ACTA ARITHMETICA
XVIII (1971)

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

$$\pi(X)^{-1} \sum_{p \leqslant X} g(p) \ll (\log X)^2 (\log\log X)^4 \tag{1}$$

for the average over all primes $p \leqslant X$ 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

$$\pi(X)^{-1} \sum_{p \leqslant X} h(p) \ll (\log X)^4 (\log\log X)^8. \tag{2}$$

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

$$\sum_{m \leqslant X} \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \Big| \sum_{n=1}^{N} e(an/q)\, a_n \Big|^2 \ll (X^2+N) \sum_{n=1}^{N} |a_n|^2 \tag{3}$$

where as usual $e(x) = e^{2\pi i x}$. In the estimation of $g(p)$ m in (3) ranged over the primes. In the estimation of $h(p)$ however m ranges over the $p^2 \leqslant X$ (together with the $p \leqslant X^{1/2}$) and it is this decrease in the size of the set of m that gives rise to the loss in effectiveness seen on comparing (2) 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

$$\pi(X)^{-1} \sum_{p \leqslant X} h(p) \ll (\log X)^3 (\log\log X)^6$$

the summation being extended over prime numbers p.

2. The Large Sieve.

LEMMA 1. *Let S be a set of positive integers. Suppose that*

$$S \subset [1, X]$$

and that the cardinality of S is Q. Then we have

$$\Big\{\Big|\sum_{q\in S}\sum_{\substack{a=1\\(a,q)=1}}^{q}\Big|\sum_{n=1}^{N}a_n e(an/q)\Big|\Big\}^2 \ll XQ(N+XQ)\sum_{n=1}^{N}|a_n|^2. \tag{4}$$

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

$$q'\in S,\quad 1\leqslant a'\leqslant q',\quad (a', q') = 1, \tag{5}$$

$$\left\|\frac{a}{q}-\frac{a'}{q'}\right\| \leqslant \frac{1}{4XQ}, \tag{6}$$

(where $\|x\|$ denotes the distance of x from the nearest integer). We write

$$\sum_{q\in S}\sum_{\substack{a=1\\(a,q)=1}}^{q}\Big|\sum_{n=1}^{N}a_n e(an/q)\Big| = \Sigma_1+\Sigma_2 \tag{7}$$

where Σ_1 contains those pairs for which $M(q, a) = 1$ and Σ_2 those for which $M(q, a) > 1$.

The estimation of both Σ_1 and Σ_2 is based on the beautiful inequality due to Davenport and Halberstam [4] that:

If $x_1, \ldots, x_R$ are real numbers and

$$\delta = \min_{j\neq k}\|x_j - x_k\|$$

then

$$\sum_{r=1}^{R}\Big|\sum_{n=1}^{N}a_n e(nx_r)\Big|^2 \ll (N+\delta^{-1})\sum_{n=1}^{N}|a_n|^2. \tag{8}$$

To estimate Σ_1 from this we put the x_r equal to those Farey fractions a/q corresponding to the summation conditions of Σ_1. Thus in this application of (8) we have

$$R \leqslant XQ \quad\text{and}\quad \delta \geqslant \frac{1}{4XQ},$$

and so

$$\Sigma_1^2 \leqslant R\sum_{r=1}^{R}\Big|\sum_{n=1}^{N}a_n e(nx_r)\Big|^2 \ll R(N+\delta^{-1})\sum_{n=1}^{N}|a_n|^2 \tag{9}$$

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

To estimate Σ_2 we assume (without loss of generality) that X is an integer, and we write

$$F(x) = \sum_{q\in S}\sum_{\substack{a=1\\(a,q)=1\\M(q,a)>1}}^{q}\sum_{\substack{y\equiv x\left(\bmod \frac{1}{XQ}\right)\\ \left|\frac{a}{q}-y\right|\leqslant\frac{1}{8XQ}}}\Big|\sum_{n=1}^{N}a_n e(an/q)\Big|.$$

Clearly we have

$$\int_0^{1/XQ}F(x)\,dx = \frac{1}{4XQ}\Sigma_2.$$

Thus we can choose x such that

$$F(x) \geqslant \tfrac{1}{4}\Sigma_2. \tag{10}$$

We write for this choice of x

$$F(x) = \sum_q\sum_a{}^{(1)}\Big|\sum_{n=1}^{N}a_n e(an/q)\Big|$$

where $\sum^{(1)}$ 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 $y \pmod 1$. For each $y \pmod 1$ choose that pair q, a, associated with y, to be included in the summation $\sum^{(2)}$ for which

$$\Big|\sum_{n=1}^{N}a_n e(an/q)\Big|$$

is maximal. Thus

$$F(x) \leqslant \sum_q\sum_a{}^{(2)}M(q, a)\Big|\sum_{n=1}^{N}a_n e(an/q)\Big|.$$

The summation $\sum^{(2)}$ is thus over a collection of pairs q, a for which the corresponding Farey fractions are at least $1/2XQ$ apart (mod 1). Hence

$$F(x)^2 \leqslant \Big\{\sum_q\sum_a{}^{(2)}M(q, a)^2\Big\}\sum_q\sum_a{}^{(2)}\Big|\sum_{n=1}^{N}a_n e(an/q)\Big|^2 \tag{11}$$

$$\ll \sum_q\sum_a{}^{(2)}M(q, a)^2(N+XQ)\sum_{n=1}^{N}|a_n|^2$$

by (8).

However we have

$$\sum_q\sum_a{}^{(2)}M(q, a)^2 \ll \sum_q\sum_a{}^{(3)}M(q, a) \tag{12}$$

where $\sum^{(3)}$ is restricted to those pairs that contribute to Σ_2. For each pair q, q' there are at most[1]

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

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

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

Only such pairs can satisfy

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

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

$$\Sigma_2^2 \ll XQ(N+XQ)\sum_{n=1}^{N}|a_n|^2.$$

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_χ be non-negative numbers. Then we have*

$$(13)\qquad \sum_{q\in S}\sum_{\chi}{}^{*} C_\chi\left|\sum_{n=1}^{N} a_n\chi(n)\right| \leqslant \sum_{q\in S} q^{-1/2}\Big(\sum_{\chi}{}^{*} C_\chi\Big)\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\sum_{n=1}^{N} a_n e(an/q)\right|$$

where the summation over χ is over primitive characters mod q.

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

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

where

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

[1] (a, b) denotes the highest common factor of a and b.

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

$$\sum_{q\in S}\sum_{\chi}{}^{*} C_\chi q^{-1/2}\left|\sum_{n=1}^{N} a_n \sum_{\substack{a=1\\(a,q)=1}}^{q}\bar{\chi}(a)e(an/q)\right| \leqslant \sum_{q\in S} q^{-1/2}\Big(\sum_{\chi}{}^{*} C_\chi\Big)\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\sum_{n=1}^{N} a_n e(an/q)\right|$$

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 my estimates for character sums mod p^2 of [2] into the argument of my estimation of $g(p)$ in [1]. The result obtained is that

$$(14)\qquad h(p) = O(p^{1/2+\varepsilon}).$$

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

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

where $h'(p)$ is the least prime primitive root mod p^2, then

$$\sum_{\substack{p\leqslant X^{1/2}\\ p\notin S_1}} h(p) \ll X^{1/2}(\log X)^2.$$

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*

$$\sum_{\chi}{}^{*} C_\chi < R.$$

Then we have

$$\Big(\sum_{q\in S}\sum_{\chi}{}^{*} C_\chi\Big|\sum_{w\leqslant H}\chi(w)\Big|^r\Big)^2 \ll R^2 Q(H^r + XQ)\pi(H)^r r!\log X,$$

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

$$Y < q \leqslant 2Y$$

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

$$\Big(\sum_{w\leqslant H}\chi(w)\Big)^r = \sum_{n=1}^{H^r}\chi(n)a_n$$

where

$$(15)\qquad \sum_{n\leqslant H^r}|a_n|^2 \leqslant r!\,\pi(H)^r.$$

Thus we have

$$\sum_{q\in S'}\sum_{\chi}^{*} C_\chi\Big|\sum_{w\leqslant H}\chi(w)\Big|^r = \sum_{q\in S'}\sum_{\chi}^{*} C_\chi\Big|\sum_{n=1}^{H^r}\chi(n)\alpha_n\Big|$$

$$\leqslant \sum_{q\in S'} q^{-1/2}\Big(\sum_{\chi}^{*} C_\chi\Big)\sum_{\substack{a=1\\(a,q)=1}}^{q}\Big|\sum_{n=1}^{H^r}\alpha_n e(an/q)\Big|$$

by Lemma 2. But by Lemma 1 the latter expression is

$$\leqslant Y^{-1/2}R(YQ')^{1/2}(H^r+YQ')^{1/2}\Big(\sum_{n=1}^{H^r}|\alpha_n|^2\Big)^{1/2}$$

$$\leqslant RQ'^{1/2}(H^r+XQ)^{1/2}\big(r!\,\pi(H)^r\big)^{1/2}$$

by (15). Since S can be divided into $\ll \log X$ such subsets S' we obtain

$$\sum Q'^{1/2} \ll \Big(\sum 1\Big)^{1/2}\Big(\sum Q'\Big)^{1/2} \ll Q^{1/2}(\log X)^{1/2}$$

which completes the proof of the lemma.

We write

$$T_q = \sum_{\chi}^{*} C_\chi\Big|\sum_{w\leqslant H}\chi(w)\Big|, \quad \text{and} \quad \varrho(q) = \sum_{\chi}^{*} C_\chi.$$

For any pair of parameters λ and R, both greater than 1, we define

$$S_2 = S_2(\lambda, R)$$

to be the set of primes $p \leqslant X^{1/2}$ and squares of such primes for which

$$\varrho(q) < R \quad \text{and} \quad T_q > \lambda^{-1}\pi(H).$$

LEMMA 4. *Let*

$$2 \leqslant H \leqslant X^{2/3}.$$

Then if H is sufficiently large we have

$$\operatorname{card} S_2 \ll X^{1/4}\left(\frac{\log X}{\log H}\right)^{1/4}\exp\left\{\frac{\log(X^3H^2)\log(\lambda^2R^2\log X)}{4\log H}\right\}$$

the constant being absolute.

Proof. By Hölder's inequality if $q\in S_2$ we have

$$T_q^r \leqslant \Big(\sum_{\chi}^{*} C_\chi\Big)^{r-1}\sum_{\chi}^{*} C_\chi\Big|\sum_{w\leqslant H}\chi(w)\Big|^r.$$

Thus by Lemma 3 we obtain

$$\sum_{q\in S_2} T_q^r \ll R^r Q^{1/2}(H^r+XQ)^{1/2}\big(\pi(H)^r r!\log X\big)^{1/2}$$

and so since

$$Q \ll X^{1/2}/\log X$$

we have

$$\operatorname{card} S_2 \ll R^r X^{1/4}(H^r+X^{3/2})^{1/2}\lambda^r\pi(H)^{-r/2}(r!)^{1/2}.$$

Now we choose

$$r = \left[\frac{3\log X}{2\log H}\right]+1 = \left[\frac{\log(X^{3/2}H)}{\log H}\right],$$

so that

$$H^r > X^{3/2},$$

and obtain (by applying the prime number theorem) that

$$\operatorname{card} S_2 \ll R^r(r!)^{1/2}(1+\delta)^{r/2}(\log H)^{r/2}\lambda^r X^{1/4}$$

provided that H is sufficiently large (in terms of δ). Finally by Stirling's formula for $r!$ we deduce that

$$\operatorname{card} S_2 \ll \left(\frac{\log X}{\log H}\right)^{1/4} X^{1/4}\exp\left\{\frac{\log(X^{3/2}H)\log(\lambda^2R^2\log X)}{2\log H}\right\}$$

as required.

We write

$$V = (\log\log X)^2.$$

Let

$$P = P(q) = \prod_{\substack{s|\varphi(q)\\ s\leqslant V}} s,$$

the product being extended over primes s. Define

$$C_\chi^{(1)} = \begin{cases}\varphi(\operatorname{ord}\chi)^{-1} & \text{if } 1<\operatorname{ord}\chi\,|\,P(q),\\ 0 & \text{otherwise,}\end{cases}$$

$$C_\chi^{(2)} = \begin{cases}(\operatorname{ord}\chi)^{-1} & \text{if } \operatorname{ord}\chi \text{ is a prime } > V,\\ 0 & \text{otherwise.}\end{cases}$$

Then as in Lemma 4 of [3] we have that if (²)

$$V \geqslant 4\nu\big(\varphi(p^2)\big)P/\varphi(P),$$

$$T_p^{(1)}+T_{p^2}^{(1)} \leqslant \frac{\pi(H)}{4} \quad \text{and} \quad T_p^{(2)}+T_{p^2}^{(2)} \leqslant \frac{\varphi(P)}{4P}\pi(H),$$

where $P = P(p^2)$, and if H is sufficiently large

$$h'(p) \leqslant H.$$

Let S_3 denote the subset of the set S_4 of primes $\leqslant X^{1/2}$ and their squares, for which

(16) $$h'(p)\tau\big(\varphi(p^2)\big) < (\log X)^B$$

(²) $\nu(n)$ = the number of distinct prime divisors of n.

and

$$h'(p) < D(\log X)^3 \left(\varrho^{(1)}(p^2) + \varrho^{(2)}(p^2)\,\frac{p(p-1)}{\varphi(\varphi(p^2))}\right)^6$$

where D is an absolute constant to be determined later.

LEMMA 5. *We have*

$$\sum_{q \in S_4 - S_3} h(p) \ll X^{1/2}/(\log X)^2.$$

Proof. We denote by $S_5(R_1, R_2, W)$ the subset of S_4 satisfying (16) and

$$\tfrac{1}{2}W \leqslant P/\varphi(P) < W,$$

$$\tfrac{1}{2}R_i \leqslant \varrho^{(i)}(q) < R_i, \quad i = 1, 2,$$

$$T_q^{(i)} > \lambda_i^{-1}\pi(H) \quad \text{for some } i = 1 \text{ or } 2$$

where

$$\lambda_1 = 8 \quad \text{and} \quad \lambda_2 = 8W.$$

We note that for S_5 to be non-empty we have λ_i, R_i both

$$\ll (\log X)^B.$$

We choose

$$H = E(\log X)^3 \max_{i=1,2} (\lambda_i^6 R_i^6) \ll (\log X)^{12B+3}.$$

Thus since

$$S_5 \subset S_2^{(1)} \cup S_2^{(2)},$$

we have by Lemma 4 that

$$\operatorname{card} S_5 \ll X^{1/4}(\log X)^{1/4} \exp\left\{\tfrac{1}{12}\log(X^3 H)\left(1 - \frac{\log E}{\log H}\right)\right\}$$

$$\ll X^{1/4}(\log X)^{1/4} \exp\left\{\tfrac{1}{4}\log X\left(1 + O\left(\frac{\log\log X}{\log X}\right)\right)\left(1 - \frac{\log E}{(12B+4)\log\log X}\right)\right\}$$

and so if E is sufficiently large

$$\operatorname{card} S_5 \ll X^{1/2}(\log X)^{B+5}.$$

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

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

[2] — *On character sums and L-series II*, Proc. London Math. Soc. (3), 13 (1963), pp. 524–536.

[3] — and P. D. T. A. Elliott, *The average of the least primitive root*, Mathematika 15 (1968), pp. 39–50.

[4] H. Davenport and H. Halberstam, *The values of a trigonometrical polynomial at well spaced points*, Mathematika 13 (1966), pp. 91–96.

DEPARTMENT OF MATHEMATICS
THE UNIVERSITY
Nottingham, NG7 2RD

Received on 15. 3. 1970