}, \qquad w_j = \min\{1, y_r + \delta_j\}, \qquad 1 \le j \le r-1.$$

Then

$$\mathrm{Vol}(A) = \int_0^1 \int_{z_{r-1}}^{w_{r-1}} \dots \int_{z_1}^{w_1} dy_1 \dots dy_r = \int_0^1 (w_1 - z_1)\dots(w_{r-1} - z_{r-1})\, dy_r.$$

One checks that

$$w_j - z_j = h(y_r, \delta_j), \qquad 1 \le j \le r-1.$$

Hence $\mathrm{Vol}(A) = c(\delta_1, \dots, \delta_{r-1})$, which completes the proof of Theorem 2.

4. The case of plane curves revisited. The reader might wonder why the bound for the error term in Theorem 2 in the case $r = 2$ is not as sharp as the bounds for the error terms in (1) and (2). Following the proof of Theorems 1 and 2 above, it is clear that the quality of the upper bounds for the error terms provided by this method depends on the shape of the given region Ω. Let us now see how one can recover the estimate (2), with exactly the same bound for the error term. We proceed as in the proof of Theorem 2 with $r = 2$. The estimate (2) corresponds to the case $\mathbf{u} = \mathbf{0}$, but we take here a general $\mathbf{u}$ and choose a representative $\mathbf{v} = (v_1, v_2)$ of $\mathbf{u}$ in $\mathbb{R}^2$.

The point now is that the region A defined in the previous section does not need to be broken in small cubes since it can be written as a union of two parallelograms and a square: $A = A_1 \cup A_2 \cup A_3$, where

$$A_1 = \{(v_1 + y_1, v_2 + y_2) \in \mathbb{R}^2 : 0 \le y_2 < 1 - \delta,\ 0 \le y_1 - y_2 < \delta\},$$
$$A_2 = \{(v_1 + y_1, v_2 + y_2) \in \mathbb{R}^2 : 0 \le y_1 < 1 - \delta,\ 0 \le y_2 - y_1 < \delta\},$$
$$A_3 = \{(v_1 + y_1, v_2 + y_2) \in \mathbb{R}^2 : 1 - \delta \le y_1, y_2 < 1\}.$$

It follows that

$$\{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p) : t(\mathbf{x}) \in \Omega\} = \Sigma_1 + \Sigma_2 + \Sigma_3, \tag{18}$$

where

$$\Sigma_1 = \sum_{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)} \chi_{[0,(1-\delta)p)}(x_2)\chi_{[0,\delta p)}(x_1 - x_2),$$
$$\Sigma_2 = \sum_{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)} \chi_{[0,(1-\delta)p)}(x_1)\chi_{(0,\delta p)}(x_2 - x_1),$$
$$\Sigma_3 = \sum_{\mathbf{x} \in \mathcal{C}(\mathbf{F}_p)} \chi_{[(1-\delta)p,p)}(x_1)\chi_{[(1-\delta)p,p)}(x_2).$$

Now each of the sums Σ_1, Σ_2, Σ_3 may be treated in the same way we estimated $N(\mathbf{J})$ in the proof of Theorem 1. One obtains asymptotic results with square root upper bounds for the error terms as in (14). Putting all these together yields (2).

The above discussion shows that if the region Ω in Theorem 1 can be written as a union of L nonoverlapping parallelepipeds in $\mathbb{T}^r$ then the upper bound for the error term in Theorem 1 can be replaced by $O_{r,d}(Lp^{-1/2}\log^r p)$. Thus in particular one has the following improved version of (5):

COROLLARY 1. *Let $r \ge 2$ be an integer, $\boldsymbol{\delta} = (\delta_1, \dots, \delta_{r-1}) \in \mathbb{R}^{r-1}$ with $0 < \delta_1, \dots, \delta_{r-1} \le 1/2$, p a prime number and $\mathcal{C}$ an irreducible curve of degree d in $\mathbb{A}^r(\overline{\mathbf{F}}_p)$, defined over $\mathbf{F}_p$ and not contained in any hyperplane. Then*

$$\varrho_{r,p,\mathcal{C},\boldsymbol{\delta}} = 2^{r-1}\delta_1 \dots \delta_{r-1} + O_{r,d}(p^{-1/2}\log^r p). \tag{19}$$

References

[1] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.

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

[3] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris, 1948.

[4] W. Zhang, *On the distribution of inverses modulo n*, J. Number Theory 61 (1996), 301–310.

[5] Z. Zheng, *The distribution of zeros of an irreducible curve over a finite field*, ibid. 59 (1996), 106–118.

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

Alexandru Zaharescu
Institute of Mathematics of the
Romanian Academy
P.O. Box 1-764
70700 Bucureşti, Romania

Department of Mathematics
University of Illinois at Urbana-Champaign
Altgeld Hall
1409 W. Green Street
Urbana, IL 61801, U.S.A.
E-mail: zaharesc@math.uiuc.edu

Received on 8.12.1999
and in revised form on 29.1.2001 (3726)