ACTA ARITHMETICA
114.2 (2004)

On the difference of the consecutive primitive roots

by

Yonghui Wang (Beijing) and Claus Bauer (San Francisco, CA)

1. Introduction. Let q be an odd prime number and consider the set of consecutive primitive roots mod q with representatives $1 < g_1 < \cdots < g_{\phi(q-1)} < q$. In 1962, Burgess [B1, Theorem 3] gave an asymptotic formula for the number of primitive roots in every interval of length greater than $q^{1/4+\varepsilon}$. In 1998, C. Cobeli and A. Zaharescu [CZ] proved that this sequence has a Poisson distribution if q is very large. In this paper, we study the average value of the differences of $g_{i+1} - g_i$. We define

$$V_\gamma(q) := \sum_{1 \le i < \phi(q-1)} (g_{i+1} - g_i)^\gamma. \tag{1}$$

To the best knowledge of the authors, $V_\gamma(q)$ has not been studied hitherto for any value of $\gamma > 0$, not even in case $\gamma = 2$. In this paper, we estimate $V_\gamma(q)$ unconditionally and assuming GRH.

In the unconditional case, we obtain an estimate for γ in the range $0 < \gamma < 4$. We first apply the estimate of character sums due to Burgess [B1], to prove an estimate for $0 < \gamma < 3$. We call this "Method I". Then we apply a new method to estimate character sums that was developed by Friedlander and Iwaniec [FI]. Using this method, which we call "Method II", we can estimate $V_\gamma(q)$ for the larger range $0 < \gamma < 4$. In this respect, we can regard this paper as an application of the new method by Friedlander and Iwaniec [FI] which is superior to Burgess's in this case. Assuming GRH, we modify our Method I to prove the estimate for $V_\gamma(q)$ for all $\gamma > 0$.

In particular, we prove the following two theorems:

2000 *Mathematics Subject Classification*: Primary 11L40.

Key words and phrases: consecutive primitive roots, character sums.

The first author's work was supported partly by KeGanJu Youth Foundation of Beijing and by Chinese Natural Science Foundation Tianyuan Youth Foundation, and was done while the first author was a visiting scholar at the Mathematical Institute of the Academic China and Morningside center.

THEOREM 1.1. *For any fixed real number $0 < \gamma < 4$, we have*

$$V_\gamma(q) := \sum_{1 \le i < \phi(q-1)} (g_{i+1} - g_i)^\gamma \ll_\gamma \phi(q-1)P^{-\gamma}$$

where $P = \phi(q-1)/(q-1)$, and $f \ll_\gamma g$ is the usual Vinogradov symbol denoting the relationship $|f| \le cg$ for some constant c depending on γ.

We will use all these notations in the rest of this paper.

COROLLARY 1.2. *Assuming the Grand Riemann Hypothesis (GRH), for any fixed real number $\gamma > 0$,*

$$V_\gamma(q) := \sum_{1 \le i < \phi(q-1)} (g_{i+1} - g_i)^\gamma \ll_\gamma \phi(q-1)P^{-\gamma}.$$

2. Lemmas for Method I. In this section, we establish the estimates needed for Method I. We make use of an idea of Montgomery and Vaughan in [MV], which is related to a discrete version of the Selberg integral. Further, we apply estimates for character sums shown by Burgess.

First, we introduce the following characteristic function:

$$\delta(n) = \begin{cases} 1 & \text{if } n \text{ is a primitive root mod } q, \\ 0 & \text{otherwise.} \end{cases}$$

It is well known, and proved in detail in C. Cobeli and A. Zaharescu [CZ], that

$$\delta(n) = \sum_{k \mid q-1} \frac{\mu(k)}{k} \sum_{\chi^k = \chi_0} \chi(n), \tag{2}$$

where χ are Dirichlet characters mod q, and χ_0 is the principal character. Without further mention, we will use the fact that if $k \mid q-1$, then there are exactly k characters mod q with $\chi^k = \chi_0$.

We define

$$M_s(q;h) := \sum_{n=1}^{q} \Big(\sum_{m=1}^{h} \delta(n+m) - hP \Big)^s.$$

This is the sth moment of the number of primitive roots modulo q in an interval of length h about its mean hP. It can be considered as the discrete form of the Selberg integral which was first introduced in [MV]. For further use, we state two lemmas:

LEMMA 2.1 ([M, p. 118, (13.2)]). *Assuming GRH, if χ is a non-principal character modulo q, then*

$$S_h(n) := \Big| \sum_{m=1}^{h} \chi(n+m) \Big| \ll_\varepsilon h^{1/2} q^\varepsilon \ll_r h^{1/2+1/r}$$

if $h > q^{1/2r^2}$ by taking $\varepsilon = 1/2r^3$ for a sufficiently large positive integer r.

LEMMA 2.2 (Burgess [B2]). *If q is a prime, χ is a non-principal character modulo q, and h and r are arbitrary positive integers, then*

$$S_h(n) \ll h^{1-1/r} q^{1/4r+1/4r^2} \log q,$$

where the implied constant is independent of all variables. Furthermore, for any sufficiently small $\varepsilon > 0$, there exists a $\delta = \delta(\varepsilon)$ such that if χ is a non-principal character modulo q, and h is an integer satisfying $h \geq q^{1/4+\varepsilon}$, then

$$S_h(n) \ll h^{1-\delta(\varepsilon)}.$$

We will use these two lemmas to establish the following estimates:

LEMMA 2.3. *For any fixed positive integer s, and for any positive integer h that satisfies $h \geq q^{1/4+\varepsilon}$,*

$$M_s(q;h) \ll_{s,\varepsilon} qP^s h^{s(1-\delta/2)},$$

where $\delta = \delta(\varepsilon)$ is independent of s, and ε is sufficiently small.

LEMMA 2.4. *Assuming GRH, for any fixed positive integer s and any sufficiently large integer $r > 0$, for any positive integer $h > q^{1/2r^2}$, we have*

$$M_s(q;h) \ll_{s,r} qP^s h^{(1/2+2/r)s},$$

where s and r are independent of each other.

Proof of Lemma 2.3. Applying (2), we see

$$\begin{aligned}
(3)\quad & M_s(q;h) \\
&= \sum_{n=1}^{q} \Bigg(\sum_{m=1}^{h} \sum_{k|q-1} \frac{\mu(k)}{k} \sum_{\chi^k=\chi_0} \chi(m+n) - hP \Bigg)^s \\
&= \sum_{n=1}^{q} \Bigg(\sum_{\chi \,(\mathrm{mod}\, q)} \sum_{m=1}^{h} \chi(m+n) \sum_{k|q-1,\, \mathrm{ord}\,(\chi)|k} \frac{\mu(k)}{k} - hP \Bigg)^s \\
&= \sum_{n=1}^{q} \Bigg(P \sum_{\chi \neq \chi_0 \,(\mathrm{mod}\, q)} \frac{\mu(\mathrm{ord}(\chi))}{\phi(\mathrm{ord}(\chi))} \sum_{m=1}^{h} \chi(m+n) + P \sum_{m=1}^{h} \chi_0(m+n) - hP \Bigg)^s,
\end{aligned}$$

where $\mathrm{ord}(\chi)$ denotes the order of χ, i.e. $\mathrm{ord}(\chi) = \min\{k > 0 \mid \chi^k = \chi_0\}$ and the last equality in (3) holds due to the following relation: For any integer t that divides $q-1$, we have

$$\begin{aligned}
\sum_{k|q-1,\, t|k} \frac{\mu(k)}{k} &= \sum_{tk'|q-1} \frac{\mu(tk')}{tk'} = \frac{\mu(t)}{t} \sum_{\substack{k|\frac{q-1}{t} \\ (k,t)=1}} \frac{\mu(k)}{k} = \frac{\mu(t)}{t} \prod_{\substack{p|\frac{q-1}{t} \\ (p,t)=1}} \left(1 - \frac{1}{p}\right) \\
&= \frac{\mu(t)}{t} \prod_{p|q-1} \left(1 - \frac{1}{p}\right) \Big/ \prod_{p|t} \left(1 - \frac{1}{p}\right) = \frac{\mu(t)}{\phi(t)} P.
\end{aligned}$$

Since q is an odd prime number, for any $h \le q$ we obtain

$$\Big|\sum_{m=1}^{h}\chi_0(m+n)-h\Big| = \#\{1\le m\le h \mid (m+n,q)\ne 1\}\le 1.$$

Therefore,

$$\begin{aligned}
M_s(q;h) &= \sum_{n=1}^{q}\bigg(P\sum_{\chi\ne\chi_0 \,(\mathrm{mod}\, q)}\frac{\mu(\mathrm{ord}(\chi))}{\phi(\mathrm{ord}(\chi))}\sum_{m=1}^{h}\chi(m+n)+O(P)\bigg)^s\\
&= P^s\sum_{n=1}^{q}\bigg(\sum_{\chi\ne\chi_0 \,(\mathrm{mod}\, q)}\frac{\mu(\mathrm{ord}(\chi))}{\phi(\mathrm{ord}(\chi))}\sum_{m=1}^{h}\chi(m+n)\bigg)^s\\
&\quad + O\bigg(P^s\sum_{n=1}^{q}\bigg(\sum_{\chi\ne\chi_0 \,(\mathrm{mod}\, q)}\frac{\mu(\mathrm{ord}(\chi))}{\phi(\mathrm{ord}(\chi))}\sum_{m=1}^{h}\chi(m+n)\bigg)^{s-1}+\cdots+1\bigg)\\
&=: I_s + O(I_{s-1}+\cdots+1), \qquad \text{say.}
\end{aligned}$$

Thus, it suffices to estimate I_s. As we assume $h \ge q^{1/4+\varepsilon}$, we can apply Lemma 2.2 as follows:

$$\begin{aligned}
(4)\qquad |I_s| &= P^s\bigg|\sum_{n=1}^{q}\sum_{\chi_1\ne\chi_0 \,(\mathrm{mod}\, q)}\cdots\sum_{\chi_s\ne\chi_0 \,(\mathrm{mod}\, q)}\frac{\mu(\mathrm{ord}(\chi_1))}{\phi(\mathrm{ord}(\chi_1))}\cdots\frac{\mu(\mathrm{ord}(\chi_s))}{\phi(\mathrm{ord}(\chi_s))}\\
&\qquad\times\Big(\sum_{m=1}^{h}\chi_1(m+n)\Big)\cdots\Big(\sum_{m=1}^{h}\chi_s(m+n)\Big)\bigg|\\
&\le P^s\sum_{n=1}^{q}\sum_{t_1|q-1,\,t_1>1}\cdots\sum_{t_s|q-1,\,t_s>1}\frac{|\mu(t_1)|\cdots|\mu(t_s)|}{\phi(t_1)\cdots\phi(t_s)}\\
&\qquad\times\sum_{\chi_1^{t_1}=\chi_0}\cdots\sum_{\chi_s^{t_s}=\chi_0}\Big|\Big(\sum_{m=1}^{h}\chi_1(m+n)\Big)\cdots\Big(\sum_{m=1}^{h}\chi_s(m+n)\Big)\Big|\\
&\ll P^s\sum_{n=1}^{q}\sum_{t_1|q-1}\cdots\sum_{t_s|q-1}\frac{|\mu(t_1)|\cdots|\mu(t_s)|}{\phi(t_1)\cdots\phi(t_s)}\sum_{\chi_1^{t_1}=\chi_0}\cdots\sum_{\chi_s^{t_s}=\chi_0}h^{s(1-\delta)}\\
&\ll qP^sh^{s(1-\delta)}\sum_{t_1|q-1}\cdots\sum_{t_s|q-1}\frac{|\mu(t_1)|t_1\cdots|\mu(t_s)|t_s}{\phi(t_1)\cdots\phi(t_s)}\\
&\ll qP^sh^{s(1-\delta)}\bigg(\sum_{t|q-1}\frac{|\mu(t)|t}{\phi(t)}\bigg)^s \le qP^sh^{s(1-\delta)}\tau(q-1)^{2s}\\
&\ll_\varepsilon qP^sh^{s(1-\delta/2)}.
\end{aligned}$$

Here, $\delta=\delta(\varepsilon)$ is independent of s, and $\tau(n)=\sum_{d|n}1$ is the divisor function.

The third to last inequality is valid because of

$$\sum_{t|q-1} \frac{|\mu(t)|t}{\phi(t)} = \prod_{p|q-1} \left(1 + \frac{p}{p-1}\right) \ll \tau(q-1)^2.$$

The last inequality of (4) holds since $h \geq q^{1/4+\varepsilon}$ and $\tau(n) \ll_\delta n^{\delta/16}$ for any given $\delta > 0$.

Lemma 2.4 is proved in the same way by applying Lemma 2.1 instead of Lemma 2.2. We will also need an estimate which will be used for ranges of h smaller than those assumed in Lemmas 2.3 and 2.4. In order to establish this estimate, we will make use of the following lemma:

LEMMA 2.5 ([J, Lemma 1]). *Let $\chi_1, \ldots, \chi_t$ be Dirichlet characters modulo an odd prime q with some $\chi_i \neq \chi_0$. Let further $m_1, \ldots, m_t$ be distinct integers modulo q. Then*

$$\Big| \sum_{n=1}^{q} \chi_1(m_1+n) \cdots \chi_t(m_t+n) \Big| \leq (t - t_0 - 1)q^{1/2} + t_0 + 1,$$

where t_0 is the number of characters χ_i such that $\chi_i = \chi_0$.

Proof. This is a special case of J. Johnsen's [J, Lemma 1].

We now prove the following estimate:

LEMMA 2.6. *For any integer h that satisfies $P^{-1} < h < q$, we have*

$$M_s(q;h) \ll_{s,\varepsilon} q^{1/2+\varepsilon}(hP)^s + q(hP)^{s/2}$$

for any positive integer $s \geq 2$.

Proof. By definition,

$$\begin{aligned} M_s(q;h) &= \sum_{n=1}^{q} \Big(\sum_{m=1}^{h} \delta(n+m) - hP \Big)^s \\ &= \sum_{f=0}^{s} \binom{s}{f} (-hP)^{s-f} \sum_{n=1}^{q} \Big(\sum_{m=1}^{h} \delta(n+m) \Big)^f. \end{aligned} \tag{5}$$

For $f > 0$, the inner sum over n can be written as

$$\sum_{m_1=1}^{h} \cdots \sum_{m_f=1}^{h} \sum_{n=1}^{q} \delta(n+m_1) \cdots \delta(n+m_f). \tag{6}$$

It is easily seen that for the estimation of the inner sum over n we only need to consider the values of the δ-function on distinct elements of $m_1, \ldots, m_f$.

Let $\mathcal{B} = \{m_1, \dots, m_f\}$, and denote by $t = \operatorname{card}(\mathcal{B})$ the number of different elements of $\mathcal{B}$. We can assume that $m_1, \dots, m_t$ are distinct. Thus,

$$
\begin{aligned}
(7)\quad & \sum_{n=1}^{q} \delta(n+m_1)\cdots\delta(n+m_f) \\
&= \sum_{n=1}^{q} \delta(n+m_1)\cdots\delta(n+m_t) \\
&= \sum_{n=1}^{q} \Bigg(\sum_{k_1 \mid q-1} \frac{\mu(k_1)}{k_1} \sum_{\chi_1^{k_1}=\chi_0} \chi_1(n+m_1) \Bigg) \\
&\quad \times \cdots \times \Bigg(\sum_{k_t \mid q-1} \frac{\mu(k_t)}{k_t} \sum_{\chi_t^{k_t}=\chi_0} \chi_t(n+m_t) \Bigg) \\
&= \sum_{k_1 \mid q-1} \cdots \sum_{k_t \mid q-1} \frac{\mu(k_1)\cdots\mu(k_t)}{k_1\cdots k_t} \sum_{n=1}^{q} \chi_0(n+m_1)\cdots\chi_0(n+m_t) \\
&\quad + \sum_{k_1 \mid q-1} \cdots \sum_{k_t \mid q-1} \frac{\mu(k_1)\cdots\mu(k_t)}{k_1\cdots k_t} \sum_{\chi_1,\dots,\chi_t}{}' \sum_{n=1}^{q} \chi_1(n+m_1)\cdots\chi_t(n+m_t),
\end{aligned}
$$

where $\sum'_{\chi_1,\dots,\chi_t}$ denotes the summation over $\chi_1^{k_1} = \chi_0, \dots, \chi_t^{k_t} = \chi_0$ with some $\chi_i \neq \chi_0$. We note that $m_1, \dots, m_t$ are distinct modulo q, which implies

$$
\sum_{n=1}^{q} \chi_0(n+m_1)\cdots\chi_0(n+m_t) = q - t.
$$

Applying Lemma 2.5 and using an argument similar to the proof of Lemma 2.3, we can write the last expression in (7) as follows:

$$
\begin{aligned}
(8)\quad & (q-t)\Bigg(\sum_{k \mid q-1} \frac{\mu(k)}{k} \Bigg)^t + O\Big(tq^{1/2} \Big(\sum_{k \mid q-1} |\mu(k)| \Big)^t \Big) \\
&\qquad = (q-t)P^t + O_\varepsilon(tq^{1/2+\varepsilon}) = qP^t + O_\varepsilon(tq^{1/2+\varepsilon}P^t).
\end{aligned}
$$

We can add the additional term P^t to the O-term since $P^{-1} < \tau(q-1) \ll q^\varepsilon$.

In order to estimate (6), we denote by $S(f,t)$ the Stirling number of the second kind, i.e. the number of ways of partitioning a set of cardinality f into exactly t non-empty subsets. Consequently, $S(f,t)t!$ is the number of surjective maps from a set of cardinality f onto a set of cardinality t. Using (8), we can now write the expression in (6) as follows:

$$(9)\qquad \sum_{m_1=1}^{h}\cdots\sum_{m_f=1}^{h}\sum_{n=1}^{q}\delta(n+m_1)\cdots\delta(n+m_f)$$

$$= \sum_{t=1}^{\min(f,h)} \sum_{\substack{\mathcal{B}\subseteq\{1,\dots,h\}\\ \mathcal{B}=\{m_1,\dots,m_t \mid m_i\neq m_j \text{ if } i\neq j\}}} S(f,t)t!\Big\{\sum_{n=1}^{q}\delta(n+m_1)\cdots\delta(n+m_t)\Big\}$$

$$= \sum_{t=1}^{\min(f,h)} \sum_{\mathcal{B}\subseteq\{1,\dots,h\},\,\mathrm{card}(\mathcal{B})=t} S(f,t)t!(qP^t+O_\varepsilon(tq^{1/2+\varepsilon}P^t))$$

$$= \sum_{t=1}^{\min(f,h)} \binom{h}{t} S(f,t)t!(qP^t+O_\varepsilon(tq^{1/2+\varepsilon}P^t))$$

$$= \sum_{t=0}^{f} \binom{h}{t} S(f,t)t!(qP^t+O_\varepsilon(tq^{1/2+\varepsilon}P^t)),$$

where we assumed that $f\le h$. An analysis of the final part of the proof will show that the case $f>h$ can be treated in the same way. In the following, we set $\binom{h}{t}=0$ for $t>h$ and $S(f,0)=0$ for $f>0$, $S(0,t)=0$ for $t>0$, and $S(0,0)=1$. Thus, from (5) and (9) we obtain

$$M_s(q;h)=q\sum_{f=0}^{s}\binom{s}{f}(-hP)^{s-f}\sum_{t=0}^{f}\binom{h}{t}S(f,t)t!P^t+O_{s,\varepsilon}(q^{1/2+\varepsilon}(hP)^s).$$

We obtain the error term from the estimates $S(f,t)t!t\ll_s 1$ for $t\le f\le s$ and $\sum_{t=0}^{f}\binom{h}{t}P^t\ll(hP)^f+(hP)\ll(hP)^f$ by $P^{-1}<h$. By using combinatorial recursions, the main term on the right hand side was estimated in [MV, Lemma 11] as follows:

$$\begin{aligned}\mu_s(h,P) &:= \sum_{f=0}^{s}\binom{s}{f}(-hP)^{s-f}\sum_{t=0}^{f}\binom{h}{t}S(f,t)t!P^t\\ &\ll (hP)^{[s/2]}+hP\ll(hP)^{s/2},\end{aligned}$$

for any integer $s\ge 2$. This proves the lemma.

Montgomery and Vaughan ([MV, p. 326, Lemma 9]) have given a probabilistic interpretation of $\mu_s(h,P)$. Let X be a binomial random variable with parameters h and P; then $\mu_s(h,P)$ equals the expectation value of the sth moment of the difference between X and its expected value hP, i.e.,

$$\mu_s(h,P)=E((X-hP)^s)=\sum_{k=0}^{h}\binom{h}{k}P^k(1-P)^{h-k}(k-hP)^s.$$

This interpretation can help us to understand the theorem.

3. Lemmas for Method II. In the previous section, we established Lemmas 2.3 and 2.6 which will allow us to estimate the expression (1) for all $\gamma > 0$ under GRH and in the case of $0 < \gamma < 3$ unconditionally. In order to extend the range to $0 < \gamma < 4$ we will investigate values of h in the "middle" range $q^{1/2r} < h < q^{1/4+\varepsilon}$. We use a new method for the estimation of character sums introduced by Iwaniec and Friedlander [FI]. We first show the following lemma:

LEMMA 3.1. *Let $\mathcal{D}$ be a $(2A+1)$-spaced set modulo q, i.e. $|d_1 - d_2| \geq 2A+1$ for all $d_1, d_2 \in \mathcal{D}$, and assume $|\mathcal{D}|(2A+1) < q$, $B < A$. Define*

$$\nu(u) := \sharp\{(a,b,d) \mid M - A \leq a \leq M + A, 1 \leq b \leq B, \\ d \in \mathcal{D}, a - d \equiv bu \pmod q\}.$$

Then

$$\sum_{u=1}^{q} \nu^2(u) \ll |\mathcal{D}|AB \log q.$$

Proof. We use the usual notation $e(x) = \exp(2\pi i x)$. Defining $\overline{b}$ via $b\overline{b} \equiv 1 \pmod q$, we see that

$$\begin{aligned}
\sum_{u=1}^{q} \nu^2(u) &= \sum_{u=1}^{q} \left| \frac{1}{q} \sum_{d \in \mathcal{D}} \sum_{M-A \leq a \leq M+A} \sum_{1 \leq b \leq B} \sum_{n=1}^{q} e\left(\frac{((a-d)\overline{b} - u)n}{q}\right) \right|^2 \\
&= \frac{1}{q^2} \sum_{a_1,a_2} \sum_{b_1,b_2} \sum_{d_1,d_2} \sum_{n_1,n_2} e\left(\frac{(a_1-d_1)\overline{b}_1 n_1 - (a_2-d_2)\overline{b}_2 n_2}{q}\right) \\
&\quad \times \sum_{u=1}^{q} e\left(\frac{u(n_1-n_2)}{q}\right) \\
&= \frac{1}{q} \sum_{a_1,a_2} \sum_{b_1,b_2} \sum_{d_1,d_2} \sum_{n} e\left(\frac{((a_1-d_1)\overline{b}_1 - (a_2-d_2)\overline{b}_2)n}{q}\right) \\
&= \sharp \left\{ (a_1,a_2,b_1,b_2,d_1,d_2) \;\middle|\; \begin{array}{c} M-A \leq a_1, a_2 \leq M+A, \\ 1 \leq b_1, b_2 \leq B,\ d_1, d_2 \in \mathcal{D}, \\ (a_1-d_1)b_2 \equiv (a_2-d_2)b_1 \pmod q \end{array} \right\} \\
&=: |S|, \qquad \text{say.}
\end{aligned}$$

Due to symmetry, we only need to estimate the subset S' of S that satisfies $b_1 \leq b_2$. Let $\mathcal{R} = \{r = a - d \mid M - A \leq a \leq M + A,\ d \in \mathcal{D}\}$. As $\mathcal{D}$ is a $(2A+1)$-spaced set modulo q and $|\mathcal{D}|(2A+1) < q$, we find that $\mathcal{R}$ is the union of $|\mathcal{D}|$ disjoint segments of length $2A+1$ in $[1,q]$. Defining $r_i = a_i - d_i \in \mathcal{R}$, $i \in \{1,2\}$, we see that S' can be considered as the product of the set $\mathcal{R}$ and the set $\{(b_1,b_2) \mid 1 \leq b_1, b_2 \leq B, b_1 \leq b_2\}$ with the

constraint $r_1 b_2 \equiv r_2 b_1 \pmod q$. We note that the value of the variable r_1 is uniquely determined if the variables of r_2, b_1, b_2 are given, since $|\mathcal{R}| < q$. Furthermore, $r_2 b_1 - r_1 b_2 = k_0 q$, hence for given b_1, b_2 we have $r_2 b_1 \equiv k_0 q \pmod{b_2}$. Thus,

$$\begin{aligned}
|S'| &\le \sum_{1\le b_2\le B}\sum_{1\le b_1\le b_2}\sum_{r_2\in\mathcal{R},\, r_2\equiv l \,(\mathrm{mod}\, b_2/(b_1,b_2))} 1\\
&\le \sum_{1\le b_2\le B}\sum_{1\le b_1\le b_2}\left(|\mathcal{D}|\left(\frac{2A+1}{b_2/(b_1,b_2)}+1\right)\right)\\
&\ll |\mathcal{D}|A\sum_{b_2\le B}\frac{1}{b_2}\sum_{b_1\le b_2}(b_1,b_2)+O(|\mathcal{D}|B^2)\\
&\ll |\mathcal{D}|A\sum_{b_2\le B}\frac{1}{b_2}\sum_{d\mid b_2}d\sum_{b_1\le b_2,\, b_1\equiv 0 \,(\mathrm{mod}\, d)} 1+O(|\mathcal{D}|B^2)\\
&\ll |\mathcal{D}|A\sum_{b_2\le B}\tau(b_2)+O(|\mathcal{D}|B^2)\ll |\mathcal{D}|AB\log q.
\end{aligned}$$

We also require a lemma of Burgess [B1, Lemma 2] which is based on A. Weil's work.

LEMMA 3.2. *We have*

$$\sum_{x=1}^{q}\Big|\sum_{m=1}^{h} e(my)\chi(m+x)\Big|^{2r} \ll_r qh^r + q^{1/2}h^{2r}. \tag{10}$$

Our version of the lemma differs from the original [B1, Lemma 2] *by the additional factor $e(my)$. We show that the original proof still applies.*

Proof. We see that

$$\begin{aligned}
&\sum_{x=1}^{q}\Big|\sum_{m=1}^{h} e(my)\chi(m+x)\Big|^{2r}\\
&= \sum_{x=1}^{q}\sum_{m_1=1}^{h}\cdots\sum_{m_{2r}=1}^{h} e(m_1y)\cdots e(m_ry)e(-m_{r+1}y)\cdots e(-m_{2r}y)\\
&\quad\times\chi((m_1+x)\cdots(m_r+x))\overline{\chi}((m_{r+1}+x)\cdots(m_{2r}+x))\\
&\le \sum_{m_1=1}^{h}\cdots\sum_{m_{2r}=1}^{h}\Big|\sum_{x=1}^{q}\chi((m_1+x)\cdots(m_r+x))\overline{\chi}((m_{r+1}+x)\cdots(m_{2r}+x))\Big|.
\end{aligned}$$

The last expression was estimated in [B1, Lemma 2, formulas (8), (9)] to obtain the result without the additional factor $e(my)$. We now state a lemma that will be crucial for Method II.

LEMMA 3.3. *Let $\mathcal{D}$ be a $(2A+1)$-spaced set modulo q and $|\mathcal{D}|(2A+1) < q$. For any given positive integer r, if $A > q^{1/2r}$, then*

$$|S_\chi| := \Big| \sum_{M<a\le M+A} \sum_{d\in\mathcal{D}} \chi(a+d) \Big| \ll |\mathcal{D}|^{1-1/2r} A^{1-1/r} q^{1/4r+1/4r^2} (\log q)^2.$$

REMARK. This lemma is similar to Theorem $2'$ in [FI] with minor changes in the assumptions and results. In what follows, we adapt the original proof to establish Lemma 3.3.

Proof. We define a function $f(x) = \min(x-M, 1, M+A+1-x)$ in the interval $[M, M+A+1]$ and $f(x) = 0$ elsewhere. Denote by g the Fourier transform of f, i.e.,

$$g(y) = \int_{-\infty}^{\infty} f(x) e(-yx)\, dx.$$

Applying partial integration as in [BI], we find $|g(y)| \le \min(A+1, |\pi y|^{-1}, (\pi y)^{-2})$. Hence,

$$\int_{-\infty}^{\infty} |g(y)|\, dy \ll \log A.$$

Setting $BC = A$, we obtain

$$\begin{aligned}
(11)\quad & |S_\chi| \\
&= \Big| A^{-1} \sum_{d\in\mathcal{D}} \sum_{M-A\le a\le M+A} \sum_{1\le b\le B} \sum_{1\le c\le C} f(a+bc)\chi(a+bc+d) \Big| \\
&\le A^{-1} \sum_{d\in\mathcal{D}} \sum_{M-A\le a\le M+A} \sum_{1\le b\le B} \int_{-\infty}^{\infty} \Big| \sum_{1\le c\le C} g(y) e(y(a+bc))\chi(a+d+bc) \Big| dy \\
&\le A^{-1} \sum_d \sum_a \sum_b \int_{-\infty}^{\infty} \frac{1}{b} \Big| g\Big(\frac{y}{b}\Big) \Big| \Big| \sum_{1\le c\le C} e(yc)\chi((a+d)\overline{b}+c) \Big| dy,
\end{aligned}$$

by variable change and noting that $\chi(b) \ne 0$ for $1 \le b \le B$ since q is prime. Using the estimates established for $g(y)$ above, we find that $h(y) := |g(y/b)|/b \le \min(A+1, |y|^{-1}, By^{-2})$ and

$$\int_{-\infty}^{\infty} h(y)\, dy \ll \log q.$$

Using these estimates, we obtain from (11):

$$\begin{aligned}
|S_\chi| &\ll A^{-1} \log q \sum_d \sum_a \sum_b \Big| \sum_{1\le c\le C} e(yc)\chi((a+d)\overline{b}+c) \Big| \\
&= A^{-1} \log q \sum_{u \,(\mathrm{mod}\, q)} \nu(u) \Big| \sum_{1\le c\le C} e(yc)\chi(u+c) \Big|
\end{aligned}$$

for some $y \in \mathbb{R}$, where

$$\nu(u) = \sharp\{(a,b,d) \mid M-A \le a \le M+A,\ 1 \le b \le B,\ d \in \mathcal{D},\ a+d \equiv bu \pmod q\}.$$

Hence by Lemmas 3.1, 3.2 and by Hölder's inequality,

$$\begin{aligned}|S_\chi| &\ll A^{-1}\log q\Big(\sum_{u \,(\mathrm{mod}\, q)} \nu(u)^{2r/(2r-1)}\Big)^{1-1/2r}\\ &\quad\times\Big(\sum_{u \,(\mathrm{mod}\, q)}\Big|\sum_{1\le c\le C} e(yc)\chi(u+c)\Big|^{2r}\Big)^{1/2r}\\ &\ll A^{-1}\log q\Big(\sum_{u \,(\mathrm{mod}\, q)} \nu(u)^2\Big)^{1-1/2r}(qC^r + q^{1/2}C^{2r})^{1/2r}\\ &\ll A^{-1}\log q(|\mathcal{D}|AB\log q)^{1-1/2r}(qC^r + q^{1/2}C^{2r})^{1/2r}.\end{aligned}$$

Choosing $C = q^{1/2r}$ and $B = Aq^{-1/2r} > 1$ completes the proof of the lemma.

4. Proof of the theorems

4.1 *Method I.* Let $L(y) = \sharp\{i \mid 1 \le i \le \phi(q-1),\ g_{i+1} - g_i > y\}$. Then for any fixed $\gamma > 0$, by partial summation,

$$V_\gamma = \gamma \int_0^\infty L(y) y^{\gamma-1}\, dy. \tag{12}$$

We see that in order to prove our theorem, it is sufficient to establish an upper bound for $L(y)$. We will now derive an upper bound for $L(y)$ that depends on $M_s(q;h)$. We set $h = [y/4]$, hence $y \ge 4h$. If $g_{i+1} - g_i > y$, then for $g_i < n < g_i + h$, the interval $[n+1, n+h]$ contains no primitive roots. Therefore,

$$L(y)h(hP)^s \le M_s(q;h). \tag{13}$$

Applying Lemmas 2.3 and 2.6 to (13), we obtain the following upper bounds for $L(y)$: For sufficiently small $\varepsilon > 0$, by Lemma 2.3,

$$L(y) \ll_{s,\varepsilon} \phi(q-1)P^{-1}y^{-\delta_1(\varepsilon)s/2-1} \quad \text{if } y \ge q^{1/4+\varepsilon}, \tag{14a}$$

and by Lemma 2.6, for any integer $s \ge 2$,

$$L(y) \ll_{s,\varepsilon} q^{1/2+\varepsilon}y^{-1} + q(yP)^{-s/2}y^{-1} \quad \text{if } 4P^{-1} < y < q,$$

hence

$$L(y) \ll_\varepsilon \phi(q-1)P^{-1}y^{-3+\delta_2(\varepsilon)} + q(yP)^{-s/2}y^{-1} \quad \text{if } 4P^{-1} < y < q^{1/4+\varepsilon}; \tag{14b}$$

$$L(y) \ll_r \phi(q-1)P^{-1}y^{-2r^2/3-1} + q(yP)^{-s/2}y^{-1} \quad \text{if } 4P^{-1} < y < q^{1/2r^2},\ r \in \mathbb{Z}^+. \tag{14c}$$

The relations (14b) and (14c) hold due to the respective ranges of q and y, and $\delta_2(\varepsilon)$ can be chosen sufficiently small for sufficiently small ε.

For $0 \le y \le 4P^{-1}$ the trivial estimate $L(y) \le \phi(q-1)$ is enough,

$$\gamma \int_0^{4P^{-1}} L(y) y^{\gamma-1}\, dy \ll_\gamma \phi(q-1) P^{-\gamma}. \tag{15}$$

For $y > q^{1/4+\varepsilon}$, we note that $\delta = \delta(\varepsilon)$ is independent of s in (14a). Thus, we may assume that s is taken so large that $\delta s/2 > \gamma$. Then, by (14a)

$$\begin{aligned} \gamma \int_{q^{1/4+\varepsilon}}^{\infty} L(y) y^{\gamma-1}\, dy &\ll_{\gamma,\varepsilon} \phi(q-1) P^{-1} \int_{q^{1/4+\varepsilon}}^{\infty} y^{\gamma-\delta s/2-2}\, dy \\ &\ll_{\gamma,\varepsilon} \phi(q-1) P^{-1} q^{-1/4} \ll_{\gamma,\varepsilon} \phi(q-1) \\ &\ll_{\gamma,\varepsilon} \phi(q-1) P^{-\gamma} \end{aligned} \tag{16}$$

for all $\gamma > 0$.

For $4P^{-1} < y < q^{1/4+\varepsilon}$, we use the estimate (14b). For any fixed γ with $0 < \gamma < 3$, we take a $\delta(\varepsilon)$ such that $0 < \gamma < 3 - \delta(\varepsilon)$. Such a $\delta(\varepsilon)$ can always be found if ε is chosen sufficiently small. We obtain

$$\begin{aligned} &\gamma \int_{4P^{-1}}^{q^{1/4+\varepsilon}} L(y) y^{\gamma-1}\, dy \\ &\qquad \ll_{\gamma,\varepsilon} \phi(q-1) P^{-1} \int_{4P^{-1}}^{q^{1/4+\varepsilon}} \left(y^{-1-(3-\gamma-\delta(\varepsilon))} + (yP)^{-s/2} y^{\gamma-2}\right) dy \\ &\qquad \ll_{\gamma,\varepsilon} \phi(q-1) P^{-\gamma}. \end{aligned} \tag{17}$$

Therefore, Theorem 1.1 follows from (15)–(17) for $0 < \gamma < 3$ by taking an appropriate ε. Corollary 1.2 (GRH case) follows by the same argument when we apply Lemma 2.4 instead of Lemma 2.3 and (14c) instead of (14b). First, under GRH, we deduce from (13) and Lemma 2.4 that

$$L(y) \ll_r q y^{-(1/2-2/r)s-1} \ll_r \phi(q-1) P^{-1} y^{-(1/2-2/r)s-1}$$

for $y \ge q^{1/2r^2}$. Since s is also independent of r in Lemma 2.4, we can take s sufficiently large such that $\gamma - (1/2 - 2/r)s < 0$, to obtain

$$\begin{aligned} \gamma \int_{q^{1/2r^2}}^{\infty} L(y) y^{\gamma-1}\, dy &\ll_{\gamma,r} \phi(q-1) P^{-1} \int_{q^{1/2r^2}}^{\infty} y^{\gamma-(1/2-2/r)s-2}\, dy \\ &\ll_{\gamma,r} \phi(q-1) P^{-\gamma}. \end{aligned} \tag{18}$$

For $y \le q^{1/2r^2}$, by (14c),

$$\gamma \int_{4P^{-1}}^{q^{1/2r^2}} L(y) y^{\gamma-1}\,dy \tag{19}$$
$$\ll_{\gamma,r} \phi(q-1)P^{-1} \int_{4P^{-1}}^{q^{1/2r^2}} (y^{\gamma-2r^2/3-2} + (yP)^{-s/2} y^{\gamma-2})\,dy$$
$$\ll_{\gamma,r} \phi(q-1)P^{-\gamma},$$

if we choose r sufficiently large such that $\gamma < 2r^2/3$. Now, Corollary 1.2 follows from (15), (18) and (19).

4.2. *Method II.* In this section we prove Theorem 1.1 for $0 < \gamma < 4$. We will need the following lemma:

LEMMA 4.1. *Define $\mathcal{N}$ to be a set of N integers $n_i \in [1, q-1]$, $1 \le i \le N$, such that $n_1 < \cdots < n_N$ and the integers are $(2h+1)$-spaced, i.e. $|n_i - n_j| > 2h+1$ for $i \ne j$. If there exists a δ' such that for all $n_i \in \mathcal{N}$, the interval $[n_i, n_i + h]$ contains at most $Ph^{1-\delta'}$ primitive roots, then for any positive integer r, if $q^{1/2r^2} < h < q$, we have*

$$N \ll_r qh^{-4+4/r} \ll_r \phi(q-1)P^{-1}h^{-4+4/r}.$$

When the set $\mathcal{N}$ is modified so that each n_i corresponds to a primitive root g_j and $g_{j+1} - g_j > y$ for $1 \le j \le N-1$, then

$$L(y) = N \ll_r \phi(q-1)P^{-1}y^{-4+4/r} \tag{20}$$

for $q^{1/2r^2} < y < q$.

Proof. Arguing as in the proof of Lemma 2.4 (see (3)), we see that

$$\sum_{n_i \in \mathcal{N}} \sum_{m=1}^{h} \delta(m+n_i)$$
$$= P \sum_{n_i \in \mathcal{N}} \sum_{\chi \ne \chi_0,\, t=\mathrm{ord}(\chi)} \frac{\mu(t)}{\phi(t)} \sum_{m=1}^{h} \chi(m+n_i) + NhP + O(NP).$$

Under the assumption of the lemma, the left hand side is less than $NPh^{1-\delta'}$. Comparing both sides, we must have

$$Nh \ll \sum_{\chi \ne \chi_0,\, t=\mathrm{ord}(\chi)} \frac{1}{\phi(t)} \Big| \sum_{n_i \in \mathcal{N}} \sum_{m=1}^{h} \chi(m+n_i) \Big| \tag{21}$$
$$\ll \tau^2(q) \Big| \sum_{n_i \in \mathcal{N}} \sum_{m=1}^{h} \chi(m+n_i) \Big|$$
$$\ll N^{1-1/2r'} h^{1-1/r'} q^{1/4r'+1/4r'^2} (\log q)^2 \tau^2(q).$$

The last inequality is obtained by applying Lemma 3.3 if $h \geq q^{1/2r'}$. Taking $r' = r^3$, for $h > q^{1/2r^2} > q^{1/2r'}$, we obtain

$$N \leq N^2 \ll_r h^{-4} q^{1+2/r'} \ll_r h^{-4+4/r} q.$$

This proves the lemma.

Now, we prove Theorem 1.1 for all $0 < \gamma < 4$. Using (20) instead of the relation (14b), we can follow the argument in (17) to establish

$$\gamma \int_{q^{1/2r^2}}^{q^{1/4+\varepsilon}} L(y) y^{\gamma-1}\, dy \ll_{\gamma,\varepsilon} \phi(q-1) P^{-\gamma}. \tag{22}$$

The theorem therefore follows from (16), (19) and (22).

References

[BI] E. Bombieri and H. Iwaniec, *On the order of* $\zeta(1/2+it)$, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 13 (1986), 449–472.

[B1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), 179–192.

[B2] —, *On character sums and L-series. II*, ibid. 13 (1963), 524–536.

[CZ] C. Cobeli and A. Zaharescu, *On the distribution of primitive roots mod p*, Acta Arith. 83 (1998), 143–153.

[FI] J. Friedlander and H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc. 119 (1993), 365–372.

[J] J. Johnsen, *On the distribution of powers in finite fields*, J. Reine Angew. Math. 251 (1971), 10–19.

[M] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, 1971.

[MV] H. L. Montgomery and R. C. Vaughan, *On the distribution of reduced residues*, Ann. of Math. (2) 123 (1986), 311–333.

Department of Mathematics
The Capital Normal University
Beijing 100037, P.R. China
E-mail: yhwang@mail.cnu.edu.cn
arith_wsun@sohu.com

Dolby Laboratories
San Francisco, CA, U.S.A.
E-mail: cb@dolby.com

Received on 7.8.2003
and in revised form on 22.2.2004 (4589)