On a generalization of Polya inequality and some of its statistical implications

William M.Y. Goh
MCS Department, Drexel University, Philadelphia, PA 19104, USA

Received 5 October 2000; received in revised form 23 April 2001

Abstract

Let $p$ be a prime and $\chi$ a nonprincipal character mod $p$. Let $1 \leq m \leq p$ and $l$ an integer so that $p \nmid l$. Then, we have $|\sum_{a=0}^{m-1} \chi(a)(a+l)| \leq 3\sqrt{p}\ln p$. The proof makes use of estimation on Kloosterman sum via the Riemann hypothesis on finite fields. As simple consequence of the theorem we obtain a uniform distribution of consecutive quadratic residues mod $p$. © 2002 Published by Elsevier Science B.V.

Keywords: Character; Gauss sum; Kloosterman sum; Quadratic residue; Distribution; Legendre symbol; Riemann hypothesis on finite fields

1. Introduction

For a set $S$ of $n$ points in the unit square, let $T(S)$ be the minimum area of a triangle whose vertices are three distinct points of $S$. Let $T(n) = \max T(S)$, where $S$ ranges over all sets of $n$ points in the unit square. The Heilbron conjecture says that $T(n) = O(1/n^2)$. This conjecture turned out to be false. It was disproved by Komlós et al. The interested reader should consult their paper [7]. In fact, they use a rather complicated probabilistic construction, showing the existence of a set $S$ of $n$ points such that $T(S) = \Omega(\ln n/n^2)$. To make the study of $T(n)$ more interesting, Paul Erdős provides the following explicit construction: Let $p$ be a prime and let

$$A := \{(x, x^2) \in [0, p - 1] \times [0, p - 1]: x^2 \text{ is reduced mod } p\}.$$

Contracting the set $A$ by a factor of $p - 1$ in both coordinates gives a set $S$ of $p$ points in the unit square. Erdős showed that $T(S) \geq 1/2(p - 1)^2$ [see p. 30 in [1]]. Although his example does not lead to an improvement of the result of Komlós et al. it does offer a sense of concreteness to the problem. The behavior of the points in set $A$ is rather erratic. While $x$ varies through the integers
from 0 to \( p - 1 \), the value \( x^2 \mod p \) can be very jumpy. This observation leads us to the study of the statistical distribution of quadratic residues mod \( p \) in the interval \([0, p - 1]\).

An integer \( k \) is called a quadratic residue mod \( p \) if \( k \equiv x^2 \mod p \) for some integer \( x \). Let \( 0 < \beta < 1 \). We ask the question: Does the fraction of quadratic residues lying in the interval \([0, \beta(p - 1)]\) approach a limit as \( p \to \infty \)? This question can be easily solved by appealing to an inequality discovered by G. Polya [2,4].

**Theorem 1.** Let \( p \) be a prime and \( \chi \) a nonprincipal character mod \( p \). Let \( 1 \leq m \leq p \). Then we have

\[
\left| \sum_{a=0}^{m-1} \chi(a) \right| \leq \sqrt{p} \ln p.
\]

Let \( F_p = \mathbb{Z}/p\mathbb{Z} \), the finite field that consists of \( p \) residue classes mod \( p \). A character mod \( p \) is just a group homomorphism from the multiplicative group \( F_p - \{0\} \) to the multiplicative group \( \mathbb{C} - \{0\} \), where \( \mathbb{C} \) is the complex field. The principal character, denoted by \( \varepsilon \), is the character defined by the relation \( \varepsilon(a) = 1 \) for all \( a \in F_p - \{0\} \). It is often useful to extend the domain of definition of a character to all of \( F_p \). If \( \chi \neq \varepsilon \), we do this by defining \( \chi(0) = 0 \). For \( \varepsilon \) we define \( \varepsilon(0) = 1 \). For motivation of such extensions and some basic properties of characters the reader is referred to [5]. Perhaps the simplest nontrivial character is the Legendre symbol which is defined below.

\[
\left( \frac{a}{p} \right) = \begin{cases} 
0, & \text{if } p \mid a, \\
1, & \text{if } a \text{ is a quadratic residue mod } p, \\
-1, & \text{if } a \text{ is not a quadratic residue mod } p.
\end{cases}
\]

Now let \( A_\beta := \{0 \leq k \leq \beta(p - 1) : k \text{ is a quadratic residue mod } p\} \).

Then in terms of the Legendre symbol the cardinality of \( A_\beta \) is expressed as

\[
|A_\beta| = \sum_{a=1}^{\lfloor \beta(p-1) \rfloor} \frac{1}{2} \left( 1 + \left( \frac{a}{p} \right) \right).
\]

Here, \( \lfloor \cdot \rfloor \) denotes the floor function which appears in the upper limit of the summation. Note that the total number of quadratic residues is \((p - 1)/2\). Hence the fraction of quadratic residues in \([0, \beta(p - 1)]\) is

\[
\frac{|A_\beta|}{(p - 1)/2} = \frac{\beta(p - 1)}{p - 1} + \frac{\sum_{a=1}^{\lfloor \beta(p-1) \rfloor} \left( \frac{a}{p} \right)}{p - 1}.
\]

Polya’s inequality is applied to the second term of the above sum and we get

\[
\frac{|A_\beta|}{(p - 1)/2} = \beta + O\left( \frac{\ln p}{\sqrt{p}} \right) \to \beta, \quad \text{as } p \to \infty.
\]

This result can be phrased as: the quadratic residues are asymptotically uniformly distributed.
An integer $a$ is called a consecutive quadratic residue mod $p$ if both $a$ and $a + 1$ are quadratic residues mod $p$. To study the distribution of consecutive quadratic residues, we are led to consider the sum

$$\sum_{a=1}^{m-1} \left( \frac{a}{p} \right) \left( \frac{a + 1}{p} \right).$$

To obtain an estimate of the sum we prove the following theorem.

**Theorem 2.** Let $p$ be a prime and $\chi$ a nonprincipal character mod $p$. Let $1 \leq m \leq p$ and $l$ an integer such that $p \nmid l$. Then we have

$$\left| \sum_{a=0}^{m-1} \chi(a)\chi(a + l) \right| \leq 3 \sqrt{p} \ln p.$$

The proof makes an extensive use of Gauss sums and Kloosterman sums. Our main goal in this paper is to prove Theorem 2. The details are presented in Section 3.

2. Characters, Gauss sums and Kloosterman sums

Recall that $F_p$ is the finite field of residue classes mod $p$. Let $\chi$ be a character on $F_p$ and $a \in F_p$. Set

$$G(a, \chi) = \sum_t \chi(t)e^{2\pi iat/p},$$

where the sum is over all $t$ in $F_p$. $G(a, \chi)$ is called a Gauss sum on $F_p$ belonging to the character $\chi$.

The following propositions are well-known. The reader is referred to [5].

**Proposition 3.** If $a \neq 0$ and $\chi \neq \varepsilon$, we have $G(a, \chi) = \overline{\chi(a)}G(1, \chi)$. If $a \neq 0$ and $\chi = \varepsilon$, we have $G(a, \chi) = 0$. If $a = 0$ and $\chi \neq \varepsilon$, we have $G(0, \chi) = 0$. If $a = 0$ and $\chi = \varepsilon$, we have $G(a, \chi) = p$. Here $\overline{\chi(a)}$ is the complex conjugate of $\chi(a)$.

**Proposition 4.** If $\chi \neq \varepsilon$ then $|G(1, \chi)| = \sqrt{p}$.

**Proposition 5** (Inversion). For any character $\chi$ on $F_p$ and any $k \in F_p$ we have

$$\chi(k) = \frac{1}{p} \sum_{a \in F_p} G(a, \chi)e^{-2\pi iak/p}.$$

A Kloosterman sum with multiplicative characters is a sum of the form

$$\sum_{\substack{x_1x_2\cdots x_n = a \\ x_i \in F_p - \{0\}}} \chi_1(x_1)\chi_2(x_2) \cdots \chi_n(x_n)e^{2\pi ik(x_1 + x_2 + \cdots + x_n)/p},$$
Here, \( a \) and \( k \) are two nonzero elements of \( F_p \). The literature on Kloosterman sums is extensive. The interested reader should consult [6] and the bibliography therein. For the purpose of this paper, we are concerned with the case where \( a = 1 \) and \( n = 2 \). We mention the following difficult theorem.

**Theorem 6.**

\[
\left| \sum_{\substack{x,\beta = 1 \\ x,\beta \in F_p}} \chi_1(x) \chi_2(\beta) e^{2\pi i k (x+\beta)/p} \right| \leq 2\sqrt{p}.
\]

*Here \( \chi_1 \) and \( \chi_2 \) are two characters on \( F_p \) and \( k \neq 0 \).*

The proof of theorem requires a fairly complete knowledge of algebraic geometry. However, a brief outline is provided below: By a theorem of Deligne [3,6] the sum in question is \((-1)^{\text{trace}(F_1 | KI_1)}\). As the Kloosterman sum here is lisse of rank 2 and pure of weight 1, we have

\[
|\text{trace}(F_1 | KI_1)| \leq 2(\sqrt{p})^{2-1} = 2\sqrt{p}.
\]

Hence the result follows.

### 3. Proof of Theorem 2

The proof makes use of converting an incomplete sum into a complete sum by introducing the indicator function. Let

\[
S := \sum_{a=0}^{m-1} \chi(a) \chi(a+l).
\]

By Proposition 5 we have

\[
\chi(a+l) = \frac{1}{p} \sum_{b=0}^{p-1} G(b, \chi) e^{-2\pi i b(a+l)/p}.
\]

(1)

Inserting (1) in \( S \) and interchanging the order of summation we get

\[
S = \frac{1}{p} \sum_{b=0}^{p-1} G(b, \chi) e^{-2\pi i b/l/p} \tilde{S}(b),
\]

(2)

where \( \tilde{S}(b) = \sum_{a=0}^{m-1} \chi(a) e^{-2\pi i a/p} \).

Introducing the indicator function \( g(a) \) of the interval \([0, m - 1]\), that is,

\[
g(a) = \begin{cases} 
1 & \text{if } 0 \leq a \leq m - 1, \\
0 & \text{if } m \leq a \leq p,
\end{cases}
\]

we can write

\[
\tilde{S}(b) = \sum_{a=0}^{p-1} \chi(a) e^{-2\pi i a/p} g(a).
\]
Plugging in \( \hat{S}(b) \) the well known [4] formula for \( g(a) \) i.e.,

\[
g(a) = \frac{m}{p} + \frac{1}{p} \sum_{n=1}^{p-1} e^{2\pi i a/p} \left( \frac{1 - e^{-2\pi i n/m}}{1 - e^{-2\pi i n/p}} \right),
\]

we have

\[
\hat{S}(b) = \frac{m}{p} G(-b, \chi) + \frac{1}{p} \sum_{n=1}^{p-1} \left( \frac{1 - e^{-2\pi i n/m}}{1 - e^{-2\pi i n/p}} \right) G(n - b, \chi).
\]

Insert the above equation in Eq. (2) to get

\[
S = S_1 + S_2,
\]

where

\[
S_1 = \frac{m}{p^2} \sum_{b=0}^{p-1} G(b, \chi) e^{-2\pi i b l/p} G(-b, \chi)
\]

and

\[
S_2 = \frac{1}{p^2} \sum_{b=0}^{p-1} G(b, \chi) e^{-2\pi i b l/p} \left\{ \sum_{n=1}^{p-1} \left( \frac{1 - e^{-2\pi i n/m}}{1 - e^{-2\pi i n/p}} \right) G(n - b, \chi) \right\}.
\]

The sum \( S_1 \) is easy to estimate using Propositions 3 and 4:

First, we apply Proposition 3 to \( S_1 \)

\[
S_1 = \frac{m}{p^2} G^2(1, \chi) \sum_{b=0}^{p-1} \tilde{\chi}(b) \tilde{\chi}(-b) e^{-2\pi i b l/p}.
\]

Note that \( \tilde{\chi} \) is also a character on \( F_p \), hence \( \tilde{\chi}(-b) = \tilde{\chi}(-1) \tilde{\chi}(b) \). So

\[
S_1 = \frac{m}{p^2} G^2(1, \chi) \tilde{\chi}(-1) S_{11},
\]

where

\[
S_{11} = \sum_{b=0}^{p-1} \tilde{\chi}^2(b) e^{-2\pi i b l/p}.
\]

Now if \( \chi \) is a real character (i.e. the Legendre symbol since the modulus \( p \) is a prime) and since \( p \not\mid l \) we have

\[
S_{11} = \sum_{b=1}^{p-1} e^{-2\pi i b l/p} = -1.
\]

If \( \chi \) is a complex character, so is \( \tilde{\chi}^2 \). Then by Proposition 3

\[
S_{11} = G(-l, \tilde{\chi}^2) = \chi^2(-l) G(1, \tilde{\chi}^2).
\]

Again by Proposition 4 we see that in both cases we always have

\[ |S_{11}| \leq \sqrt{p}. \]
Hence from (6) and note that $0 \leq m \leq p$

$$|S_1| \leq \frac{m}{p^2} |G(1, \chi)|^2 \sqrt{p} \leq \sqrt{p}. \quad (7)$$

We turn to estimate the sum $S_2$ in (5). Applying Proposition 3 to the Gauss sums in $S_2$ and interchanging the order of summation we get

$$S_2 = \frac{G^2(1, \chi)}{p} \sum_{n=1}^{p-1} \left( \frac{1 - e^{-2\pi im/p}}{1 - e^{-2\pi i/p}} \right) S_{21}, \quad (8)$$

where $S_{21} = \sum_{b=0}^{p-1} \tilde{\mu}(b) \tilde{\mu}(n - b)e^{-2\pi ib/p}$.

To make further progress, we combine the characters in the sum $S_{21}$. Thus

$$S_{21} = \sum_{b=0}^{p-1} \tilde{\mu}(b(n - b))e^{-2\pi ib/p}. \quad (9)$$

Inserting the inversion formula for $\tilde{\mu}(b(n - b))$ and interchanging the order of summation we obtain

$$S_{21} = \frac{1}{p} \sum_{a=1}^{p-1} G(a, \tilde{\mu}) \tilde{\Sigma}_{21}, \quad (10)$$

where

$$\tilde{\Sigma}_{21} = \sum_{b=0}^{p-1} e^{2\pi i(b(n - b)a + bl)/p}. \quad (11)$$

The term corresponding to $a = 0$ is dropped from the sum $S_2$ since $G(0, \tilde{\mu}) = 0$ by Proposition 3. The summation index $b$ in $\tilde{\Sigma}_{21}$ may be conveniently viewed as a field element in the field $F_p$, so we can complete the squares for the quadratic $b^2a - b(l + na)$. Thus

$$b^2a - b(l + na) = a \left( b - \frac{na + l}{2a} \right)^2 - \frac{(na + l)^2}{4a}. \quad (12)$$

Inserting this in the sum $\tilde{\Sigma}_{21}$ we get

$$\tilde{\Sigma}_{21} = e^{-2\pi i((na + l)^2/4a)/p} \sum_{b=0}^{p-1} e^{2\pi i(a - (na + l)/2a)^2/p}. \quad (13)$$

Now as $b$ runs through the field $F_p$ in the sum $\tilde{\Sigma}_{21}$ so does $b - (na + l)/2a$. Hence

$$\tilde{\Sigma}_{21} = e^{-2\pi i((na + l)^2/4a)/p} \sum_{b=0}^{p-1} e^{2\pi iab^2/p}. \quad (14)$$

Note that the sum $\sum_{b=0}^{p-1} e^{2\pi iab^2/p}$ is equal to $G(a, \chi_0)$ where $\chi_0$ is the Legendre symbol [4]. Hence by Proposition 3 we have

$$\tilde{\Sigma}_{21} = e^{-2\pi i((na + l)^2/4a)/p} \chi_0(a)G(1, \chi_0). \quad (15)$$
Here for consistency of notations we use $\chi_0(a)$ for $(a/p)$. Putting this in $S_{21}$ in (10) we arrive at
\[
S_{21} = \frac{G(1, \bar{\chi}) G(1, \chi_0)}{p} S'_{21},
\]
(14)
where
\[
S'_{21} = \sum_{a=1}^{p-1} \chi(a) \chi_0(a) e^{-2\pi i ((na+l)/4a)/p}.
\]

The sum $S'_{21}$ is related to a Kloosterman sum with characters as we shall demonstrate: Expand the quadratic in the exponent of $S'_{21}$ to get
\[
S'_{21} = e^{-2\pi i (nl)/p} \sum_{a=1}^{p-1} \chi(a) \chi_0(a) e^{-2\pi i ((n^2/4)a+((l^2/4)(1/a))/p)}.
\]
(15)
Recall that for Legendre symbol $\chi_0(a)$ we have $\chi_0(1/a) = \chi_0(1/a)$. Inserting $(n^2/4)a = \alpha$, and $(l^2/4)1/a = \beta$ in the sum $S'_{21}$ we have
\[
S'_{21} = e^{-2\pi i (nl/2)/p} K \left( \frac{4}{n^2} \right) \sum_{\alpha\beta = n^2 l^2/4} \chi(\alpha) \chi_0(\beta) e^{-2\pi i (\alpha + \beta)/p}.
\]
(16)
where
\[
S''_{21} = \sum_{\alpha, \beta = 1} \chi(\alpha') \chi_0(\beta') e^{-2\pi i (n/4)(\alpha' + \beta')/p}.
\]

We see that $S''_{21}$ is a Kloosterman sum with characters. By Theorem 6 we have $|S''_{21}| \leq 2\sqrt{p}$. This implies from (16) that
\[
|S'_{21}| \leq 2\sqrt{p}.
\]
(17)
Again from (17), (14) and Proposition 4 we see
\[
|S_{21}| = \left| \frac{G(1, \bar{\chi})}{p} \right| |G(1, \chi_0)| |S'_{21}| \leq |S''_{21}| \leq 2\sqrt{p}.
\]
(18)
With (18) at our disposal we can estimate the sum $S_2$ in (8).
\[
|S_2| \leq \frac{|G(1, \bar{\chi})|^2}{p^2} \left| \sum_{n=1}^{p-1} \left( \frac{1 - e^{-2\pi i n m/p}}{1 - e^{-2\pi i n/p}} \right) \right| |S_{21}|
\]
\[
\leq \frac{2}{\sqrt{p}} \sum_{n=1}^{p-1} \left| \frac{1 - e^{-2\pi i n m/p}}{1 - e^{-2\pi i n/p}} \right|.
\]
(19)
To finish estimating $S_2$ we note that
\[
\left| \frac{1 - e^{-2\pi in/p}}{1 - e^{-2\pi n/p}} \right| \leq \frac{2}{|1 - e^{-2\pi n/p}|} = \frac{1}{|\sin n\pi/p|}.
\]

By Jordan’s inequality which states that $\sin x \geq \frac{2}{\pi}x$, for $0 \leq x \leq \pi$, it is easy to show that
\[
\left| \sin \frac{n\pi}{p} \right| \leq 2 \left\langle \frac{n}{p} \right\rangle,
\]
where $\langle x \rangle$ denotes the distance between $x$ and the nearest integer to $x$. Hence
\[
\left| \frac{1 - e^{-2\pi in/p}}{1 - e^{-2\pi n/p}} \right| \leq \frac{1}{2\langle \frac{n}{p} \rangle}.
\]

(20)

Inserting this estimate in (19) we get
\[
|S_2| \leq \frac{2}{\sqrt{p}} \sum_{n=1}^{p-1} \frac{1}{2\langle \frac{n}{p} \rangle} \leq \frac{2}{\sqrt{p}} \sum_{n=1}^{(p-1)/2} \frac{p}{n} < 2\sqrt{p} \ln p.
\]

(21)

Combining (21), (7) and (5) we get
\[
|S| \leq \sqrt{p} + 2\sqrt{p} \ln p < 3\sqrt{p} \ln p.
\]

This completes the proof. $\square$

4. Uniform distribution of consecutive quadratic residues

As an easy application of Theorems 1 and 2 we demonstrate a uniform distribution of consecutive quadratic residues. Recall an integer $a$ is called a consecutive quadratic residue mod $p$ if both $a$ and $a + 1$ are quadratic residues mod $p$. Let $0 < \beta < 1$ and $C_\beta:=\{0 \leq a \leq \beta(p - 1): a$ is a consecutive quadratic residue mod $p\}$. Then the cardinality of $C_\beta$ can be expressed as
\[
|C_\beta| = \sum_{a=0}^{\lfloor \beta(p-1) \rfloor} \left( \frac{1}{2} \left( 1 + \left( \frac{a}{p} \right) \right) \right) \left( \frac{1}{2} \left( 1 + \left( \frac{a+1}{p} \right) \right) \right),
\]
where $(a/p)$ is, as usual, the Legendre symbol. Denote by $N_p$ the total number of consecutive quadratic residues mod $p$. Then the fraction of consecutive quadratic residues lying in the interval $[0, \beta(p - 1)]$ is
\[
\frac{|C_\beta|}{N_p} = \frac{1}{N_p} \frac{1}{4} \sum_{a=0}^{\lfloor \beta(p-1) \rfloor} \left( 1 + \left( \frac{a}{p} \right) + \left( \frac{a+1}{p} \right) + \left( \frac{a}{p} \right) \left( \frac{a+1}{p} \right) \right).
\]

An application of Theorems 1 and 2 to the above sum gives
\[
\frac{|C_\beta|}{N_p} = \frac{1}{4N_p} \left( \beta(p - 1) + O(\sqrt{p} \ln p) \right).
\]
It is well known that \( N_p = \frac{1}{4}(p - 4 - (\frac{-1}{p})) \) [4]. Hence
\[
\lim_{p \to \infty} \frac{|C_\beta|}{N_p} = \beta.
\]

5. Conclusion

The author believes that the results in this paper can be generalized in at least two directions. We can ask the following two questions.

First, let \( \chi \) be a nonprincipal character mod \( p \) and \( 1 \leq m \leq p \). Also let \( l_1, l_2, \ldots, l_k \) be \( k \) fixed distinct integers such that \( p | l_i \) for all \( 1 \leq i \leq k \). Is it true that there exists a number \( A_k \) depending only on \( k \) such that
\[
\left| \sum_{a=0}^{m-1} \chi(a)\chi(a + l_1) \cdots \chi(a + l_k) \right| \leq A_k \sqrt{p \ln p}.
\]

Secondly, we may generalize the notion of consecutive residue to \( k \)-consecutive residue mod \( p \). More explicitly, an integer \( a \) is said to be a \( k \)-consecutive residue if \( a, a+1, a+2, \ldots, a+k \) are all quadratic residues mod \( p \). Are \( k \)-consecutive residues asymptotically uniformly distributed?

An affirmative answer to the first question implies the affirmative answer to the second. Finally we may also generalize the notion of quadratic residues to cubic residues. Thus a similar question of uniform distribution of cubic residues can be asked.

Acknowledgements

The author is extremely grateful for many useful suggestions pointed out by an anonymous referee.

References