Character sums and arithmetic combinatorics

Mei-Chu Chang

Abstract In this survey we review some old and new results on character sums and their applications to various problems in analytic number theory, e.g., smallest quadratic nonresidues, Dirichlet L-function, Linnik's problem. We also discuss open problems in this area. Some of the techniques involved belong to arithmetic combinatorics. One may hope for these methods to lead to further progress.

Keywords Character sums • Zero-free regions.

Mathematics Subject Classification (2010): 11L40, 11M06.

A function $\chi : \mathbb{Z}/q\mathbb{Z} \to \{z \in \mathbb{C} : |z| = 1\} \cup \{0\}$ is a multiplicative character mod q if it satisfies the properties that $\chi(mn) = \chi(m)\chi(n)$, and $\chi(n) = 0$ if $\gcd(n, q) \neq 1$. We are interested in bounding non-trivially the character sum of χ over an interval of length $H \leq q$. More precisely, we want to study the following problem.

Problem 1. *Assuming χ is non-principal and $q \gg 0$, how small $H = H(q)$ can be such that*

$$\Big|\sum_{n=a+1}^{a+H} \chi(n)\Big| < H^{1-\epsilon} \ ? \tag{1}$$

In 1918, Polya and Vinogradov (Theorem 12.5 in [27]) had the estimate for $H \gg \sqrt{q}\log q$.

Theorem 1 (Polya-Vinogradov). *Let χ be a non-principal Dirichlet character* mod q. *Then*

$$\Big|\sum_{m=a+1}^{a+H} \chi(m)\Big| < Cq^{\frac{1}{2}}(\log q).$$

M.-C. Chang (✉)
Department of Mathematics, University of California, Riverside, CA 92521, USA
e-mail: mcc@math.ucr.edu

A. Beveridge et al. (eds.), *Recent Trends in Combinatorics*, The IMA Volumes in Mathematics and its Applications 159, DOI 10.1007/978-3-319-24298-9_17

Forty four years later Burgess [5] improved Polya and Vinogradov's result to $H > q^{\frac{1}{4}+\varepsilon}$, first for prime moduli, then for cube-free moduli.

Theorem 2 (Burgess). *For $\varepsilon > 0$ there exists $\delta > 0$ such that if $H > p^{\frac{1}{4}+\varepsilon}$, then*

$$\Big|\sum_{m=a+1}^{a+H} \chi(m)\Big| \ll p^{-\delta} H.$$

Using sieving, there is the following

Corollary 1. *The smallest quadratic nonresidue* mod *p is at most $p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.*

At present time, Burgess' estimate is still the best. Davenport and Lewis generalized it to higher dimensions by replacing the interval by a box $B \subset \mathbb{F}_{p^n}$.

Let $\{\omega_1, \dots, \omega_n\}$ be an arbitrary basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Then for any $x \in \mathbb{F}_{p^n}$, there is a unique representation of x in terms of the basis.

$$x = x_1\omega_1 + \cdots + x_n\omega_n$$

A *box* $B \subset \mathbb{F}_{p^n}$ is a set such that for each j, the coefficients x_j form an interval.

$$\begin{aligned} B &= \Big\{\sum_{j=1}^{n} x_j\omega_j : x_j \in [a_j+1, a_j+H_j], \quad \forall i\Big\} \\ &= \prod_{j=1}^{n} [a_j+1, a_j+H_j]. \end{aligned} \tag{2}$$

Davenport and Lewis had the following non-trivial estimate for character sums over boxes. (See [6, 28] for work on special boxes.)

Theorem 3. [12, Theorem 2] *Let $H_j = H$ for $j = 1, \dots, n$, with*

$$H > p^{\frac{n}{2(n+1)}+\delta} \text{ for some } \delta > 0 \tag{3}$$

and let $p > p(\delta)$. Then, with B defined as above

$$\Big|\sum_{x\in B} \chi(x)\Big| < (p^{-\delta_1} H)^n,$$

where $\delta_1 = \delta_1(\delta) > 0$.

For $n = 1$ (i.e., $\mathbb{F}_q = \mathbb{F}_p$) this is Burgess' result. But as n increases, the exponent in (3) tends to $\frac{1}{2}$.

Motivated by the work of Burgess and Davenport-Lewis, we obtained the following estimates on incomplete character sums. Our result improves Theorem DL for $n > 4$ [7, 8] and is also uniform in n.

Theorem 4. *Let χ be a non-trivial multiplicative character of $\mathbb{F}_{p^n}$, and let $\varepsilon > 0$ be given. If*

$$B = \prod_{j=1}^{n} [a_j + 1, a_j + H_j]$$

is a box satisfying

$$\prod_{j=1}^{n} H_j > p^{(\frac{2}{5}+\varepsilon)n},$$

then for $p > p(\varepsilon)$

$$\Big|\sum_{x\in B} \chi(x)\Big| \ll_n p^{-\frac{\varepsilon^2}{4}} |B|,$$

unless n is even and $\chi|_{F_2}$ is principal, where F_2 is the subfield of size $p^{n/2}$, in which case

$$\Big|\sum_{x\in B} \chi(x)\Big| \le \max_{\xi} \big|B \cap \xi F_2\big| + O_n(p^{-\frac{\varepsilon^2}{4}} |B|).$$

The proof of Theorem 4 used ingredients and techniques from sum–product theory, specially multiplicative energy. Theorem 4 was improved by Konyagin [30] for regular boxes.

Theorem 5. [30] *Let χ be a non-trivial multiplicative character of $\mathbb{F}_{p^n}$, and let B be given as in* (2) *with*

$$H_j = H > p^{\frac{1}{4}+\epsilon}, \quad \forall j.$$

Then

$$\Big|\sum_{x\in B} \chi(x)\Big| \ll_n p^{-\delta} |B|,$$

where $\delta = \delta(\epsilon) > 0$.

Problem 2. *Obtain a non-trivial estimate on $\sum_{x\in B} \chi(x)$, assuming $|B| > q^{1/4+\varepsilon}$ and B not 'essentially' contained in a multiplicative translate of a subfield.*

As in [12] (see p. 131), Theorem 4 has the following application to the distribution of primitive roots of $\mathbb{F}_{p^n}$.

Corollary 2. *Let $B \subset \mathbb{F}_{p^n}$ be as in Theorem 4 and satisfying $\max_\xi \left|B \cap \xi F_2\right| < p^{-\varepsilon}|B|$ if n even. The number of primitive roots of $\mathbb{F}_{p^n}$ belonging to B is*

$$\frac{\varphi(p^n-1)}{p^n-1}|B|(1+o(p^{-\tau'})),$$

where $\tau' = \tau'(\varepsilon) > 0$ and assuming $n \ll \log\log p$.

The proof of Corollary 2 is by combining character sums estimate with the following.

$$\frac{\phi(p^n-1)}{p^n-1}\left\{1+\sum_{\substack{d|p^n-1\\ d>1}}\frac{\mu(d)}{\phi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(x)\right\} = \begin{cases}1 \text{ if } x \text{ is primitive,}\\ 0 \text{ otherwise.}\end{cases}$$

We also generalize Burgess's inequality in a slightly different direction.

Theorem 6. *Let $\mathcal{P}$ be a proper d-dimensional generalized arithmetic progression in $\mathbb{F}_p$ with*

$$|\mathcal{P}| > p^{\frac{2}{5}+\varepsilon}, \text{ some } \varepsilon > 0$$

If χ is a non-principal multiplicative character of $\mathbb{F}_p$, we have

$$\left|\sum_{x\in\mathcal{P}}\chi(x)\right| < p^{-\tau}|\mathcal{P}|,$$

where $\tau = \tau(\varepsilon, d) > 0$ and assuming $p > p(\varepsilon, d)$.

Remark 6.1. The exponent $\frac{2}{5} < \frac{1}{2}$ does not depend on d.

Remark 6.2. Similar results hold for $\mathbb{F}_{p^n}$ with worse exponent.

Using Freiman's theorem, sum–product, and character sums, we obtained the following.

Corollary 3. *Given $C > 0$ and $\varepsilon > 0$, there is a constant $\kappa = \kappa(C, \varepsilon)$ and a positive integer $k < k(C, \varepsilon)$ such that if $A \subset \mathbb{F}_p$ satisfies*

(i) $|A| > p^{2/5+\varepsilon}$
(ii) $|A + A| < C|A|$.

Then we have

$$|A^k| > \kappa p,$$

where $A^k = A \cdots A$ is the k-fold product set of A.

There is also the study of multi-linear character sums.

Let $(L_j)_{1\le j\le n}$ be n independent linear forms in n variables over $\mathbb{F}_p$, and let χ be a non-principal multiplicative character mod p. Denote a box by $B = \prod_{i=1}^{n} [a_i,\ a_i + H]$. We are interested in the following non-trivial estimates

$$\Big|\sum_{x\in B} \chi\Big(\prod_{j=1}^{n} L_j(x)\Big)\Big| < p^{-\delta} H^n. \tag{4}$$

Theorem 7 (Burgess). *Assume*

$$H > p^{\frac{1}{2}-\frac{1}{2(n+1)}+\varepsilon}. \tag{5}$$

Then (4) *holds.*

For $n = 1$, condition (5) is the well-known Burgess assumption $H > p^{\frac{1}{4}+\varepsilon}$ for character sum bound. For $n = 2$, it is $H > p^{\frac{1}{3}+\varepsilon}$. We generalized the Burgess assumption to any dimension. (See [4].)

Theorem 8 (Bourgain-Chang). *Assume*

$$H > p^{\frac{1}{4}+\varepsilon}, \quad \textit{for any } n.$$

Then (4) *holds.*

The theorem above has application to character sums of polynomials.

Theorem 9. *Let $f(x_1, \dots, x_d)$ be a homogeneous polynomial of degree d and split over $\overline{\mathbb{F}}_p$, and let $B = \prod_{i=1}^{d} [a_i, a_i + H] \subset \mathbb{F}_p^d$ be a box of length H with*

$$H = p^{\frac{1}{4}+\varepsilon}.$$

Then

$$\Big|\sum_{x\in B} \chi(f(x))\Big| < p^{-\delta} H^d.$$

This improves Gillett's condition $H > p^{\frac{d}{2(d+1)}+\varepsilon}$.

Coming back to Problem 1, for special moduli, the condition on H in Burgess' theorem can be improved. One can proved (1) for much smaller intervals. There are two classical results, based on quite different arguments by Graham–Ringrose ([27], Corollary 12.15) and Iwaniec ([27], Theorem 12.16).

First, for the modulus q, we set up the following notations for the largest prime divisor $\mathcal{P}$ of q, and the *core* k of q.

$$\mathcal{P} = \max_{p|q} p \quad \text{and} \quad k = \prod_{p|q} p.$$

Theorem 10. [18] *Let χ be a primitive character of modulus $q \geq 3$ with q square free. Then, for*

$$N = |I| \geq q^{\frac{4}{\sqrt{\log\log q}}} + \mathcal{P}^9$$

we have

$$\Big|\sum_{n \in I} \chi(n)\Big| \ll N e^{-\sqrt{\log q}}.$$

The purpose of the work of Graham and Ringrose is to study the following least quadratic nonresidue problem.

Problem 3. *Let p be a prime, and let $n(p)$ be the least quadratic nonresidue mod p. Find a lower bound on $n(p)$.*

Independent of Burgess' result $n(p) \leq p^{\frac{1}{4\sqrt{e}}+\varepsilon}$, Friedlander [14] and Salié [35] showed that $n(p) = \Omega(\log p)$, i.e., there are infinitely many p such that $n(p) > c \log p$ for some absolute constant c. By assuming the Generalized Riemann Hypothesis, in 1971 Montgomery [33] proved that $n(p) = \Omega(\log p \ \log\log p)$. Using Theorem 10, Graham and Ringrose showed that $n(p) = \Omega(\log p \ \log\log\log p)$ unconditionally.

In 1974, Iwaniec [26] proved the following theorem by generalizing Postnikov's theorem [34].

Theorem 11. [34] *Let χ be a primitive character of modulus q, $2 \nmid q$. Then, for*

$$k^{100} < N < N' \leq 2N \tag{6}$$

we have

$$\Big|\sum_{N < n \leq N'} \chi(n)\Big| \leq C^{s(\log s)^2} N^{1-\frac{c}{s^2 \log s}},$$

where $s = \frac{\log q}{\log N}$.

Theorem 11 is good for q powerful. A related problem is about the digital aspects of the primes. Let $x < N = 2^n$. Write

$$x = x_0 + 2x_1 + 2^2 x_2 + \cdots + 2^{n-1} x_{n-1} \quad \text{with} \quad x_0, x_1, \cdots, x_{n-1} \in \{0, 1\}.$$

For $A \subset \{1, \cdots, n\}$, given $\{\alpha_j \in \{0,1\}\}_{j \in A}$, one expects

$$\big|\{p = x < N : x_j = \alpha_j, \ \forall j \in A\}\big| \sim \frac{N}{\log N}\, 2^{-|A|}.$$

Problem 4. *How large can A be?*

For related work, see Sierpinski [39], Harman–Katai [22], Bourgain [3].

Theorem 10 is for q with small prime factors (smooth moduli), for which one assumes

$$\log N \gg \log \mathcal{P} + \frac{\log q}{\sqrt{\log \log q}}. \tag{7}$$

On the other hand, Theorem 11 is for q with small core. Condition (6) implies that

$$\log N \gg \log k. \tag{8}$$

If fix k, to get non-trivial result, in Theorem 11, one needs to assume

$$\log N \gg \log k + (\log q)^{\frac{3}{4}+\epsilon}. \tag{9}$$

Both are special cases of the following theorem in [11].

Denote

$$K = \frac{\log q}{\log k}.$$

Theorem 12. *Assume N satisfies*

$$q > N > \mathcal{P}^{10^3}$$

and

$$\log N > (\log q)^{\frac{9}{10}} \;+\; 10^3 \,\frac{\log 2K}{\log \log q}\, \log k\;. \tag{10}$$

Let χ be a primitive multiplicative character modulo q and I an interval of size N. Then

$$\Big|\sum_{x\in I} \chi(x)\Big| \ll N e^{-(\log N)^{3/5}}. \tag{11}$$

Remark 12.1. In the same spirit as assumptions (7) and (9), assumption (10) can be replaced by the stronger and friendlier assumption.

$$\log N \gg \log \mathcal{P} \;+\; \frac{\log q}{\log \log q}. \tag{12}$$

(The second term of condition (12) is clearly bigger than either term of (10).)

Remark 12.2. This result is completely general and gives bounds for very short character sums as soon as $\log \mathcal{P}$ is small compared with $\log q$.

Remark 12.3. To compare Theorem 12 with Theorem 10, we note also that condition (12) gives a better result than (7). Moreover, condition (7) is restricted to square free q. As for comparing Theorem 12 with Theorem 11, we let k be square free and $q = k^m$, where m is large but not too large. More precisely, we assume $\log m = o(\log\log k)$. Theorem 11 certainly requires that $\log N > C \log k$ while condition (10) in Theorem 12 becomes $\log N > (m \log k)^{\frac{9}{10}} + C \frac{\log m}{\log\log q} \log k$, which is clearly better.

Remark 12.4. We did not try to optimize the power of $\log q$ in the first term in (10) nor the saving in (11).

The following is a mixed character sum version of Theorem 12 (see also [10]).

Theorem 13. [15] *Under the assumptions of Theorem 12,*

$$\Big| \sum_{x \in I} \chi(x) e^{if(x)} \Big| < N e^{-\sqrt{\log N}}$$

assuming $f(x) \in \mathbb{R}[x]$ *of degree at most* $(\log N)^c$ *for some* $c > 0$.

Corollary 4. *Let* $T > 0$. *Assume* N *satisfies*

$$q > N > \mathcal{P}^{10^3}$$

and q *satisfies*

$$\log N > (\log qT)^{\frac{9}{10}} + 10^3 \frac{\log 2K}{\log\log q} \log k.$$

Then for χ *primitive, we have*

$$\Big| \sum_{n \in I} \chi(n) n^{it} \Big| < N e^{-\sqrt{\log N}} \quad \textit{for} \quad |t| < T.$$

Following the classical arguments going back to Hadamand, de-la-Vallee-Poissin, and Landau, the above estimates lead to zero-free regions for the corresponding Dirichlet L-functions. Denote

$$L(s, \chi) = \sum_n \chi(n) n^{-s}, \qquad s = \rho + it.$$

Iwaniec [26] obtained the following results.

Theorem 14. [26] *Assume* $|L(s, \chi)| < M$ *for* $\rho > 1 - \eta$, $|t| < T^2$. *Then* $L(s, \chi)$ *has no zeros in the region* $\rho > 1 - \frac{\eta}{400 \log M}$, $|t| < T$, *except for possible Siegel zeros.*

Corollary 5. [26] *Assume Y and $\gamma > 0$ satisfy*

$$\Big|\sum_{n\sim N}\chi(n)n^{it}\Big| < N^{1-\gamma} \quad \textit{for } N > Y, |t| < T.$$

Then

$$\rho > 1 - \frac{c}{\log Y + \frac{1}{\gamma}\ \log\frac{1}{\gamma} + \frac{1}{\gamma}\ \log\log\frac{qT}{Y}}\ .$$

From Corollary 4 and Corollary 5, one derives bounds on the Dirichlet L-function $L(s,\chi)$ and zero-free regions the usual way. For a detailed argument, see, for instance, Lemmas 8–11 in [26]. This leads to the following theorem.

Theorem 15. *Let χ be a primitive multiplicative character with modulus q. For $T > 0$, let*

$$\theta = c\min\Big(\frac{1}{\log\mathcal{P}}, \frac{\log\log k}{(\log k)\log 2K}, \frac{1}{(\log qT)^{9/10}}\Big).$$

Then the Dirichlet L-function $L(s,\chi) = \sum_n \chi(n)n^{-s}$, $s = \rho + it$ has no zeros in the region $\rho > 1-\theta,\ |t| < T$, except for possible Siegel zeros.

It follows in particular that $\theta\log qT \to \infty$ if $\frac{\log\mathcal{P}}{\log q} \to 0$.

In certain range of k, this improves Iwaniec's bound (See [27], Theorem 8.29.)

$$\theta = \min\Big\{c\ \frac{1}{(\log T)^{\frac{2}{3}}(\log\log T)^{\frac{1}{3}}}\ , \frac{1}{\log k}\Big\}.$$

A well-known application of zero-free region is to primes in arithmetic progressions. In 1944, Linnik proved the following theorem about the least prime in an arithmetic progression.

Theorem 16. [31, 32] *There exists c such that if $(a,q) = 1$, then there is a prime $p < q^c$ such that $p \equiv a$ mod q.*

For explicit value of c in Theorem 16, Xylouris [40] has the best estimate $c = 5.2$ by using Heath-Brown [23, 24] (who obtained $c = 5.5$) proposed improvements.

Theorem 15 gives a lower c for q smooth.

Theorem 17. *In Theorem 16, one may take $c = \frac{12}{5} + \epsilon$, assuming $\log\mathcal{P} < \frac{\log q}{\log\log q}$.*

Estimates on short character sums are also related to Polya–Vinogradov's theorem. Based on the work of Granville and Soundararajan [19] (which characterizes when character sums are large), Goldmakher [17] used Theorem 10 to improve Polya–Vinogradov's bound on $\sum_{n<x}\chi(n)$ and obtained the following.

Theorem 18. [18] *Let* χ mod q *be a primitive character. Then*

$$\Big|\sum_{n<x}\chi(n)\Big| \ll \sqrt{q}\ \log q\ \sqrt{\log^3 q}\ \Big(\frac{1}{\log^2 q}+\frac{\log\mathcal{P}}{\log q}\Big)^{\frac{1}{4}}.$$

When q *is square free, then*

$$\Big|\sum\chi(n)\Big| \ll \sqrt{q}\ \ \frac{\log q}{(\log\log q)^{\frac{1}{4}}}.$$

Instead of Theorem 10, we use Theorem 17 (and Granville–Soundararajan) and obtain the following.

Corollary 6. *Let* χ mod q *be a primitive character, and let*

$$M=(\log q)^{\frac{9}{10}}+(\log 2K)\frac{\log k}{\log\log k}+\log\mathcal{P}.$$

Then

$$\Big|\sum_{n<x}\chi(n)\Big| \ll \sqrt{q}\ \ \sqrt{\log q}\ \ \sqrt{M}\ \ \sqrt{\log\log\log q}.$$

When q *is square free,*

$$\Big|\sum_{n<x}\chi(n)\Big| \ll \sqrt{q}\ \ \frac{\log q}{(\log\log q)^{\frac{1}{2}}}.$$

Let $f(x_1,\dots,x_n)\in\mathbb{F}_q[x_1,\dots,x_n]$, $q=p^\ell$ be a polynomial of degree d. We are interested in bounding the exponential sum

$$S=\sum_{x_1,\dots,x_n} e_p\Big(\mathrm{Tr}\big(f(x_1,\dots,x_n)\big)\Big) \tag{13}$$

as well as a certain incomplete sums where the variables are restricted to a 'box' $B\subset\mathbb{F}_q^n$. More specifically, we consider various instances of this question where Deligne type estimates are not applicable, either because f is too singular or the box B is too small. In their work on Gowers' norms, Green and Tao [20] obtain non-trivial bounds in the situation where $\mathbb{F}_q=\mathbb{F}_p$ and d are fixed and n is large, assuming that the value of f is not determined by a few polynomials of lower degree.

Problem 5. *Obtain quantitative version of the Green–Tao result.*

For Problem 5, see the recent result by Forni and Flaminio [13].

Estimates of this type are also particularly relevant to circuit complexity [21].

Using methods from geometry of numbers, W. Schmidt [36] obtained bounds on incomplete sums (13) over boxes, but without exploring the effect of large n or ℓ.

Problem 6. *Investigate the bounds obtained in* [36] *when n or ℓ is large.*

It is possible that techniques from arithmetic combinatorics may be relevant.
For $n = 1$, estimates of this type are obtained in [2].
There are some other problems related to Problem 1.

Problem 7. *Let V be a vector subspace of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, not essentially contained in a multiplicative translate of a subfield. Under what assumptions on $\dim_{\mathbb{F}_p} V$ can one obtain non-trivial bounds on $\sum_{x\in V} \chi(x)$?*

The arithmetic combinatorics approach permits to go below the $n/2$ barrier of classical methods. We are particularly interested in the situation where p is fixed and n is large. Assuming $\xi \in \mathbb{F}_{p^n}$ a generator, one may specify further $V = \langle \xi^j : j \in S\rangle$ with $S \subset \{0, 1, \dots, n-1\}$. In the special case $S = \{0, 1, \dots, m\}$, V. Shoup [38] used the Hasse–Weil method to get results for $m = O(\log n)$.

In the paper [8], we also succeeded in improving Karacuba's result on character sums of the type

$$\sum_{x\in I} \Big|\sum_{y\in A} \chi(x+y)\Big|, \tag{14}$$

where χ is a multiplicative character $\pmod p$, I an interval and $A \subset \mathbb{F}_p$ arbitrary. This result was important to the recent work [16] on the distribution of quadratic and higher order residues $\pmod p$. See also [25].

Further improvement on Karacuba's result was obtained by X. Shao [37].

Theorem 19. [39] *Let $q \in \mathbb{Z}_+$ be cube-free and $\chi \bmod q$ be non-principal. If $A \subset [1, q]$ is a union of disjoint intervals $I_1, \dots, I_s$ with $|A| > q^{1/4+\varepsilon} s^{1/2}$ and $|I_j| > q^{\varepsilon}$, $(1 \le j \le s)$ for any $\varepsilon > 0$, then $\sum_{n\in A} \chi(n)$ has a non-trivial bound.*

One could expect that for 'most p' better results are obtainable. However, the following problem seems still open.

Problem 8. *Show that for most p, the largest gap between quadratic residues is $o(p^{1/4})$.*

The following interesting character sum questions were highlighted in Karacuba's survey [29].

Problem 9. *Obtain a non-trivial bound on general sums*

$$\sum_{x\in A,\, y\in B} \chi(x+y),$$

when $|A| \sim \sqrt{p} \sim |B|$.

It is well-known that this question is related to the Paley graph conjecture and also relevant to the theory of 'extractor' in computer science [1].

Problem 10. *Prove that for p large and $a \neq 0 \pmod p$*

$$\sum_{1 \le x < H} \left(\frac{x+a}{p}\right) \Lambda(x) = o(H),$$

when $H \sim \sqrt{p}$.

Results of this type were obtained by Vinogadov, for large values of H.

Problem 11. *Prove that for large p*

$$\min \left\{ 1 \le x \le p : \left(\frac{a+x^2}{p}\right) = -1 \right\} = o(\sqrt{p})$$

uniformly in $1 \le a \le p$.

In [9], the bound $p^{\frac{1}{2\sqrt{e}}+\varepsilon}$ was obtained, but for $a \neq 0$ given.

Acknowledgements Research by Mei-Chu Chang was supported in part by NSF grant DMS 1301608.

References

1. B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, A. Wigderson, Simulating independence: new constructions of condensers, Ramsey graphs, dispersers, and extractors. J. ACM **57**, 52 (2010). Preliminary version in STOC 2005
2. J. Bourgain, On exponential sums in finite Fields, in *An Irregular Mind*, ed. by I. Bárány, J. Solymosi. Bolyai Society Mathematical Studies, Budapest, vol. 21 (Springer, Berlin, 2010)
3. J. Bourgain, Prescribing the binary digits of primes. Isr. J. Math. **194**, 935–955 (2013)
4. J. Bourgain, M.-C. Chang, On a multilinear character sum of Burgess. C. R. Math. Acad. Sci. **348**(3–4), 115–120 (2010)
5. D.A. Burgess, On character sums and primitive roots. Proc. Lond. Math. Soc. (3) **12**, 179–192 (1962)
6. D.A. Burgess, Character sums and primitive roots in finite fields. Proc. Lond. Math. Soc. (3) **37**, 11–35 (1967)
7. M.-C. Chang, On a question of Davenport and Lewis and new character sum bounds in finite fields. Duke Math. J. **145**(3), 409–442 (2008)
8. M.-C. Chang, Character sums in finite fields. AMS Contemp. Math. **518**, 83–98 (2009)
9. M.-C. Chang, On character sums of binary quadratic forms. J. Number Theory **129**(9), 2064–2071 (2009)
10. M.-C. Chang, An estimate of incomplete mixed character sums, in *An Irregular Mind*, ed. by I. Bárány, J. Solymosi. Bolyai Society Mathematical Studies, Budapest, vol. 21 (Springer, Berlin, 2010), pp. 243–250
11. M.-C. Chang, Short character sums for composite moduli. J. d'Anal. Math. **123**, 1–33 (2014)

12. H. Davenport, D. Lewis, Character sums and primitive roots in finite fields. Rend. Circ. Matem. Palermo-Serie II-Tomo XII-Anno **12**, 129–136 (1963)
13. G. Forni, L. Flaminio, On effective equidistribution for higher step nilflows arXiv:1407.3640
14. V.R. Friedlander, On the least n-th power non-residue. Dokl. Akad. Nauk. SSSR **66**, 351–352 (1949)
15. P.X. Gallagher, Primes in progressions to prime-power modulus. Invent. Math. **16**, 191–201 (1972)
16. M.Z. Garaev, S.V. Konyagin, Y. Malykhin, Asymptotics for the sum of powers of distances between power residues modulo a prime. Proc. Steklov Inst. Math. **276**(1), 77–89 (2012)
17. L. Goldmakher, Character sums to smooth moduli are small. Can. J. Math. **62**, 1099 (2010)
18. S.W. Graham, C.J. Ringrose, Lower bounds for least quadratic nonresidues, in *Analytic Number Theory* (Allerton Park, IL, 1989). Progress in Mathematics, vol. 85 (Birkhauser, Boston, 1990), pp. 269–309
19. A. Granville, K. Soundararajan, Large character sums: pretentious characters and the *Pólya*-Vinogradov theorem. J. Am. Math. Soc. **20**, 357–384 (2007)
20. B. Green, T. Tao, The distribution of polynomials over finite fields, with applications to the Gowers norms. Contrib. Discret. Math.**4**(2), 1–36 (2009)
21. F. Green, A. Roy, H. Straubing, Bounds on an exponential sum arising in Boolean circuit complexity. C. R. Math. Acad. Sci. **341**(5), 279–282 (2005)
22. G. Harman, I. Katai, Primes with preassigned digits II. Acta. Arith. **133**(2), 171–184 (2008)
23. D.R. Heath-Brown, Siegel zeros and the least prime in an arithmetic progression. Q. J. Math. Oxf. Ser. (2) **41**, 405–418 (1990)
24. D.R. Heath-Brown, Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. Proc. Lond. Math. Soc. (3) **64**(2), 265–338 (1992)
25. D.R. Heath-Brown, Burgess's bounds for character sums. arXiv:1203.5219
26. H. Iwaniec, On zeros of Dirichlet's L series. Invent. Math. **23**, 97–104 (1974)
27. H. Iwaniec, E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, 2004)
28. A.A. Karacuba, A certain arithmetic sum. Sov. Math. Dokl. **12**(4), 1172–1174 (1971)
29. A.A. Karatsuba, Arithmetic problems in the theory of Dirichlet characters. (Russian, English) Russ. Math. Surv. **63**(4), 641–690 (2008); translation from Usp. Mat. Nauk **63**(4), 43–92 (2008)
30. S.V. Konyagin, Estimates of character sums in finite fields. Mat. Z. **88**(4), 529–542 (2010)
31. Y.V. Linnik, On the least prime in an arithmetic progression I. The basic theorem. Rec. Math. (Mat. Sbornik) N.S. **15**(57), 139–178 (1944)
32. Y.V. Linnik, On the least prime in an arithmetic progression II. The Deuring-Heilbronn phenomenon. Rec. Math. (Mat. Sbornik) N.S. **15**(57), 347–368 (1944)
33. H.L. Montgomery, *Topics in Multiplicative Number Theory*. Lecture Notes in Mathematics, vol. 227 (Springer, New York, 1971)
34. A.G. Postnikov, On Dirichlet L-series with the character modulus equal to the power of a prime number. J. Indian Math. Soc. (N.S.) **20**, 217–226 (1956)
35. H. Salié, Uber den kleinsten positiven quadratischen Nichtrest nach einer Primzahl. Math. Nachr. **3**, 7–8 (1949)
36. W. Schmidt, Bounds for exponential sums. *Acta Arith*. **44**(3), 281–297 (1984)
37. X. Shao, Character sums over unions of intervals, *Forum Math*. **27**(5), 3017–3026 (2015)
38. V. Shoup, Searching for primitive roots in finite fields. Math. Comput. **58**, 369–380 (1992)
39. W. Sierpinski, Sur un probléme concernment les nombres $k \cdot 2n + 1$. Elem. Math. **15**, 63–74 (1960)
40. T. Xylouris, On Linnik's constant (2009). arXiv:0906.2749