The average of the least primitive root modulo $p^2$

by

D. A. Burgess (Nottingham)

1. In 1968 Dr. Elliott and I [3] obtained the estimate

$$\pi(X)^{-1} \sum_{p \leq X} g(p) \ll (\log X)^4 (\log \log X)^4$$

for the average over all primes $p \leq X$ of the least primitive root $g(p)$ to the modulus $p$. Professor Heilbronn proposed to me the problem of the similar estimation of the least primitive root $h(p)$ to the modulus $p^2$. The argument of [3] remains applicable with slight modifications but yields only the weaker estimate

$$\pi(X)^{-1} \sum_{p \leq X} h(p) \ll (\log X)^4 (\log \log X)^8.$$ 

The argument of [3] was based on the Large Sieve inequality which may be stated as

$$\sum_{n=1}^{N} \sum_{m=1}^{m} \left| \sum_{n=1}^{N} \sigma(n/m) \alpha_n \right|^2 \ll (X^2 + N) \sum_{n=1}^{N} |\alpha_n|^2$$

where as usual $\sigma(n) = \sigma_{\text{mult}}$. In the estimation of $g(p)$ $m$ in (3) ranged over the primes. In the estimation of $h(p)$ however $m$ ranges over the $p^2 \leq X$ (together with the $p \leq X^{1/2}$) and it is this decrease in the size of the set of $m$ that gives rise to the loss in effectiveness seen on comparing (3) with (1). The purpose of this paper is to regain in part this effectiveness by producing a modified form of the Large Sieve which will reflect such restrictions on the set of sieving moduli $m$. The resultant estimation for the average of $h(p)$ is contained in the following theorem:

**Theorem.** For large $X$

$$\pi(X)^{-1} \sum_{p \leq X} h(p) \ll (\log X)^8 (\log \log X)^4$$

the summation being extended over prime numbers $p$. 
2. The Large Sieve.

Lemma 1. Let \( S \) be a set of positive integers. Suppose that
\[
S \subseteq [1, X]
\]
and that the cardinality of \( S \) is \( Q \). Then we have
\[
\left| \sum_{q \leq Q} \sum_{\substack{a \leq X \mod q \leq a' \leq X \mod q \leq a' \leq q, \quad (a', q') = 1,}} \sum_{n=1}^{N} a_n e(an/q) \right|^2 \ll XQ(N + XQ) \sum_{n=1}^{N} |a_n|^2.
\]

Proof. For each pair \( q, a \) in the summation on the left-hand-side of (4) let \( M(q, a) \) denote the number of pairs \( q', a' \) satisfying
\[
q' \leq S, \quad 1 \leq a' \leq q', \quad (a', q') = 1,
\]
\[
\left| \frac{a}{q} - \frac{a'}{q'} \right| \leq \frac{1}{4XQ},
\]
(where \( \|x\| \) denotes the distance of \( x \) from the nearest integer). We write
\[
\sum_{q \leq Q} \sum_{\substack{a \leq X \mod q \leq a' \leq X \mod q \leq a' \leq q, \quad (a', q') = 1,}} \sum_{n=1}^{N} a_n e(an/q) = \Sigma_1 + \Sigma_2
\]
where \( \Sigma_1 \) contains those terms for which \( M(q, a) = 1 \) and \( \Sigma_2 \) those for which \( M(q, a) > 1 \).

The estimation of both \( \Sigma_1 \) and \( \Sigma_2 \) is based on the beautiful inequality due to Davenport and Halberstam [4] that:

If \( x_1, \ldots, x_K \) are real numbers and
\[
\delta = \min_{i \neq k} \|x_i - x_k\|
\]
then
\[
\sum_{i=1}^{K} \left( \sum_{n=1}^{N} a_n e(nx_i) \right)^2 \ll (N + \delta^{-1}) \sum_{n=1}^{N} |a_n|^2.
\]

To estimate \( \Sigma_1 \) from this we put the \( x_i \) equal to those Farey fractions \( a/q \) corresponding to the summation conditions of \( \Sigma_1 \). Thus in this application of (8) we have
\[
R \leq XQ \quad \text{and} \quad \delta \geq \frac{1}{4XQ},
\]
and so
\[
\Sigma_1 \ll R \sum_{n=1}^{N} \left( \sum_{n=1}^{N} a_n e(nx_i) \right)^2 \ll R(N + \delta^{-1}) \sum_{n=1}^{N} |a_n|^2 \ll XQ(N + XQ) \sum_{n=1}^{N} |a_n|^2.
\]

To estimate \( \Sigma_2 \) we assume (without loss of generality) that \( X \) is an integer, and we write
\[
F(x) = \sum_{q \leq Q} \sum_{\substack{a \leq X \mod q \leq a' \leq X \mod q \leq a' \leq q, \quad (a', q') = 1,}} \sum_{n=1}^{N} a_n e(an/q).
\]

Clearly we have
\[
\int_{0}^{1/4XQ} F(x) dx = \frac{1}{4XQ} \Sigma_2.
\]

Thus we can choose \( \sigma \) such that
\[
F(x) \geq \frac{1}{4} \Sigma_2.
\]
We write for this choice of \( x \)
\[
F'(x) = \sum_{a} \sum_{n=1}^{N(\sigma)} \left| \sum_{n=1}^{N} a_n e(an/q) \right|
\]
where \( \Sigma^{(\sigma)} \) denotes a summation restricted to those pairs \( q, a \) which contribute to \( F(x) \). Two pairs \( q, a \) and \( q', a' \) in this summation satisfy (6) if and only if they correspond to the same \( y \mod 1 \). For each \( y \mod 1 \) choose that pair \( q, a \), associated with \( y \), to be included in the summation \( \Sigma^{(\sigma)} \) for which
\[
\left| \sum_{n=1}^{N} a_n e(an/q) \right|
\]
is maximal. Thus
\[
F(x) \ll \sum_{q} \sum_{a} \left| \sum_{n=1}^{N(\sigma)} M(q, a) \right| \sum_{n=1}^{N} |a_n|^2
\]
The summation \( \Sigma^{(\sigma)} \) is thus over a collection of pairs \( q, a \) for which the corresponding Farey fractions are at least \( 1/2XQ \) apart \( \mod 1 \). Hence
\[
F(x)^2 \ll \left( \sum_{q} \sum_{a} \left| \sum_{n=1}^{N(\sigma)} M(q, a)^2 \right| \sum_{n=1}^{N} |a_n|^2 \right)^{\frac{1}{2}} \ll \sum_{q} \sum_{a} \left( \sum_{n=1}^{N} \left| \sum_{n=1}^{N} a_n e(an/q) \right|^2 \right)^{\frac{1}{2}}
\]
by (8).

However we have
\[
\sum_{q} \sum_{a} \sum_{n=1}^{N(\sigma)} M(q, a)^2 \ll \sum_{q} \sum_{a} \sum_{n=1}^{N(\sigma)} M(q, a)
\]
$$\sum^\infty_n$$ is restricted to those pairs that contribute to $\Sigma_n$. For each pair $q, q'$ there are at most $^{(3)}$

$$2 \frac{X}{q} (q, q')$$

pairs $a, a'$ (for which $q, a$ and $q', a'$ both satisfy (5)) for which

$$qa' - q'a = n$$

when $n$ is divisible by $(q, q')$ and none otherwise. Thus there are at most $5X/Q$ such pairs $a, a'$ for which

$$|qa' - q'a| \leq q/Q.$$ 

Only such pairs can satisfy

$$\left| \frac{a}{q} - \frac{a'}{q'} \right| \leq \frac{1}{QX},$$

from which we deduce that $\ll XQ$ such sets $q, q', a, a'$ satisfy (6). But this latter collection is counted by the right-hand side of (12) so that from (10) and (11) we obtain

$$\Sigma^2 \ll XQ(N + XQ) \sum_{n=1}^N |a_n|^2.$$ 

This together with (7) and (9) completes the proof.

For problems concerning primitive roots the Large Sieve is required in a character sum form. A convenient connection between character and exponential sums for our investigation is the following:

**Lemma 2.** Let $S$ be as in Lemma 1. Let $C_z$ be non-negative numbers. Then we have

$$\sum_{q \in S} \sum^* C_z \sum_{n=1}^N a_n \chi(n) \leq \sum_{q \in S} q^{-1/2} \left( \sum^* C_z \sum_{n=1}^N a_n \chi(an/q) \right)$$

where the summation over $\chi$ is over primitive characters mod $q$.

Proof. We use the well-known identity that if $\chi$ is a primitive character mod $q$ then

$$\chi(n) = \frac{1}{\tau(\chi)} \sum_{a \equiv 1}^q \chi(a)e(an/q)$$

where

$$|\tau(\chi)| = q^{1/2}.$$ 

(3) $(a, b)$ denotes the highest common factor of $a$ and $b$.

Thus the left-hand side of (13) is equal to

$$\sum_{q \in S} \sum_{z} C_z q^{-1/2} \left| \sum_{n=1}^N a_n \chi(an/q) \right| \leq \sum_{q \in S} q^{-1/2} \left( \sum_z C_z \sum_{n=1}^N a_n \chi(an/q) \right)$$

as required.

**3. The argument of Burgess and Elliott.** Fundamental to the argument in [3] is the existence of a suitable bound for $g(p)$. Similarly we require a bound for $h(p)$. This can be obtained by substituting any estimates for character sums mod $p^t$ of [2] into the argument of my estimation of $g(p)$ in [1]. The result obtained is that

$$h(p) = O(p^{10/7}).$$

Now the argument contained in the first five lemmas of [3], with the obvious modifications, shows that if

$$S_1 = \{ p \leq X^{1/2} : \pi(p-1)h'(p) < (\log X)^2 \}$$

where $h'(p)$ is the least primitive root mod $p$, then

$$\sum_{p \leq X^{1/2}} h(p) \ll X^{1/2}\log X.$$ 

We require this inequality which cannot be deduced from Lemma 1 since (14) is not sufficiently sharp for this.

**4. Analogue of the argument of Burgess and Elliott.**

**Lemma 3.** Let $S$ be a set of $q$ for which

$$\sum_X C_z < R.$$ 

Then we have

$$\left( \sum_{q \in S} \sum_{z} C_z \sum_{w \in R} \chi(w) \right)^2 \ll R^2 Q(H^2 + XQ)\pi(H)^r!\log X,$$

where (as in [3]) we follow the convention that $w$ is always restricted to be prime.

Proof. Let $S'$ be the subset of $S$ for which

$$Y < q \leq 2Y$$

and let the cardinality of $S'$ be $Q'$. As in Lemma 1 of [3] we have

$$\left( \sum_{w \in R} \chi(w) \right)^r = \sum_{n=1}^{Hr} \chi(n) a_n$$

where

$$\sum_{n \equiv Hr} |a_n|^2 \leq r! \pi(H)^r.$$
Thus we have
\[ \sum_{x \leq X} \sum_{\omega \in H} a_x \chi(\omega)^r = \sum_{x \leq \lambda} \sum_{\omega \in H} a_x \chi(\omega)^r. \]
and by Lemma 2. But by Lemma 1 the latter expression is
\[ \ll X^{-1/2} R X Q^{1/2} (H + X)^{1/2}. \]
by (15). Since \( D \) can be divided into \( \ll \log X \) such subsets \( D' \) we obtain
\[ \ll X^{1/2} \left( \sum_{x \leq \lambda} a_x \right)^2 \ll q^{1/2} \left( \log X \right)^{1/2}, \]
which completes the proof of the lemma.

We write
\[ T_q = \sum_{x \leq \lambda} a_x \chi(\omega)^r, \quad \text{and} \quad \varphi(q) = \sum_{\omega \in D} a_x \chi(\omega). \]

For any pair of parameters \( \lambda \) and \( R \), both greater than 1, we define
\[ S_\lambda = S_\lambda(\lambda, R) \]
to be the set of primes \( p \leq X^{1/2} \) and squares of such primes for which
\[ \varphi(q) < R \quad \text{and} \quad T_q > \lambda^{-1} \chi(H). \]

**Lemma 4.** Let
\[ 2 \leq H \leq X^{1/2}. \]
Then if \( H \) is sufficiently large we have
\[ \text{card} S_\lambda \ll X^{1/4} \frac{\log X}{\log H} \exp \left( \frac{\log (X^2 H) \log (12 R^2 \log X)}{4 \log H} \right), \]
the constant being absolute.

**Proof.** By Hölder's inequality if \( q \in S_\lambda \) we have
\[ T_q \ll \left( \sum_{x \leq \lambda} a_x \right)^{r-1} \sum_{x \leq \lambda} a_x \chi(\omega)^r. \]
Thus by Lemma 3 we obtain
\[ \sum_{q \in S_\lambda} T_q \ll R\gamma \left( H + X \right)^{1/2} \chi(H)^{r/2} (r!)^{1/2}; \]
and so since
\[ Q \ll X^{1/2} / \log X \]
we have
\[ \text{card} S_\lambda \ll R\gamma X^{1/2} \left( H^2 + X^2 \right)^{1/2} \chi(H)^{r/2} (r!)^{1/2}. \]

Now we choose
\[ r = \left[ \frac{3 \log X}{2 \log H} \right] + 1 = \left[ \frac{\log (X^{1/2} H)}{\log H} \right], \]
so that
\[ H^r > X^{3/2}, \]
and obtain (by applying the prime number theorem) that
\[ \text{card} S_\lambda \ll (r!)^{1/2} (1 + \delta)^{1/2} (\log H)^{r/2} \pi(X^{1/4}), \]
provided that \( H \) is sufficiently large (in terms of \( \delta \)). Finally by Stirling's formula for \( r! \) we deduce that
\[ \text{card} S_\lambda \ll \left( \frac{\log X}{\log H} \right)^{1/4} \pi(X^{1/4}) \exp \left( \frac{\log (X^{1/2} H) \log (2 X^2 \log X)}{2 \log H} \right) \]
as required.

We write
\[ V = (\log \log X)^2. \]

Let
\[ P = P(q) = \prod_{s \leq q} s, \]
the product being extended over primes \( s \). Define
\[ C_s^{(1)} = \begin{cases} \varphi(\text{ord} \chi)^{-1} & \text{if } 1 < \text{ord} \chi \leq P(q), \\ 0 & \text{otherwise}, \end{cases} \]
\[ C_s^{(2)} = \begin{cases} (\text{ord} \chi)^{-1} & \text{if } \text{ord} \chi \text{ is a prime } > V, \\ 0 & \text{otherwise}. \end{cases} \]

Then as in Lemma 4 of [3] we have that if \( \delta \)
\[ V > 4\phi(p^2) P(\phi(P)), \]
\[ T_{\delta}^{(1)} + T_{\delta}^{(2)} \leq \frac{\pi(H)}{\delta} \quad \text{and} \quad T_{\delta}^{(3)} + T_{\delta}^{(4)} \leq \frac{\phi(P)}{4P} \pi(H), \]
where \( P = P(p^2) \), and if \( H \) is sufficiently large
\[ h'(p) \leq H. \]

Let \( S_\lambda \) denote the subset of the set \( S_\lambda \) of primes \( \leq X^{1/2} \) and their squares, for which
\[ h'(p) \leq H. \]

(16) \[ h'(p) \phi(p^2) < (\log X)^B \]
and
\[ \phi(p^2) = \text{the number of distinct prime divisors of } n. \]
and
\[ h'(p) < D \left( \log X \right)^2 \left( \sigma^2(p^3) + \frac{p(p-1)}{\varphi(q(p)^2)} \right) \]
where \( D \) is an absolute constant to be determined later.

**Lemma 5.** We have
\[ \sum_{p \in S_4^{-1}} h(p) \ll X^{1/2}/(\log X)^2. \]

**Proof.** We denote by \( S_4(R_1, R_2, W) \) the subset of \( S_4 \) satisfying (16) and
\[ \frac{1}{2} W \leqslant P/\varphi(P) \leqslant W, \]
\[ \frac{1}{2} R_i \leqslant \sigma^2(q) < R_i, \quad i = 1, 2, \]
\[ T_0^2 > \lambda_i^{-1} \pi(H) \quad \text{for some } i = 1 \text{ or } 2 \]
where
\[ \lambda_0 = 8 \quad \text{and} \quad \lambda_2 = 8W. \]

We note that for \( S_5 \) to be non-empty we have \( \lambda_4, R_4 \) both
\[ \ll (\log X)^2. \]

We choose
\[ H = E(\log X)^3 \max_{i=1,2} (\lambda_i^2 R_i^4) \ll (\log X)^{12 H-1}. \]

Thus since
\[ S_5 \subset S_5^{(i)} \cup S_5^{(2)}, \]
we have by Lemma 4 that
\[ \text{card} S_5 \ll X^{1/4}(\log X)^{1/4} \exp \left\{ \frac{1}{4} \log (X^3 H) \left( 1 - \frac{\log E}{\log H} \right) \right\} \]
\[ \ll X^{1/4}(\log X)^{1/4} \exp \left\{ \frac{1}{4} \log X \left( 1 + O \left( \frac{\log \log X}{\log X} \right) \right) \left( 1 - \frac{\log E}{(12 B + 4) \log \log X} \right) \right\} \]
and so if \( E \) is sufficiently large
\[ \text{card} S_5 \ll X^{1/2}(\log X)^{2+1}. \]

From this we deduce Lemma 5 by the argument of Lemma 6 of [3].

**Proof of Theorem.** The proof of the theorem follows by the argument of [3].

References


Received on 16. 3. 1979

__________