

ALEXANDRU ZAHARESCU

**The distribution of the values of a rational
function modulo a big prime**

Journal de Théorie des Nombres de Bordeaux, tome 15, n° 3 (2003),
p. 863-872

http://www.numdam.org/item?id=JTNB_2003__15_3_863_0

© Université Bordeaux 1, 2003, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

The distribution of the values of a rational function modulo a big prime

par ALEXANDRU ZAHARESCU

RÉSUMÉ. Étant donné un grand nombre premier p et une fonction rationnelle $r(X)$ définie sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, on évalue la grandeur de l'ensemble $\{x \in \mathbb{F}_p : \tilde{r}(x) > \tilde{r}(x+1)\}$, où $\tilde{r}(x)$ et $\tilde{r}(x+1)$ sont les plus petits représentants de $r(x)$ et $r(x+1)$ dans \mathbb{Z} modulo $p\mathbb{Z}$.

ABSTRACT. Given a large prime number p and a rational function $r(X)$ defined over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we investigate the size of the set $\{x \in \mathbb{F}_p : \tilde{r}(x) > \tilde{r}(x+1)\}$, where $\tilde{r}(x)$ and $\tilde{r}(x+1)$ denote the least positive representatives of $r(x)$ and $r(x+1)$ in \mathbb{Z} modulo $p\mathbb{Z}$.

1. Introduction

Several problems on the distribution of points satisfying various congruence constraints have been investigated recently. Given a large prime number p , for any $a \in \{1, 2, \dots, p-1\}$ let $\bar{a} \in \{1, 2, \dots, p-1\}$ be such that $a\bar{a} \equiv 1 \pmod{p}$. A question raised by D.H. Lehmer (see Guy [4, Problem F12]) asks to say something nontrivial about the number, call it $N(p)$, of those a for which a and \bar{a} are of opposite parity. The problem was studied by Wenpeng Zhang in [8], [9] and [10] who proved that

$$(1) \quad N(p) = \frac{p}{2} + O\left(p^{1/2} \log^2 p\right)$$

and then generalized (1) to the case when p is replaced by any odd number q . In [2] it is obtained a generalization of (1), in which the pair (a, \bar{a}) is replaced by a point lying on a more general irreducible curve defined mod p . Zhang also studied the problem of the distribution of distances $|a - \bar{a}|$, where a, \bar{a} run over the set of integers in $\{1, \dots, n-1\}$ which are relatively prime to n . He proved in [11] that for any integer $n \geq 2$ and any $0 < \delta \leq 1$ one has

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

where $\varphi(n)$ is the Euler function and $d(n)$ denotes the number of divisors of n . In [12] Zhiyong Zheng investigated the same problem, with (a, \bar{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 [12] that for any $0 < \delta \leq 1$ one has:

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

A generalization of this problem, where the pair (x, y) is replaced by a point lying on an irreducible curve in a higher dimensional affine space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, has been obtained in [3].

There are different ways to measure the randomness of the distribution of a given set. B. Z. Moroz showed in [5] that the squares (or the l -th powers, if l divides $p - 1$) are randomly distributed among the values $\{i_p(f(0)), \dots, i_p(f(p - 1))\}$ of a fixed irreducible polynomial $f(X)$ in $\mathbb{Z}[X]$ modulo a prime p , as $p \rightarrow \infty$ (here i_p stands for the reduction modulo p).

In the present paper we study what happens with the order of residue classes mod p when they are transformed through a rational function $r(X) \in \mathbb{F}_p(X)$. For any $y \in \mathbb{F}_p$ denote by $j(y)$ the least positive representative of y in \mathbb{Z} modulo $p\mathbb{Z}$. To any rational function $r(X) \in \mathbb{F}_p(X)$ we associate the map $\tilde{r} : \mathbb{F}_p \rightarrow \{0, 1, \dots, p - 1\}$ given by $\tilde{r}(x) = j(r(x))$ if $x \in \mathbb{F}_p$ is not a pole of $r(X)$, and $\tilde{r}(x) = 0$ if x is a pole of $r(X)$. As the degree of $r(X)$ will be assumed to be small in terms of p in what follows, the contribution of the poles of $r(X)$ in our asymptotic results will be negligible. If we count those $x \in \mathbb{F}_p$ for which $\tilde{r}(x + 1) < \tilde{r}(x)$, respectively those x for which $\tilde{r}(x + 1) > \tilde{r}(x)$, there should be no bias towards any one of these inequalities. In other words one would expect that for about half of the elements $x \in \mathbb{F}_p$, $\tilde{r}(x + 1)$ is larger than $\tilde{r}(x)$ and for about half of the elements $x \in \mathbb{F}_p$, $\tilde{r}(x + 1)$ is smaller than $\tilde{r}(x)$.

In order to handle the above problem, we fix nonzero positive integers a, b and study the distribution of the set $\{b\tilde{r}(x+1) - a\tilde{r}(x) : x \in \mathbb{F}_p\}$. For any real number t consider the set $\mathcal{M}(a, b, p, r, t) = \{x \in \mathbb{F}_p : b\tilde{r}(x+1) - a\tilde{r}(x) < tp\}$ and denote by $D(a, b, p, r, t)$ the number of elements of $\mathcal{M}(a, b, p, r, t)$. Our aim is to provide an asymptotic formula for $D(a, b, p, r, t)$.

We now introduce a function $G(t, a, b)$ which will play an important role in the estimation of $D(a, b, p, r, t)$.

$$G(t, a, b) = \begin{cases} 0, & \text{if } t < -a \\ \frac{(t+a)^2}{2ab}, & \text{if } -a \leq t \leq W \\ \left(1 - \frac{(W+a)^2}{ab}\right) \frac{t-W}{Z-W} + \frac{(W+a)^2}{2ab}, & \text{if } W < t < Z \\ 1 - \frac{(t-b)^2}{2ab}, & \text{if } Z \leq t < b \\ 1, & \text{if } b \leq t \end{cases}$$

where $W = \min\{0, b - a\}$ and $Z = \max\{0, b - a\}$. We will prove the following

Theorem 1.1. *For any positive integers a, b, d , any prime number p , any real number t and any rational function $r(X) = \frac{f(X)}{g(X)}$ which is not a linear polynomial, with $f, g \in \mathbb{F}_p[X]$, $\deg f, \deg g \leq d$, one has*

$$(3) \quad D(a, b, p, r, t) = pG(t, a, b) + O_{a,b,d} \left(p^{1/2} \log^2 p \right).$$

As a consequence of Theorem 1.1 we show that the inequality $\tilde{r}(x) > \tilde{r}(x + 1)$ holds indeed for about half of the values of x in \mathbb{F}_p .

Corollary 1.2. *Let p be a prime number, d a positive integer and let $r(X) = \frac{f(X)}{g(X)}$ be a rational function which is not a linear polynomial, with $f, g \in \mathbb{F}_p[X]$ and $\deg f, \deg g \leq d$. Then one has*

$$\#\{x \in \mathbb{F}_p : \tilde{r}(x) > \tilde{r}(x + 1)\} = \frac{p}{2} + O_d \left(p^{1/2} \log^2 p \right).$$

As another application of Theorem 1.1 we obtain an asymptotic result for all the even moments of the distance between $\tilde{r}(x + 1)$ and $\tilde{r}(x)$.

Corollary 1.3. *Let k be a positive integer and let $p, d, r(X)$ be as in the statement of Corollary 1. Then we have*

$$\begin{aligned} M(p, r, 2k) &:= \sum_{x \in \mathbb{F}_p} (\tilde{r}(x + 1) - \tilde{r}(x))^{2k} \\ &= \frac{p^{2k+1}}{(k + 1)(2k + 1)} + O_{k,d} \left(p^{2k+1/2} \log^2 p \right). \end{aligned}$$

In particular, for $k = 1$ one has

$$M(p, r, 2) = \frac{p^3}{6} + O_d(p^{5/2} \log^2 p).$$

This says that in quadratic average $|\tilde{r}(x + 1) - \tilde{r}(x)|$ is $\sim \frac{p}{\sqrt{6}}$.

2. Proof of Theorem 1.1

We will need the following lemma, which is a consequence of the Riemann Hypothesis for curves defined over a finite field (see [7], [6], [1]).

Lemma 2.1. *Let p be a prime number and \mathbb{F}_p the field with p elements. Let ψ be a nontrivial character of the additive group of \mathbb{F}_p and let $R(X)$ be a nonconstant rational function. Then*

$$\sum_{a \in \mathbb{F}_p} \psi(R(a)) = O(\sqrt{p}),$$

where the poles of $R(X)$ are excluded from the summation, and the implicit O -constant depends at most on the degrees of the numerator and denominator of $F(X)$.

Let now p be a prime number, let a, b, d be positive integers less than p , let t be a real number and let $r(X) = \frac{f(X)}{g(X)}$, $r(X)$ not a linear polynomial, with $f(X), g(X) \in \mathbb{F}_p[X]$, $\deg f(X), \deg g(X) \leq d$. For any $y, z \in \{0, 1, \dots, p-1\}$ we set

$$(4) \quad H(y, z) = H(t, y, z, a, b) = \begin{cases} 1, & \text{if } bz - ay < tp \\ 0, & \text{if } bz - ay \geq tp \end{cases}$$

Then we may write $D(a, b, p, r, t)$ in the form

$$\begin{aligned} D(a, b, p, r, t) &= \sum_{x \in \mathbb{F}_p} H(\tilde{r}(x), \tilde{r}(x+1)) \\ &= \sum_{0 \leq y, z \leq p-1} H(y, z) \#\{x \in \mathbb{F}_p : \tilde{r}(x) = y, \tilde{r}(x+1) = z\}. \end{aligned}$$

Next, we write $D(a, b, p, r, t)$ in terms of exponential sums mod p . Denote as usual $e_p(w) = e^{\frac{2\pi iw}{p}}$ for any w . Using the equalities

$$\sum_{0 \leq m \leq p-1} e_p(m(y - \tilde{r}(x))) = \begin{cases} p, & \text{if } \tilde{r}(x) = y \\ 0, & \text{else} \end{cases}$$

and

$$\sum_{0 \leq n \leq p-1} e_p(n(z - \tilde{r}(x+1))) = \begin{cases} p, & \text{if } \tilde{r}(x+1) = z \\ 0, & \text{else} \end{cases}$$

we find that

$$(5) \quad \begin{aligned} D(a, b, p, r, t) &= \frac{1}{p^2} \sum_{0 \leq y, z \leq p-1} H(y, z) \\ &\times \sum_{x \in \mathbb{F}_p} \sum_{0 \leq m \leq p-1} e_p(m(y - \tilde{r}(x))) \sum_{0 \leq n \leq p-1} e_p(n(z - \tilde{r}(x+1))) \end{aligned}$$

$$\begin{aligned}
 &= \frac{1}{p^2} \sum_{0 \leq m, n \leq p-1} \sum_{0 \leq y, z \leq p-1} H(y, z) e_p(my + nz) \sum_{x \in \mathbb{F}_p} e_p(-m\tilde{r}(x) - n\tilde{r}(x + 1)) \\
 &= \frac{1}{p^2} \sum_{0 \leq m, n \leq p-1} \check{H}(m, n) S(-m, -n, r, p),
 \end{aligned}$$

where

$$(6) \quad \check{H}(m, n) = \sum_{0 \leq y, z \leq p-1} H(y, z) e_p(my + nz)$$

and

$$(7) \quad S(-m, -n, r, p) = \sum_{x \in \mathbb{F}_p} e_p(-m\tilde{r}(x) - n\tilde{r}(x + 1)).$$

Note that for $m = n = 0$ one has

$$(8) \quad S(0, 0, r, p) = p.$$

Next, we claim that if $(m, n) \neq (0, 0)$ then the rational function $h(X) = mr(X) + nr(X + 1) \in \mathbb{F}_p(X)$ is nonconstant. Indeed, if $n = 0$ then $m \neq 0$ and $h(X) = mr(X)$ is nonconstant by the hypotheses from the statement of the theorem. The same conclusion holds if $m = 0$ and $n \neq 0$. Let now $m \neq 0, n \neq 0$ and assume that

$$(9) \quad mr(X) + nr(X + 1) = c$$

for some $c \in \mathbb{F}_p$. Suppose first that $r(X)$ is not a polynomial and choose a root $\alpha \in \overline{\mathbb{F}_p}$ of the denominator of $r(X)$, where $\overline{\mathbb{F}_p}$ denotes the algebraic closure of \mathbb{F}_p . Since α is a pole of $r(X)$, from (9) it follows that α is also a pole of $r(X + 1)$, that is $\alpha + 1$ is a pole of $r(X)$. By repeating the above reasoning with α replaced by $\alpha + 1$ we see that $\alpha + 2, \alpha + 3, \dots, \alpha + p - 1$ are poles of $r(X)$. This forces $\deg g(X)$ to be $\geq p$, so $d \geq p$, in which case (3) becomes trivial. Let us suppose now that $r(X)$ is a polynomial, say

$$r(X) = a_l X^l + a_{l-1} X^{l-1} + \dots + a_1 X + a_0$$

with $a_0, \dots, a_l \in \mathbb{F}_p, a_l \neq 0$. Then by the hypotheses of Theorem 1.1 it follows that $l \geq 2$. Looking at the coefficient of X^l in (9) we deduce that $m + n = 0$ in \mathbb{F}_p . But then, the coefficient of X^{l-1} on the left side of (9) equals lna_l , which is nonzero in \mathbb{F}_p , contradicting (9). This proves our claim that $h(X)$ is nonconstant in $\mathbb{F}_p(X)$. By Lemma 2.1 it follows that

$$(10) \quad |S(-m, -n, r, p)| = O_d(\sqrt{p})$$

for any $(m, n) \neq (0, 0)$.

Next, we proceed to evaluate the coefficients $\check{H}(m, n)$. We calculate explicitly $\check{H}(0, 0)$ and provide upper bounds for $|\check{H}(m, n)|$ for $(m, n) \neq (0, 0)$. There are four cases.

I. $m = 0, n \neq 0$. We have

$$\check{H}(0, n) = \sum_{0 \leq y, z \leq p-1} H(y, z) e_p(nz).$$

By the definition of $H(y, z)$ it follows that for each $y \in \{0, 1, \dots, p-1\}$ we have a sum of $e_p(nz)$ with z running over a subinterval of $\{0, 1, \dots, p-1\}$, that is a sum of a geometric progression with ratio $e_p(n)$. The absolute value of such a sum is $\leq \frac{2}{|e_p(n)-1|}$ and consequently

$$(11) \quad |\check{H}(0, n)| \leq \frac{2p}{|e_p(n) - 1|} = \frac{p}{\sin \frac{n\pi}{p}} \leq \frac{p}{2 \left\| \frac{n}{p} \right\|},$$

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

II. $m \neq 0, n = 0$. Similarly, as in case I, we have

$$(12) \quad |\check{H}(m, 0)| \leq \frac{p}{2 \left\| \frac{m}{p} \right\|}.$$

III. $m \neq 0, n \neq 0$. We need the following lemma.

Lemma 2.2. *Let $h, k \not\equiv 0 \pmod{p}$, L, T and $u \geq 0$ be integers. Let $S = \sum_{y=0}^L \sum_{z=0}^{uy+T} e_p(hy) e_p(kz)$. Then one has*

$$|S| = O \left(\frac{1}{\left\| \frac{k}{p} \right\|} \min \left\{ L, \frac{1}{\left\| \frac{h+uk}{p} \right\|} \right\} + \frac{1}{\left\| \frac{k}{p} \right\|} \cdot \frac{1}{\left\| \frac{h}{p} \right\|} \right).$$

Proof. One has

$$\begin{aligned} S &= \sum_{y=0}^L e_p(hy) \sum_{z=0}^{uy+T} e_p(kz) \\ &= \sum_{y=0}^L e_p(hy) \frac{1 - e_p(k(uy + T + 1))}{1 - e_p(k)} \\ &= \frac{1}{1 - e_p(k)} \sum_{y=0}^L e_p(hy) - \frac{e_p(k(T + 1))}{1 - e_p(k)} \sum_{y=0}^L e_p((h + ku)y). \end{aligned}$$

Thus

$$|S| \leq \frac{1}{|1 - e_p(k)|} \left| \sum_{y=0}^L e_p(hy) \right| + \frac{1}{|1 - e_p(k)|} \left| \sum_{y=0}^L e_p((h + ku)y) \right|.$$

Note that

$$\frac{1}{|1 - e_p(k)|} = \frac{1}{\left|1 - e^{\frac{2\pi ik}{p}}\right|} = \frac{1}{\left|e^{-\frac{\pi ik}{p}} - e^{\frac{\pi ik}{p}}\right|} = \frac{1}{\left|2 \sin \frac{\pi k}{p}\right|} = O\left(\frac{1}{\left\|\frac{k}{p}\right\|}\right).$$

Also,

$$\left|\sum_{y=0}^L e_p(hy)\right| = \frac{|1 - e_p(h(L+1))|}{|1 - e_p(h)|} = O\left(\frac{1}{\left\|\frac{h}{p}\right\|}\right).$$

Lastly, if $h + ku$ is not a multiple of p , then

$$\left|\sum_{y=0}^L e_p((h + ku)y)\right| = \frac{|1 - e_p((h + ku)(L+1))|}{|1 - e_p(h + ku)|} = O\left(\frac{1}{\left\|\frac{h+ku}{p}\right\|}\right).$$

We also have the bound

$$\left|\sum_{y=0}^L e_p((h + ku)y)\right| \leq L + 1,$$

which is valid for any h, k and u . Putting the above bounds together, Lemma 2.2 follows.

We now return to the estimation of $\check{H}(m, n)$. Writing

$$\check{H}(m, n) = \sum_{\substack{0 \leq y, z \leq p-1 \\ bz - ay < tp}} e_p(my + nz)$$

as a sum of b sums according to the residue of y modulo b , one arrives at sums as in Lemma 2.2, with $h = mb, k = n, u = a$. It follows that

$$(13) \quad |\check{H}(m, n)| = O_{a,b} \left(\frac{1}{\left\|\frac{n}{p}\right\|} \min \left\{ p, \frac{1}{\left\|\frac{mb+an}{p}\right\|} \right\} + \frac{1}{\left\|\frac{n}{p}\right\|} \cdot \frac{1}{\left\|\frac{mb}{p}\right\|} \right).$$

IV. $m, n = 0$. By definition, we have

$$\check{H}(0, 0) = \sum_{0 \leq y, z \leq p-1} H(y, z).$$

Let \mathcal{D} be the set of real points from the square $[0, p) \times [0, p)$ which lie below the line $bz - ay = tp$. Then $\check{H}(0, 0)$ equals the number of integer points (y, z) from \mathcal{D} . Therefore

$$\check{H}(0, 0) = Area(\mathcal{D}) + O(length(\partial\mathcal{D})).$$

An easy computation shows that $Area(\mathcal{D})$ equals $p^2 G(t, a, b)$ with $G(t, a, b)$ defined as in the Introduction, while the length of the boundary $\partial\mathcal{D}$ is $\leq 4p$. Hence

$$\check{H}(0, 0) = p^2 G(t, a, b) + O(p).$$

By (5) we know that

$$\left| D(a, b, p, r, t) - \frac{1}{p^2} \check{H}(0, 0) S(0, 0, r, p) \right| \leq D_1 + D_2 + D_3,$$

where

$$\begin{aligned} D_1 &= \frac{1}{p^2} \sum_{m=1}^{p-1} |\check{H}(m, 0)| |S(-m, 0, r, p)|, \\ D_2 &= \frac{1}{p^2} \sum_{n=1}^{p-1} |\check{H}(0, n)| |S(0, -n, r, p)|, \\ D_3 &= \frac{1}{p^2} \sum_{m=1}^{p-1} \sum_{n=1}^{p-1} |\check{H}(m, n)| |S(-m, -n, r, p)|. \end{aligned}$$

One has

$$\frac{1}{p^2} \check{H}(0, 0) S(0, 0, r, p) = \frac{\check{H}(0, 0)}{p} = pG(t, a, b) + O(1).$$

By (11) and (10) we have

$$D_2 = O_d \left(\frac{1}{p^2} \sum_{n=1}^{p-1} \frac{p}{\left\| \frac{n}{p} \right\|} \sqrt{p} \right) = O_d(\sqrt{p} \log p).$$

Similarly one has

$$D_1 = O_d(\sqrt{p} \log p).$$

In order to estimate D_3 we first use (10) and (13) to obtain

$$\begin{aligned} (14) \quad D_3 &= O_{a,b,d} \left(\frac{1}{p^{3/2}} \sum_{m=1}^{p-1} \sum_{n=1}^{p-1} \frac{1}{\left\| \frac{n}{p} \right\|} \min \left\{ p, \frac{1}{\left\| \frac{mb+an}{p} \right\|} \right\} \right. \\ &\quad \left. + \frac{1}{p^{3/2}} \sum_{m=1}^{p-1} \sum_{n=1}^{p-1} \frac{1}{\left\| \frac{n}{p} \right\|} \cdot \frac{1}{\left\| \frac{mb}{p} \right\|} \right) \end{aligned}$$

The first double sum in (14) is

$$\begin{aligned} &\sum_{m=1}^{p-1} \sum_{n=1}^{p-1} \frac{1}{\left\| \frac{n}{p} \right\|} \min \left\{ p, \frac{1}{\left\| \frac{mb+an}{p} \right\|} \right\} \\ &\leq \sum_{n=1}^{p-1} \frac{1}{\left\| \frac{n}{p} \right\|} \sum_{\substack{m=1 \\ mb+an \equiv 0 \pmod{p}}}^{p-1} p + \sum_{n=1}^{p-1} \frac{1}{\left\| \frac{n}{p} \right\|} \sum_{\substack{m=1 \\ mb+an \not\equiv 0 \pmod{p}}}^{p-1} \frac{1}{\left\| \frac{mb+an}{p} \right\|} \end{aligned}$$

$$\leq p \sum_{n=1}^{\frac{p-1}{2}} \frac{p}{n} + \sum_{n=1}^{p-1} \frac{1}{\left\| \frac{n}{p} \right\|} \sum_{m'=1}^{p-1} \frac{1}{\left\| \frac{m'}{p} \right\|} \leq p^2(1 + \log p) + 4p^2(1 + \log p)^2,$$

while the second double sum is

$$\sum_{m=1}^{p-1} \sum_{n=1}^{p-1} \frac{1}{\left\| \frac{n}{p} \right\|} \cdot \frac{1}{\left\| \frac{mb}{p} \right\|} = 4 \sum_{m=1}^{\frac{p-1}{2}} \frac{p}{m} \sum_{n=1}^{\frac{p-1}{2}} \frac{p}{n} \leq 4p^2(1 + \log p)^2.$$

Hence $D_3 = O_{a,b,d}(\sqrt{p} \log^2 p)$. Putting all these together, Theorem 1.1 follows.

3. Proof of the Corollaries

For the proof of the first Corollary, let us notice that

$$\#\{x \in \mathbb{F}_p : \tilde{r}(x) > \tilde{r}(x + 1)\} = D(1, 1, p, r, 0).$$

Here $W = Z = 0$ and so

$$G(0, 1, 1) = \frac{(t + a)^2}{2ab} = \frac{1}{2}.$$

Thus

$$\#\{x \in \mathbb{F}_p : \tilde{r}(x) > \tilde{r}(x + 1)\} = \frac{p}{2} + O_d(p^{\frac{1}{2}} \log^2 p)$$

which proves Corollary 1.2.

In order to prove Corollary 1.3 note that

$$\begin{aligned} M(p, r, 2k) &= \sum_{x \in \mathbb{F}_p} (\tilde{r}(x + 1) - \tilde{r}(x))^{2k} \\ &= \sum_{-p < m < p} m^{2k} \#\{x \in \mathbb{F}_p : \tilde{r}(x + 1) - \tilde{r}(x) = m\}. \end{aligned}$$

This equals

$$\begin{aligned} \sum_{-p < m < p} m^{2k} (D(\frac{m+1}{p}) - D(\frac{m}{p})) &= D(1)(p-1)^{2k} \\ &+ \sum_{-p < m < p} D(\frac{m}{p})((m-1)^{2k} - m^{2k}) \end{aligned}$$

where for any t we denote $D(t) = D(1, 1, p, r, t)$. From Theorem 1.1 it follows that

$$\begin{aligned} M(p, r, 2k) &= p^{2k+1} G(1, 1, 1) + p \sum_{-p < m < p} G(\frac{m}{p}, 1, 1)((m-1)^{2k} - m^{2k}) \\ &+ O_{k,d}(p^{2k+\frac{1}{2}} \log^2 p) + O_d(p^{1/2} \log^2 p \sum_{-p < m < p} |(m-1)^{2k} - m^{2k}|). \end{aligned}$$

Since $(m-1)^{2k} - m^{2k} = -2km^{2k-1} + O_k(p^{2k-2})$ and $0 \leq G(\frac{m}{p}, 1, 1) \leq 1$ for any m , we derive

$$M(p, r, 2k) = p^{2k+1}G(1, 1, 1) - 2kp \sum_{-p < m < p} m^{2k-1}G(\frac{m}{p}, 1, 1) + O_{k,d}(p^{2k+\frac{1}{2}} \log^2 p).$$

From the definition of G we see that

$$G(\frac{m}{p}, 1, 1) = \begin{cases} 0, & \text{if } m < -p \\ \frac{(1+\frac{m}{p})^2}{2}, & \text{if } -p \leq m \leq 0 \\ 1 - \frac{(1-\frac{m}{p})^2}{2}, & \text{if } 0 < m < p \\ 1, & \text{if } p \leq m. \end{cases}$$

Using the fact that for any positive integer r one has $\sum_{-p < m < p} m^r = \frac{2p^{r+1}}{r+1} + O_r(p^r)$ if r is even and $\sum_{-p < m < p} m^r = 0$ if r is odd, the statement of Corollary 1.3 follows after a straightforward computation.

References

- [1] E. BOMBIERI, *On exponential sums in finite fields*. Amer. J. of Math. **88** (1966), 71–105.
- [2] C. COBELI, A. ZAHARESCU, *Generalization of a problem of Lehmer*. Manuscripta Math. **104** no. 3 (2001), 301–307.
- [3] C. COBELI, A. ZAHARESCU, *On the distribution of the F_p -points on an affine curve in r dimensions*. Acta Arith. **99** no. 4 (2001), 321–329.
- [4] R.K. GUY, *Unsolved Problems in Number Theory*. Springer-Verlag, New York - Berlin, 1981, (second edition 1994).
- [5] B. Z. MOROZ, *The distribution of power residues and non-residues*. Vestnik LGU, **16** no. 19 (1961), 164–169.
- [6] G. I. PEREL'MUTER, *On certain character sums*. Uspechi Matem. Nauk, **18** (1963), 145–149.
- [7] A. WEIL, *On some exponential sums*. Proc Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.
- [8] W. ZHANG, *On a problem of D. H. Lehmer and its generalization*. Compositio Math. **86** no. 3 (1993), 307–316.
- [9] W. ZHANG, *A problem of D. H. Lehmer and its generalization II*. Compositio Math. **91** no. 1 (1994), 47–56.
- [10] W. ZHANG, *On the difference between a D. H. Lehmer number and its inverse modulo q* . Acta Arith. **68** no. 3 (1994), 255–263.
- [11] W. ZHANG, *On the distribution of inverses modulo n* . J. Number Theory **61** no. 2 (1996), 301–310.
- [12] Z. ZHENG, *The distribution of Zeros of an Irreducible Curve over a Finite Field*. J. Number Theory **59** no. 1 (1996), 106–118.

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