RANDOMNESS OF CHARACTER SUMS MODULO $m$

YOUNESS LAMZOURI AND ALEXANDRU ZAHARESCU

Abstract. Using a probabilistic model, based on random walks on the additive group $\mathbb{Z}/m\mathbb{Z}$, we prove that the values of certain real character sums are uniformly distributed in residue classes modulo $m$.

1. Introduction

A central question in number theory is to gain an understanding of character sums

$$S_{\chi}(x) = \sum_{n \leq x} \chi(n),$$

where $\chi$ is a Dirichlet character modulo $q$. When $q = p$ is a prime number and $\chi_p = \left(\frac{.}{p}\right)$ is the Legendre symbol modulo $p$, the character sums $S_p(x) = S_{\chi_p}(x)$ encode information on the distribution of quadratic residues and non-residues modulo $p$ (see for example Davenport and Erdős [5], and Peralta [13]). In particular, bounds for the order of magnitude of $S_p(x)$ lead to results on the size of the least quadratic non-residue modulo $p$ (see the work of Ankeny [2]; Banks, Garaev, Heath-Brown and Shparlinski [3]; Burgess [4]; Graham and Ringrose [6]; Lau and Wu [10]; Linnik [11]; and Montgomery [12]).

Quadratic residues and non-residues appear to occur in a rather random pattern modulo $p$, which suggests that the values of $\chi_p(n)$ mimic a random variable that takes the values 1 and $-1$ with equal probability $1/2$. This fact was recently exploited by Granville and Soundararajan [7] while investigating the distribution of the values of Dirichlet $L$-functions attached to quadratic characters at $s = 1$. Furthermore, a result of Davenport and Erdős [5] shows that short real character sums are indeed random in some sense. More specifically, they established that the values $S_p(n + H) - S_p(n)$ are distributed according to a Gaussian distribution of mean zero and variance $H$ as $H \to \infty$ in the range $\log H / \log p \to 0$ when $p \to \infty$.

In this paper, we investigate a new aspect of the randomness of these character sums. To describe our results, we first need some notation. Let $F(X)$ be a square-free

2010 Mathematics Subject Classification. Primary 11L40; Secondary 11B50, 60G50.

Key words and phrases. Character sums, distribution in residue classes, random walks on finite groups.

The First author is supported by a postdoctoral fellowship from the Natural Sciences and Engineering Research Council of Canada. Research of the second author is supported by the NSF grant DMS-0901621.
polynomial of degree $d_F \geq 1$ over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and define 
\[ S_p(F,k) := \sum_{n \leq k} \chi_p(F(n)), \]
for all positive integers $k \leq p$. Moreover, let $\Phi_p(F; m, a)$ be the proportion of positive integers $k \leq p$ for which $S_p(F,k) \equiv a \mod m$; that is 
\[ \Phi_p(F; m, a) = \frac{1}{p}|\{k \leq p : S_p(F,k) \equiv a \mod m\}|. \]
Since the values $\chi_p(F(n))$ are expected to be randomly distributed, one might guess that $\Phi_p(F; m, a) \sim 1/m$ for all $a \mod m$ as $p \to \infty$. We show that this is indeed the case in Corollary 1 below, uniformly for all $m$ in the range $m = o((\log p)^{1/4})$ as $p \to \infty$. Our strategy is to introduce a probabilistic model for the values $S_p(F,k)$ based on random walks. A simple random walk on $\mathbb{Z}$ is a stochastic process $\{S_k\}_{k \geq 1}$ where 
\[ S_k = X_1 + \cdots + X_k, \]
and $\{X_j\}_{j \geq 1}$ is a sequence of independent random variables taking the values 1 and $-1$ with equal probability $1/2$ (for further reference see Spitzer [14]). We shall model the values $S_p(F,k) \mod m$ by the stochastic process $\{S_k \mod m\}$ which may be regarded as a simple random walk on the additive group $\mathbb{Z}/m\mathbb{Z}$. To this end we consider the random variable 
\[ \Phi_{\text{rand}}(N; m, a) := \frac{1}{N}|\{k \leq N : S_k \equiv a \mod m\}|. \]
Here and throughout $\mathbb{E}(Y)$ will denote the expectation of the random variable $Y$. We first study the probabilistic model and prove

**Proposition 1.** Let $m \geq 2$ be a positive integer. Then, for all $N \geq m^2$ we have 
\[ \sum_{a=0}^{m-1} \mathbb{E} \left( \left( \Phi_{\text{rand}}(N; m, a) - \frac{1}{m} \right)^2 \right) \ll \frac{m^2}{N}. \]

Appealing to Markov’s inequality, we deduce from this result that 
\[ \Phi_{\text{rand}}(N; m, a) = \frac{1}{m}(1 + o(1)) \]
with probability $1 - o(1)$ provided that $N/m^2 \to \infty$.

Using Proposition 1, we establish an analogous estimate for the second moment of the difference $\Phi_p(F; m, a) - 1/m$ (which may be regarded as the “variance” of $\Phi_p(F; m, a)$).

**Theorem 1.** Let $p$ be a large prime number and $F(X) \in \mathbb{F}_p(X)$ be a square-free polynomial of degree $d_F \geq 1$. Then, for any integer $2 \leq m \ll (\log p)^{1/4}$ we have 
\[ \sum_{a=0}^{m-1} \left( \Phi_p(F; m, a) - \frac{1}{m} \right)^2 \ll_{d_F} \frac{m^2}{\log p}. \]
As a consequence, we obtain

**Corollary 1.** Under the same assumptions of Theorem 1, we have uniformly for all $0 \leq a \leq m - 1$

$$\Phi_p(F; m, a) = \frac{1}{m} + O_{d_F} \left( \frac{m}{\sqrt{\log p}} \right).$$

Let $R_p(F, k)$ be the number of positive integers $n \leq k$ such that $F(n)$ is a quadratic residue modulo $p$, and similarly denote by $N_p(F, k)$ the number of $n \leq k$ for which $F(n)$ is a quadratic non-residue mod $p$. Using a slight variation of our method we also prove that the values $R_p(F, k)$ (and $N_p(F, k)$) are uniformly distributed in residue classes modulo $m$. In this case, the corresponding probabilistic model involves random walks on the non-negative integers, where each step is 0 or 1 with equal probability. Define

$$\tilde{\Phi}_p(F; m, a) = \frac{1}{p} |\{k \leq p : R_p(F, k) \equiv a \mod m\}|.$$

Then, using a similar result to Proposition 1 in this case (see Proposition 3.3 below) we establish

**Theorem 2.** Let $p$ be a large prime number and $F(X) \in \mathbb{F}_p(X)$ be a square-free polynomial of degree $d_F \geq 1$. Then, for any integer $2 \leq m \ll (\log p)^{1/4}$ we have

$$\sum_{a=0}^{m-1} \left( \tilde{\Phi}_p(F; m, a) - \frac{1}{m} \right)^2 \ll_{d_F} \frac{m^2}{\log p}.$$

A similar result holds replacing $R_p(F, k)$ with $N_p(F, k)$.

An important question in the theory of random walks on finite groups is to investigate how close is the distribution of the $k$-th step of the walk to the uniform distribution on the corresponding group (see for example Hildebrand [8]). In our case this corresponds to investigating the distribution of $S_k \mod m$. Define

$$\Psi_{\text{rand}}(k; m, a) = \text{Prob}(S_k \equiv a \mod m).$$

**Proposition 2.** Let $m \geq 3$ be an odd integer and $0 \leq a \leq m - 1$. Then

$$\Psi_{\text{rand}}(k; m, a) = \frac{1}{m} + O \left( \exp \left( -\frac{\pi^2 k}{3m^2} \right) \right).$$

This shows that the distribution of $S_k$ is close to the uniform distribution on $\mathbb{Z}/m\mathbb{Z}$ when $m = o(k^{1/2})$ as $k \to \infty$. Although this result is classical (see for example Theorem 2 of Aldous and Diaconis [1]), we chose to include its proof for the sake of completeness.

We now describe an analogous result that we derive for character sums. Let $N$ be large, and for each prime $p \leq N$, we consider the walk on $\mathbb{Z}/m\mathbb{Z}$ whose $i$-th step corresponds to the value of $\chi_p(q_i) \mod m$, where $q_i$ is the $i$-th prime number. One might guess that as $p$ varies over the primes below $N$, the distribution of the $k$-th step of this
walk will be close to the uniform distribution in \(\mathbb{Z}/m\mathbb{Z}\), as \(N, k \to \infty\) if \(m = o(k^{1/2})\).
Define
\[
S_k(p) = \sum_{j \leq k} \chi_p(q_j),
\]
and
\[
\Psi_N(k; m, a) = \frac{1}{\pi(N)}|\{p \leq N : S_k(p) \equiv a \mod m\}|.
\]

Here and throughout \(\log_j\) will denote the \(j\)-th iterated logarithm, so that \(\log_1 n = \log n\) and \(\log_j n = \log(\log_{j-1} n)\) for each \(j \geq 2\). We prove

**Theorem 3.** Fix \(A \geq 1\). Let \(N\) be large, and \(k \leq A(\log_2 N)/(\log_3 N)\) be a positive integer. Then we have
\[
\Psi_N(k; m, a) = \Psi_{\text{rand}}(k; m, a) + O_A\left(\frac{1}{\log^A N}\right).
\]

Hence, using Proposition 2 we deduce

**Corollary 2.** Let \(m\) be an odd integer such that \(3 \leq m \leq k^{1/2}\). Then under the same assumptions of Theorem 3 we have uniformly for all \(0 \leq a \leq m - 1\) that
\[
\Psi_N(k; m, a) = \frac{1}{m} + O_A\left(\exp\left(-\frac{\pi^2 k}{3m^2}\right) + \frac{1}{\log^A N}\right).
\]

We remark that under the assumption of the Generalized Riemann Hypothesis for Dirichlet \(L\)-functions, we can improve the range of validity of Theorem 3 to \(k \ll (\log N)/(\log_2 N)\).

### 2. Preliminary lemmas

In this section we collect together some preliminary results which will be useful in our subsequent work. Here and throughout we shall use the notation \(e_m(x) = \exp\left(\frac{2\pi ix}{m}\right)\).
Recall the orthogonal relation
\[
\frac{1}{m} \sum_{t=0}^{m-1} e_m(tn) = \begin{cases} 
1 & \text{if } n \equiv 0 \mod m, \\
0 & \text{otherwise.}
\end{cases}
\]

Our first lemma gives the classical bound for incomplete exponential sums over \(\mathbb{F}_p\) of the form
\[
S_I(P_1, P_2) = \sum_{n \in I} \chi_p(P_1(n))e_p(P_2(n)),
\]
where \(I\) is a subinterval of \(\{0, 1, \ldots, p-1\}\), and \(P_1(X), P_2(X) \in \mathbb{F}_p[X]\), such that \(P_1(X)\) is a nontrivial square-free polynomial.

**Lemma 2.1.** Let \(p \geq 3\) be a prime number and \(I, P_1(X), P_2(X)\) be as above. Then we have
\[
|S_I(P_1, P_2)| \leq 2D\sqrt{p}\log p,
\]
where
\[ D = \deg P_1(X) + \deg P_2(X). \]

**Proof.** First if \( I = \{0, \ldots, p - 1\} \), then \( S_I(P_1, P_2) = S(P_1, P_2) \) is a complete sum and the result follows from the classical Weil bound for exponential sums [15]:
\[ |S(P_1, P_2)| \leq Dp^{1/2}. \tag{2.2} \]

Now, if \( I \) is proper subinterval of \( \{0, \ldots, p - 1\} \), we shall use a standard procedure to express our incomplete sum in terms of complete sums of the same type. Using equation (2.1) we see that
\[ S_I(P_1, P_2) = \sum_{n \mod p} \chi_p(P_1(n)) e_p(P_2(n)) \left( \sum_{m \in I} \frac{1}{p} \sum_{t \mod p} e_p(t(m - n)) \right). \]

Changing the order of summation and noting that the inner double sum is a product of two sums, one being a geometric progression and the other a complete exponential sum, we obtain
\[ S_I(P_1, P_2) = \frac{1}{p} \sum_{t \mod p} \left( \sum_{m \in I} e_p(tm) \right) \left( \sum_{n \mod p} \chi_p(P_1(n)) e_p(P_2(n) - tn) \right) \]
\[ = \frac{1}{p} \sum_{t \mod p} F_I(t) S(P_1, \tilde{P}_2), \tag{2.3} \]

where \( \tilde{P}_2(X) = P_2(X) - tX \) and \( F_I(t) = \sum_{m \in I} e_p(tm) \). If \( t \equiv 0 \mod p \) then \( F_I(t) = |I| \). Otherwise if \( I = \{M + 1, \ldots, M + N\} \), say, then
\[ F_I(t) = \frac{e_p(t(M + 1)) - e_p(t(M + N + 1))}{1 - e_p(t)}. \]

Here the numerator has absolute value at most 2, while the absolute value of the denominator is \( 2|\sin(t\pi/p)| \). Hence
\[ |F_I(t)| \leq \left| \sin \left( \frac{t\pi}{p} \right) \right|^{-1} \leq \left( 2 \left| \frac{t}{p} \right| \right)^{-1}, \]

where \( \| \cdot \| \) stands for the distance to the nearest integer. As a set of representatives modulo \( p \) we choose \( \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\} \), so that for \( t \neq 0 \) in this set we have
\[ |F_I(t)| \leq \frac{p}{2|t|}. \tag{2.4} \]

Now, we insert (2.2) and (2.4) in (2.3) to obtain
\[ |S_I(P_1, P_2)| \leq \frac{D}{p^{1/2}} \left( |I| + \sum_{1 \leq |t| \leq \frac{p}{2|t|}} \frac{p}{2|t|} \right) \leq 2D \sqrt{p} \log p. \]

This completes the proof of the lemma. \qed

The following lemma will be later used to prove that the product of distinct shifts of a square-free polynomial cannot be a square in \( \mathbb{F}_p(X) \).
Lemma 2.2. Let \( r \geq 2 \), and \( z_1, \ldots, z_r \), be distinct elements of \( \mathbb{F}_p \). Moreover, let \( \mathcal{M} \) be a nonempty finite subset of the algebraic closure \( \overline{\mathbb{F}}_p \) of \( \mathbb{F}_p \) with \( 4|\mathcal{M}| < p^{\frac{1}{2}} \). Then there exists a \( j \in \{1, \ldots, r\} \) such that the translate \( \mathcal{M} + z_j \) is not contained in \( \bigcup_{i \neq j}(\mathcal{M} + z_i) \).

Proof. Suppose that \((z_1, \ldots, z_r, \mathcal{M})\) provides a counterexample to the statement of the lemma. Then clearly for any nonzero \( t \in \mathbb{F}_p \), \((tz_1, \cdots, tz_r, t\mathcal{M})\) is also a counterexample.

We now use Minkowski’s theorem on lattice points in a symmetric convex body to find a nonzero integer \( t \) such that
\[
\begin{aligned}
|t| &\leq p - 1 \\
\left|\frac{tz_j}{p}\right| &\leq (p - 1)^{-\frac{1}{2}} \\
\vdots \\
\left|\frac{tz_r}{p}\right| &\leq (p - 1)^{-\frac{1}{2}}
\end{aligned}
\]

Another way to express this is that there are integers
\[
(2.5) \quad \begin{cases}
|y_j| \leq p(p - 1)^{-\frac{1}{2}} \\
y_j &\equiv tz_j \pmod{p}
\end{cases}
\]

for any \( j \in \{1, \ldots, r\} \). Thus \((y_1, \ldots, y_r, t\mathcal{M})\) provides a counterexample. Now let \( j_0 \) be such that
\[
|y_{j_0}| = \max_{1 \leq j \leq r} |y_j|.
\]

Choose \( \alpha \in t\mathcal{M} \) and consider the set \( \tilde{\mathcal{M}} = t\mathcal{M} \cap (\alpha + \mathbb{F}_p) \). Then \((y_1, \ldots, y_r, \tilde{\mathcal{M}})\) will also be a counterexample.

Note that \( \alpha + \mathbb{F}_p \) can be written as a union of \(|\mathcal{M}| \) intervals whose endpoints are in \( \tilde{\mathcal{M}} \). Let \( \{\alpha + a, \alpha + a + 1, \cdots, \alpha + b\} \) be the longest of these intervals. Then
\[
|b - a| \geq \frac{p}{|\mathcal{M}|} \geq \frac{p}{|\tilde{\mathcal{M}}|}.
\]

By this, \((2.5)\) and the hypothesis \( 4|\mathcal{M}| < p^{\frac{1}{2}} \) we deduce
\[
|b - a| > 4p^{1 - \frac{1}{2}} > 2|y_{j_0}|.
\]

Now the point is that if \( y_{j_0} > 0 \) then \( \alpha + a + y_{j_0} \) belongs to \( \tilde{\mathcal{M}} + y_{j_0} \) but does not belong to \( \bigcup_{i \neq j_0}(\tilde{\mathcal{M}} + y_i) \), while if \( y_{j_0} < 0 \) then \( \alpha + b + y_{j_0} \) belongs to \( \tilde{\mathcal{M}} + y_{j_0} \) but does not belong to \( \bigcup_{i \neq j_0}(\tilde{\mathcal{M}} + y_i) \). This completes the proof of the lemma. \( \square \)

Using this lemma, we prove the following result

Lemma 2.3. Let \( F(X) \in \mathbb{F}_p(X) \) be a square-free polynomial of degree \( d_F \geq 1 \). Let \( b_1, \ldots, b_L \) be distinct elements in \( \mathbb{F}_p \) such that \( L < (\log p)/\log(4d_F) \). Then, for any
a ∈ ℱ_p the polynomial

\[ H(X) = \prod_{j=1}^{L} F(aX + b_j), \]

is not a square in ℱ_p(X).

Proof. Let \( \alpha_1, \ldots, \alpha_s \) be the roots of \( F(X) \) in ℱ_p. Since \( F(X) \) is square-free then the \( \alpha_j \) are distinct and \( s = d_F \). Let \( M = \{ a^{-1}\alpha_1, \ldots, a^{-1}\alpha_s \} \), and write \( z_j = -a^{-1}b_j \) for all \( 1 \leq j \leq L \). Then note that \( M + z_j \) is the set of the roots of \( F(ax + b_j) \) in ℱ_p. By our hypothesis it follows that \( 4|F_p(X)| < p^{1/L} \). Hence, we infer from Lemma 2.2 that there exists a \( j \in \{1, \ldots, L\} \) such that at least one of the roots of \( F(ax + b_j) \) is distinct from all the roots of \( \prod_{l \neq j} F(ax + b_l) \). This shows that \( H(X) \) is not a square in ℱ_p(X) as desired.

\[ \square \]

3. Random walks on the integers modulo \( m \)

In this section we shall study the distribution of the random walk \( \{S_k \mod m\}_{k \geq 1} \) and prove Propositions 1 and 2. To this end, we establish the following preliminary lemmas.

Lemma 3.1. If \( m \geq 3 \) is an odd integer, then

\[
\max_{1 \leq t \leq m-1} \left| \cos \left( \frac{2\pi t}{m} \right) \right| \leq 1 - \frac{\pi^2}{3m^2},
\]

and

\[
\max_{1 \leq t \leq m-1} |1 + e_m(t)| \leq 2 - \frac{\pi^2}{6m^2}.
\]

Proof. We begin by proving the first assertion. If \( m \geq 5 \) is odd, then

\[
\max_{1 \leq t \leq m-1} \left| \cos \left( \frac{2\pi t}{m} \right) \right| = \cos \left( \frac{2\pi}{m} \right).
\]

Moreover we know that \( \cos(x) \leq 1 - x^2/3 \) for \( 0 \leq x \leq \pi/2 \). This yields

\[
\max_{1 \leq t \leq m-1} \left| \cos \left( \frac{2\pi t}{m} \right) \right| \leq 1 - \frac{4\pi^2}{3m^2}.
\]

Now, when \( m = 3 \) we have \( \max_{1 \leq t \leq 2} |\cos(2\pi t/m)| = \cos(\pi/m) \leq 1 - \pi^2/(3m^2) \). This establishes the first part of the lemma.

Moreover, we have

\[
|1 + e_m(t)|^2 = 2 + 2 \cos(2\pi t/m) \leq 4 \left( 1 - \frac{\pi^2}{6m^2} \right),
\]

which follows from (3.1). Therefore, using that \( \sqrt{1-x} \leq 1 - x/2 \) for \( 0 \leq x \leq 1 \) we obtain the second assertion of the lemma. \( \square \)
Lemma 3.2. If \( m \geq 2 \) is an integer, then
\[
\sum_{t=1}^{m-1} \sum_{1 \leq j_1 < j_2 \leq N} \cos \left( \frac{2\pi t}{m} \right)^{j_2-j_1} = O(m^3N),
\]
and
\[
\sum_{t=1}^{m-1} \sum_{1 \leq j_1 < j_2 \leq N} \left( \frac{1 + e_m(t)}{2} \right)^{j_2-j_1} = O(m^3N).
\]

Proof. We prove only the first statement, since the proof of the second is similar. For \( d \in \{1, \ldots, N-1\} \), the number of pairs \( 1 \leq j_1 < j_2 \leq N \) such that \( j_2 - j_1 = d \) equals \( N - d \). Therefore, the sum we are seeking to bound equals
\[
\sum_{t=1}^{m-1} \sum_{d=1}^{N-1} (N-d) \cos \left( \frac{2\pi t}{m} \right)^d.
\]

First, when \( m \) is odd, Lemma 3.1 implies that the last sum is
\[
\leq mN \sum_{d=1}^{N-1} \max_{1 \leq t \leq m-1} \left| \cos \left( \frac{2\pi t}{m} \right)^d \right| \leq \frac{mN}{1 - \max_{1 \leq t \leq m-1} \left| \cos \left( \frac{2\pi t}{m} \right) \right|} \leq \frac{3m^3N}{\pi^2}.
\]

Now, when \( m = 2r \) is even, then either \( \cos(\pi t/r) = -1 \) or \( |\cos(\pi t/r)| < 1 \). In the latter case the proof of Lemma 3.1 implies that \( |\cos(\pi t/r)| \leq 1 - \pi^2/(3r^2) \). Hence, in this case we obtain
\[
\sum_{d=1}^{N-1} (N-d) \left| \cos \left( \frac{\pi t}{r} \right) \right|^d \ll m^2N.
\]

On the other hand if \( \cos(\pi t/r) = -1 \), then our sum become
\[
\sum_{d=1}^{N-1} (N-d)(-1)^d \leq 2N.
\]

This completes the proof. \( \square \)

We begin by proving Proposition 2 first, since its proof is both short and simple.

Proof of Proposition 2. Recall that
\[
\Psi_{\text{rand}}(k; m, a) = \text{Prob}(X_1 + \cdots + X_k \equiv a \mod m) = \frac{1}{2^k} \sum_{v=(v_1,\ldots,v_k) \in \{-1,1\}^k \atop v_1 + \cdots + v_k \equiv a \mod m} 1.
\]

Hence, using (2.1) we deduce
\[
\Psi_{\text{rand}}(k; m, a) = \frac{1}{2^k m} \sum_{v=(v_1,\ldots,v_k) \in \{-1,1\}^k} \sum_{t=0}^{m-1} e_m \left( t(v_1 + \cdots + v_k - a) \right).
\]
The contribution of the term \( t = 0 \) to the above sum equals \( 1/m \). Moreover, since \( \sum_{a \in \{-1,1\}} e_m(\alpha t) = 2 \cos(2\pi t/m) \), then the contribution of the remaining terms equals
\[
\frac{1}{2k^m} \sum_{t=1}^{m-1} e_m(-at) \sum_{v=(v_1,\ldots,v_k) \in \{-1,1\}^k} e_m(t(v_1+\cdots+v_k)) = \frac{1}{m} \sum_{t=1}^{m-1} e_m(-at) \cos \left( \frac{2\pi t}{m} \right)^k.
\]

Thus, the result follows upon using Lemma 3.1.

\[\square\]

**Proof of Proposition 1.** First, note that
\[
\Phi_{\text{rand}}(N; m, a) = \frac{1}{N} \sum_{j=1}^{N} Y_j \quad \text{where} \quad Y_j = \begin{cases} 1 & \text{if } S_j \equiv a \mod m \\ 0 & \text{otherwise.} \end{cases}
\]

On the other hand, if \( \mathbf{v} = (v_1, \ldots, v_N) \in \{-1,1\}^N \), then (2.1) yields
\[
|\{1 \leq j \leq N : v_1 + \cdots + v_j \equiv a \mod m\}| = \frac{1}{m} \sum_{j=1}^{N} \sum_{t=0}^{m-1} e_m(t(v_1 + \cdots + v_j - a)).
\]

This implies
\[
(3.4)
\]
\[
\mathbb{E} \left( \left( \Phi_{\text{rand}}(N; m, a) - \frac{1}{m} \right)^2 \right) = \frac{1}{2N} \sum_{\mathbf{v} \in \{-1,1\}^N} \left( \frac{1}{N} \sum_{v_1 + \cdots + v_j \equiv a \mod m} 1 - \frac{1}{m} \right)^2.
\]

Now, expanding the summand on the RHS of (3.4) we derive
\[
\left| \sum_{j=1}^{N} \sum_{t=0}^{m-1} e_m(t(v_1 + \cdots + v_j - a)) - N \right|^2 = \sum_{j=1}^{N} \sum_{t=1}^{m-1} e_m(t(v_1 + \cdots + v_j - a))^2 \left( \sum_{1 \leq j_1, j_2 \leq N} e_m(t_1(v_1 + \cdots + v_{j_1}) - t_2(v_1 + \cdots + v_{j_2})) \right).
\]

Hence, we infer from (2.1) that
\[
(3.5)
\]
\[
\sum_{a=0}^{m-1} \sum_{j=1}^{N} \sum_{t=0}^{m-1} e_m(t(v_1 + \cdots + v_j - a)) - N \right|^2 = m \sum_{t=1}^{m-1} \sum_{1 \leq j_1, j_2 \leq N} e_m(t((v_1 + \cdots + v_{j_1}) - (v_1 + \cdots + v_{j_2})))
\]
\[
= m^2 N + m \sum_{t=1}^{m-1} \sum_{1 \leq j_1, j_2 \leq N} \left( e_m(t(v_{j_1+1} + \cdots + v_{j_2})) + e_m(-t(v_{j_1+1} + \cdots + v_{j_2})) \right).
\]
Inserting this estimate into (3.4), and using that $\sum_{\alpha \in \{-1,1\}} e_m(\alpha t) = 2 \cos(2\pi t/m)$, we obtain
\[
\sum_{a=0}^{m-1} \mathbb{E} \left( \left( \Phi_{\text{rand}}(N; m, a) - \frac{1}{m} \right)^2 \right) = \frac{1}{N} + \frac{2}{mN^2} \sum_{t=1}^{m-1} \sum_{1 \leq j_1 < j_2 \leq N} \cos \left( \frac{2\pi t}{m} \right)^{j_2-j_1}.
\]

The result follows upon using Lemma 3.2 to bound the RHS of the last identity. \hfill \Box

In order to prove Theorem 2 we require an analogous result to Proposition 1 in the case of a random walk on the non-negative integers, where each step is 0 or 1 (rather than $-1$ or 1). To this end, we take $\{\tilde{X}_j\}_{j \geq 1}$ to be a sequence of independent random variables taking the values 0 and 1 with equal probability $1/2$, and define
\[
\tilde{S}_k = \tilde{X}_1 + \cdots + \tilde{X}_k,
\]
and
\[
\tilde{\Phi}_{\text{rand}}(N; m, a) = \frac{1}{N} |\{1 \leq j \leq N : \tilde{S}_j \equiv a \mod m\}|.
\]

Using a similar approach to the proof of Proposition 1 we establish:

**Proposition 3.3.** Let $m \geq 2$ be a positive integer. Then, for all $N \geq m^2$ we have
\[
\sum_{a=0}^{m-1} \mathbb{E} \left( \left( \tilde{\Phi}_{\text{rand}}(N; m, a) - \frac{1}{m} \right)^2 \right) \ll \frac{m^2}{N}.
\]

**Proof.** We follow closely the proof of Proposition 1. First, a similar analysis used to derive (3.4) allows us to obtain
\[
\mathbb{E} \left( \left( \tilde{\Phi}_{\text{rand}}(N; m, a) - \frac{1}{m} \right)^2 \right) = \frac{1}{2N(mN)^2} \sum_{v=(v_1, \ldots, v_N) \in \{0,1\}^N} \left| \sum_{j=1}^{N} \sum_{t=0}^{m-1} e_m(t(v_1 + \cdots + v_j - a)) - N \right|^2.
\]

Hence, using the identity (3.5) in equation (3.6) we get
\[
\sum_{a=0}^{m-1} \mathbb{E} \left( \left( \tilde{\Phi}_{\text{rand}}(N; m, a) - \frac{1}{m} \right)^2 \right) = \frac{1}{N} + \frac{1}{mN^2} \sum_{t=1}^{m-1} \sum_{1 \leq j_1 < j_2 \leq N} \left( \frac{1 + e_m(t)}{2} \right)^{j_2-j_1} + \left( \frac{1 + e_m(-t)}{2} \right)^{j_2-j_1}
\]
\[
= \frac{1}{N} + \frac{2}{mN^2} \sum_{t=1}^{m-1} \sum_{1 \leq j_1 < j_2 \leq N} \left( \frac{1 + e_m(t)}{2} \right)^{j_2-j_1},
\]

upon noting that
\[
\sum_{t=1}^{m-1} \left( \frac{1 + e_m(t)}{2} \right)^d = \sum_{r=1}^{m-1} \left( \frac{1 + e_m(-r)}{2} \right)^d.
\]
by making the simple change of variables $r = m - t$. Appealing to Lemma 3.2 completes
the proof.

\[\square\]

4. Character sums with polynomials: proof of Theorems 1 and 2

We begin by proving the following key proposition which establishes the required
link with random walks. Let $p$ be a large prime number and $F(X) \in \mathbb{F}_p(X)$ be a
square-free polynomial of degree $d_F \geq 1$ in $\mathbb{F}_p(X)$. Moreover, let $L \leq (\log p)/\log(4d_F)$
be a positive integer, and put $N = [p/L] - 1$. Furthermore, for any $\mathbf{v} = (v_1, \ldots, v_L) \in
\{-1, 1\}^L$ we define

\[D_{p,F}(\mathbf{v}, L) = \{0 \leq s \leq N : \chi_p(F(sL + j)) = v_j \text{ for all } 1 \leq j \leq L}\].

**Proposition 4.1.** Let $p$, $L$, and $F(X)$ be as above. Then for any $\mathbf{v} = (v_1, \ldots, v_L) \in
\{-1, 1\}^L$ we have

\[|D_{p,F}(\mathbf{v}, L)| = \frac{p}{2L} \left(1 + O_{d_F}(p^{-1/10})\right).
\]

**Proof.** Let $S$ be the set of non-negative integers $0 \leq s \leq N$ such that $F(sL + j) \neq 0$
for all $1 \leq j \leq L$. Then $|S| = N + O_{d_F}(1)$. Moreover, note that for $s \in S$ we have

\[\frac{1}{2L} \prod_{j=1}^{L} (1 + v_j \chi_p(F(sL + j))) = \begin{cases} 
1 & \text{if } s \in D_{p,F}(\mathbf{v}, L), \\
0 & \text{otherwise}.
\end{cases}
\]

This yields

\[|D_{p,F}(\mathbf{v}, L)| = \frac{1}{2L} \sum_{s=0}^{N} \prod_{j=1}^{L} (1 + v_j \chi_p(F(sL + j))) + O_{d_F}(1).
\]

Expanding the product on the RHS of the previous estimate, we find that $|D_{p,F}(\mathbf{v}, L)|$
equals

\[\frac{1}{2L} \sum_{s=0}^{N} \left(1 + \sum_{i_1=1}^{L} \sum_{1 \leq i_1 < i_2 < \cdots < i_L \leq L} v_{i_1} \cdots v_{i_L} \chi_p(F(sL + i_1) \cdots F(sL + i_L)) \right) + O_{d_F}(1).
\]

\[= \frac{N}{2L} + \frac{1}{2L} \sum_{i_1=1}^{L} \sum_{1 \leq i_1 < \cdots < i_L \leq L} v_{i_1} \cdots v_{i_L} \sum_{s=0}^{N} \chi_p(F(sL + i_1) \cdots F(sL + i_L)) + O_{d_F}(1).
\]

Since $F(X)$ is a square-free polynomial, then it follows from Lemma 2.3 that the
polynomial $H_{i_1,\ldots,i_L}(X) = F(LX + i_1) \cdots F(LX + i_L)$ is not a square in $\mathbb{F}_p(X)$. Therefore,
using Lemma 2.1 with $P_1(X) = H_{i_1,\ldots,i_L}(X)$, $P_2(X) = 0$ and $I = \{0, \ldots, N\}$, we obtain

\[\left|\sum_{s=0}^{N} \chi_p(F(sL + i_1) \cdots F(sL + i_L))\right| \leq 2d_F L \sqrt{p \log p}.
\]
Inserting this bound in (4.3) we get
\[
|D_{p,F}(v, L)| = \frac{p}{2L} + O_d \left( L \sqrt{p \log p} \right),
\]
which completes the proof. \(\square\)

**Proof of Theorem 1.** Recall that
\[
\Phi_p(F; m, a) = \frac{1}{p} \left| \{1 \leq k \leq p : S_p(F, k) \equiv a \mod m\} \right|.
\]

Let \(L = \lceil (\log p) / (\log(4d_F)) \rceil\), and put \(N = \lceil p/L \rceil - 1\). Moreover, for any \(0 \leq s \leq N\), we define
\[
M_L(s; m, a) = \left| \{1 \leq l \leq L : S_p(F, sL + l) \equiv a \mod m\} \right|.
\]

Then, note that
\[
|\Phi_p(F; m, a) - \frac{1}{m}| \leq \frac{1}{p} \sum_{s=0}^{N} \left| M_L(s; m, a) - \frac{L}{m} \right| + O \left( \frac{L}{p} \right).
\]

To bound the sum on the RHS of (4.5), we use the Cauchy-Schwarz inequality which gives
\[
\left( \sum_{s=0}^{N} \left| M_L(s; m, a) - \frac{L}{m} \right| \right)^2 \leq (N + 1) \sum_{s=0}^{N} \left( M_L(s; m, a) - \frac{L}{m} \right)^2.
\]

Hence, combining this estimate with (4.5), we deduce
\[
\left( \Phi_p(F; m, a) - \frac{1}{m} \right)^2 \ll \frac{N}{p^2} \sum_{s=0}^{N} \left( M_L(s; m, a) - \frac{L}{m} \right)^2 + \frac{L^2}{p^2}.
\]

On the other hand, since \(S_p(sL + l) = S_p(sL) + \sum_{j=1}^{l} \chi_p(F(sL + j))\), then
\[
\sum_{a=0}^{m-1} \left( M_L(s; m, a) - \frac{L}{m} \right)^2 = \sum_{b=0}^{m-1} \left( \Delta_L(s; m, b) - \frac{L}{m} \right)^2,
\]
where
\[
\Delta_L(s; m, b) = \left| \{1 \leq l \leq L : \sum_{j=1}^{l} \chi_p(F(sL + j)) \equiv b \mod m\} \right|.
\]

Therefore, upon combining (4.6) and (4.7) we obtain
\[
\sum_{a=0}^{m-1} \left( \Phi_p(F; m, a) - \frac{1}{m} \right)^2 \ll \frac{N}{p^2} \sum_{a=0}^{m-1} \sum_{s=0}^{N} \left( \Delta_L(s; m, a) - \frac{L}{m} \right)^2 + \frac{mL^2}{p^2}.
\]
Now we evaluate the inner sum on the RHS of the previous inequality. Using (2.1) we get

\[ \sum_{s=0}^{N} \left( \Delta_L(s; m, a) - \frac{L}{m} \right)^2 = \frac{1}{m^2} \sum_{s=0}^{N} \left| \sum_{t=0}^{L-1} \sum_{t=1}^{m-1} e_m \left( t \sum_{1 \leq j \leq l} \chi_p(F(sL + j)) - a \right) - L \right|^2 \]

\[ = \frac{1}{m^2} \sum_{s=0}^{N} \left| \sum_{t=1}^{L-1} \sum_{t=1}^{m-1} e_m \left( t \sum_{1 \leq j \leq l} \chi_p(F(sL + j)) - a \right) \right|^2 \]

\[ \approx \frac{1}{m^2} \sum_{\nu \in \{-1, 1\}^L} \left| \sum_{t=1}^{L} \sum_{t=1}^{m-1} e_m \left( t(v_1 + \cdots + v_l) - \frac{1}{m} \right) \right|^2 D_{p,F}(\nu, L). \]

Hence, using Proposition 4.1 along with the identity \((3.4)\) obtained in the random walk setting, we derive

\[ \sum_{s=0}^{N} \left( \Delta_L(s; m, a) - \frac{L}{m} \right)^2 \]

\[ = \frac{p}{2^{2L} m^2 L} \sum_{\nu \in \{-1, 1\}^L} \left| \sum_{t=1}^{L} \sum_{t=1}^{m-1} e_m \left( t(v_1 + \cdots + v_l) \right) \right|^2 \left( 1 + O_{d_F} \left( p^{-1/10} \right) \right) \]

\[ = pL \mathbb{E} \left( \left( \Phi_{\text{rand}}(L; m, a) - \frac{1}{m} \right)^2 \right) \left( 1 + O_{d_F} \left( p^{-1/10} \right) \right). \]

Finally, combining this estimate with \((4.8)\) we obtain

\[ \sum_{a=0}^{m-1} \left( \Phi_p(F; m, a) - \frac{1}{m} \right)^2 \ll_{d_F} \sum_{a=0}^{m-1} \mathbb{E} \left( \left( \Phi_{\text{rand}}(L; m, a) - \frac{1}{m} \right)^2 \right) + \frac{m(\log p)^2}{p^2} \]

\[ \ll_{d_F} \frac{m^2}{\log p}, \]

which follows from Proposition 1. This completes the proof.

\[ \square \]

**Proof of Theorem 2.** We only prove the result for \(R_p(F, k)\), since the proof for \(N_p(F, k)\) is similar. Define

\[ \delta_F(j) = \begin{cases} 1 & \text{if } \chi_p(F(j)) = 1, \\ 0 & \text{otherwise}. \end{cases} \]

Then, note that

\[ R_p(F, k) = \sum_{j=1}^{k} \delta_F(j). \]

We follow closely the proof of Theorem 1. Let \(L = \lfloor (\log p)/\log(4d_F) \rfloor\), and \(N = \lfloor p/L \rfloor - 1\). For any \(0 \leq s \leq N\) we define

\[ \Delta_L(s; m, b) = \left| \{1 \leq l \leq L : \sum_{j=1}^{l} \delta_F(sL + j) \equiv b \mod m\} \right|. \]
Therefore, inserting this estimate (4.10) we obtain
\[
\sum_{a=0}^{m-1} \left( \Phi_p(F; m, a) - \frac{1}{m} \right)^2 \ll \frac{N}{p^2} \sum_{a=0}^{m-1} \sum_{s=0}^{N} \left( \Delta_L(s; m, a) - \frac{L}{m} \right)^2 + \frac{m(\log p)^2}{p^2}.
\]

Moreover, an analogous approach which leads to the identity (4.9) also gives
\[
\sum_{s=0}^{N} \left( \Delta_F(s; m, a) - \frac{L}{m} \right)^2 = \frac{1}{m^2} \sum_{v \in \{0, 1\}^L} \left| \sum_{t=1}^{L} \sum_{t=1}^{m-1} a^t \left(t(v_1 + \cdots + v_l - a)\right) \right|^2 \sum_{0 \leq s \leq N} 1.
\]

Remark that if \(F\) does not vanish in the interval \([sL + 1, sL + L]\) then
\[
\delta_F(sL + j) = \frac{1 + \chi_p(F(sL + j))}{2},
\]
for all \(1 \leq j \leq L\). Hence, writing \(\tilde{v} = (\tilde{v}_1, \ldots, \tilde{v}_L)\) with \(\tilde{v}_j = 2v_j - 1\), we deduce
\[
\sum_{0 \leq s \leq N} 1 = |D_p(\tilde{v}, L, F)| + O_{d_F}(1) = \frac{p}{2L} \left( 1 + O_{d_F} \left( p^{-1/10} \right) \right),
\]
which follows from Proposition 4.1. Thus, appealing to the identity (3.6) obtained in the random walk setting, we derive
\[
\sum_{s=0}^{N} \left( \Delta_F(s; m, a) - \frac{L}{m} \right)^2 = pL \mathbb{E} \left[ \left( \Phi_{\text{rand}}(L; m, a) - \frac{1}{m} \right)^2 \right] \left( 1 + O_{d_F} \left( p^{-1/10} \right) \right).
\]

Therefore, inserting this estimate in (4.10) and using Proposition 3.3 we obtain
\[
\sum_{a=0}^{m-1} \left( \Phi_p(F; m, a) - \frac{1}{m} \right)^2 \ll_{d_F} \sum_{a=0}^{m-1} \mathbb{E} \left[ \left( \Phi_{\text{rand}}(L; m, a) - \frac{1}{m} \right)^2 \right] + \frac{m(\log p)^2}{p^2}
\ll_{d_F} \frac{m^2}{\log p},
\]
as desired. \(\Box\)

5. Character sums of fixed length: Proof of Theorem 3

We shall derive Theorem 3 from the following proposition

Proposition 5.1. Fix \(A \geq 1\). Let \(N\) be large, and \(k \leq A(\log_2 N)/(\log_3 N)\). Then for any \(v = (v_1, \ldots, v_k) \in \{-1, 1\}^k\) we have
\[
\frac{1}{\pi(N)} |\{p \leq N : \chi_p(q_j) = v_j \text{ for all } 1 \leq j \leq k\}| = \frac{1}{2^k} \left( 1 + O_A \left( \frac{1}{\log^A N} \right) \right).
\]

Proof. If \(\log N \leq p \leq N\) then
\[
\frac{1}{2^k} \prod_{j=1}^{k} (1 + v_j \chi_p(q_j)) = \begin{cases} 
1 & \text{if } \chi_p(q_j) = v_j \text{ for all } 1 \leq j \leq k, \\
0 & \text{otherwise.}
\end{cases}
\]
Therefore we deduce that the number of primes \( p \leq N \) such that \( \chi_p(q_j) = v_j \) for all \( 1 \leq j \leq k \), equals

\[
\left( 1 + \frac{v_j}{m} \right) \left( 1 + \frac{v_i}{m} \right) + \cdots + \left( 1 + \frac{v_k}{m} \right) + O(\log N)
\]

\[
(5.1) = \frac{1}{2^k} \sum_{p \leq N} \left( 1 + \sum_{1 \leq i_1 < \cdots < i_k \leq k} v_{i_1} \cdots v_{i_k} \chi_p(q_{i_1} \cdots q_{i_k}) \right) + O(\log N)
\]

\[
= \frac{\pi(N)}{2^k} + \frac{1}{2^k} \sum_{1 \leq i_1 < \cdots < i_k \leq k} v_{i_1} \cdots v_{i_k} \sum_{p \leq N} \left( 1 + \frac{v_{i_1} \cdots v_{i_k}}{m} \right) + O(\log N).
\]

For \( 1 \leq i_1 < \cdots < i_k \leq k \) we let \( Q_{i_1, \ldots, i_k} = q_{i_1} \cdots q_{i_k} \). Then it follows from the prime number theorem that \( Q_{i_1, \ldots, i_k} \leq \prod_{j=1}^k q_j = e^{k \log k + o(1)} \leq (\log N)^{1+o(1)} \). On the other hand, quadratic reciprocity implies that \( (Q_{i_1, \ldots, i_k}) \) is a character of modulus \( Q_{i_1, \ldots, i_k} \) or \( 4Q_{i_1, \ldots, i_k} \). Therefore, appealing to the Siegel-Walfisz Theorem (see Corollary 5.29 of Iwaniec-Kowalski [9]), we deduce

\[
\sum_{p \leq N} \left( Q_{i_1, \ldots, i_k} \right) \ll (Q_{i_1, \ldots, i_k})^{1/2} \frac{N}{\log^{2A} N}.
\]

Inserting this estimate in (5.1) completes the proof. \( \square \)

**Proof of Theorem 3.** Using (2.1) we obtain

\[
\Psi_N(k; m, a) = \frac{1}{\pi(N)} |\{p \leq N : S_k(p) \equiv a \mod m\}|.
\]

\[
(5.2) = \frac{1}{m \pi(N)} \sum_{p \leq N} \sum_{t=0}^{m-1} e_m(t(S_k(p) - a))
\]

\[
= \frac{1}{m \pi(N)} \sum_{t=0}^{m-1} \sum_{v \in \{-1,1\}^k} e_m(t(v_1 + \cdots + v_k - a)) \sum_{p \leq N} 1_{\chi_p(q_j) = v_j} \text{ for } 1 \leq j \leq k
\]

Thus, appealing to Proposition 5.1 along with the identity (3.3) obtained in the random walk setting we derive

\[
\Psi_N(k; m, a) = \frac{1}{2^k m} \sum_{t=0}^{m-1} \sum_{v \in \{-1,1\}^k} e_m(t(v_1 + \cdots + v_k - a)) + O_A \left( \frac{1}{\log^4 N} \right)
\]

\[
= \Psi_{\text{rand}}(k; m, a) + O_A \left( \frac{1}{\log^4 N} \right),
\]

which completes the proof. \( \square \)

**References**

[1] D. Aldous and P. Diaconis, *Shuffling cards and stopping times*, Amer. Math. Monthly 93 (1986), no. 5, 333-348.
[2] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) 55, (1952). 65-72.

[3] W. Banks, M. Z. Garaev, D. R. Heath-Brown and I. E. Shparlinski, *Density of non-residues in Burgess-type intervals and applications*, Bull. Lond. Math. Soc. 40 (2008), 88-96.

[4] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 1957 106-112.

[5] H. Davenport and P. Erdős, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen 2, (1952). 252-265.

[6] S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic nonresidues*, Analytic number theory (Allerton Park, IL, 1989), 269–309.

[7] A. Granville and K. Soundararajan, *The distribution of values of L(1, χd)*, Geometric and Funct. Anal. 13 (2003), 992–1028.

[8] M. Hildebrand, *A survey of results on random walks on finite groups*, Probab. Surv. 2 (2005), 33-63.

[9] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[10] Y. K. Lau and J. Wu, *On the least quadratic non-residue*, Int. J. Number Theory 4 (2008), no. 3, 423-435.

[11] U. V. Linnik, *A remark on the least quadratic non-residue*, C. R. (Doklady) Acad. Sci. URSS (N.S.) 36 (1942) 119-120.

[12] H. L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, Vol. 227. Springer-Verlag, Berlin-New York, 1971.

[13] R. Peralta, *On the distribution of quadratic residues and nonresidues modulo a prime number*, Math. Comp. 58 (1992), no. 197, 433-440.

[14] F. Spitzer, *Principles of random walks*, Graduate Texts in Mathematics, Vol. 34. Springer-Verlag, New York-Heidelberg, 1976.

[15] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. 34, (1948). 204-207.

Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA

E-mail address: lamzouri@math.uiuc.edu

Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA

E-mail address: Zaharesu@math.uiuc.edu