ACTA ARITHMETICA
LXXII.1 (1995)

On prime primitive roots

by

Amora Nongkynrih (Madras)

Notation. The letters p, q and l denote prime numbers. For a positive real number H, $N(H,p)$ denotes the number of primes $q \le H$ which are primitive roots $(\bmod p)$. $N(\sigma,T,\chi)$ denotes the number of zeros of the Dirichlet L-function $L(s,\chi)$ in the rectangle $\sigma \le \operatorname{Re} s \le 1$, $-T \le \operatorname{Im} s \le T$.

For a given prime p, let

$$F_p(s) = \prod_{\chi \,(\bmod p)} L(s,\chi).$$

For any positive integer k, $\log_k x$ is defined as follows: $\log_1 x := \log x$ and for $k \ge 2$, we inductively define $\log_k x = \log_{k-1} \log x$.

$[x]$ denotes the integral part of x.

1. Introduction. The purpose of this paper is to prove a result on the distribution of primitive roots, similar to one which appeared in a paper of Elliott [3], in which he obtained an asymptotic formula for $N(H,p)$, valid for "almost all" primes p. More precisely, he obtained the following (Theorem 1 of [3]):

Let ε and B be arbitrary positive constants. Then there is a set of primes E, and a positive constant $F = F(\varepsilon, B)$, so that for all p not in E the estimate

$$N(H,p) = \frac{\phi(p-1)}{p-1}\,\pi(H)\left\{1 + O\left(\frac{1}{(\log H)^B}\right)\right\}$$

holds uniformly for $H \ge \exp(F \log_2 p \log_3 p)$. Moreover, the sequence E satisfies $E(x) = O(x^{\varepsilon})$ for all large values of x.

In proving the result, Elliott had applied the *first fundamental lemma* (Lemma 4 of [3]), but there appears to be some discrepancy in the choice of the parameters in the application of the lemma. In this paper, we use a zero density estimate for L-functions and Brun's sieve to obtain an asymptotic formula for $N(H,p)$ which holds uniformly, for "almost all" primes p, in a larger range for H than that stated in [3]. This arises as a special case of the asymptotic formula for $N(H,p)$ which holds for "almost all" p, in a wider range for H at the expense of a weaker error term.

The theorem to be proved is the following:

THEOREM 1.1. *Let α be a real number satisfying $0 < \alpha e^{1+\alpha} \le 1$. Then for almost all primes p, the following statement is true*:

Let $\alpha \ge c/(\log_2 p)^{1/2}$, for a suitable constant c. Then, given $B > 0$, there exists $C = C(B)$ such that whenever $H \ge \exp((C\log_2 p)/\alpha)$,

$$N(H,p) = \frac{\phi(p-1)}{p-1}\,\pi(H)(1+O(\alpha^{B/\alpha})). \tag{1}$$

Furthermore, the number of primes up to Y for which (1) *does not hold is*

$$O\biggl(\exp\biggl(\frac{G\log Y\log_2 Y}{\log H}\biggr)\biggr)$$

where G is a constant.

Choosing $\alpha = \log_4 p/\log_3 p$ in Theorem 1.1, we get the following:

THEOREM 1.2. *Let ε and B be arbitrary constants. Then for almost all primes p, the following holds*:

$$N(H,p) = \frac{\phi(p-1)}{p-1}\,\pi(H)\biggl(1+O\biggl(\frac{1}{(\log H)^B}\biggr)\biggr) \tag{2}$$

whenever

$$H \ge \exp\biggl(\frac{C\log_2 p\log_3 p}{\log_4 p}\biggr),$$

for some constant $C = C(\varepsilon, B)$. Furthermore, the number of primes up to Y for which (2) *does not hold is $O(Y^{\varepsilon})$.*

COROLLARY 1.3. *If $E(Y)$ denotes the number of primes up to Y for which* (1) *does not hold, then $E(Y) = O((\log Y)^F)$ when $H \ge Y^{\delta}$, for some δ and for some F, with $0<\delta<1$ and $F = F(\delta)$.*

2. The exceptional primes. Call a prime p an *exceptional prime* if (1) does not hold for p.

We need a lemma which was proved in a paper of Burgess and Elliott [1]. However, for our purposes, we require a different approach. We shall use Perron's formula to prove this lemma, and then apply a zero density estimate for L-functions. This will show that the number of exceptional primes is small.

To start with, we recall below the notation of Burgess and Elliott [1]: Let $\{\beta_{d,p}\}$ denote a double sequence of real numbers satisfying

$$0 \le \beta_{d,p} \le 1/\phi(d).$$

Define

$$T_p = \sum_{\substack{d\mid p-1\\ d>1}} \beta_{d,p} \sum_{\chi_d \pmod p} \Big|\sum_{q\le H} \chi_d(q)\Big|$$

where χ_d runs through the characters $\pmod p$ whose order is d. Let

$$\varrho(p) = \sum_{\substack{d\mid p-1\\ \beta_{d,p}>0}} 1.$$

Let λ, R be positive real numbers, $Y \ge 3$. Define

$$S_1 = S_1(\lambda, R) = \{p \le Y : \varrho(p) < R,\ T_p > \pi(H)/\lambda\}.$$

LEMMA 2.1. *If p is a prime for which $L(s,\chi)$ does not vanish for any character χ modulo p (that is, $F_p(s) \ne 0$) in* $\operatorname{Re} s > 1-\varepsilon$, *and $\varrho(p) < R$, then $T_p = O(\pi(H)/\lambda)$, provided*

$$\varepsilon \ge \max\left(\frac{4\log R}{\log H}, \frac{2\log\lambda}{\log H}, \frac{12\log_2 p}{\log H}\right).$$

Proof. Let a and T be real numbers such that $a > 1$ and T is sufficiently large. By Perron's formula, we have

$$\sum_{n\le H} \chi_d(n)\Lambda(n) = \frac{1}{2\pi i}\int_{a-iT}^{a+iT} \{L'(s,\chi_d)/L(s,\chi_d)\}\frac{H^s}{s}\,ds + O\left(\frac{H^a\log^2 pT}{T}\right)$$

since $L'(s,\chi_d)/L(s,\chi_d) = O(\log^2 pT)$ in $-1 < \operatorname{Re} s \le 2$, for a suitable choice of $\operatorname{Im} s = T$. (See, for example, [2].) Choose $a = 1 + 1/\log H$.

Since we are considering only primes p with $F_p(s) \ne 0$ in $\operatorname{Re} s > 1-\varepsilon$, moving the line of integration to $\operatorname{Re} s = 1-\varepsilon$ gives

$$\begin{aligned}\sum_{n\le H} \chi_d(n)\Lambda(n) &= \frac{1}{2\pi i}\int_{1-\varepsilon-iT}^{1-\varepsilon+iT} \{L'(s,\chi_d)/L(s,\chi_d)\}\frac{H^s}{s}\,ds + O\left(\frac{H\log^2 pT}{T}\right)\\ &= O(H^{1-\varepsilon}\log^2 pT\log T).\end{aligned}$$

In particular, choosing $T = p$, we get

$$\sum_{n\le H} \chi_d(n)\Lambda(n) = O(H^{1-\varepsilon}\log^3 p). \tag{3}$$

Notice that

$$\sum_{q<H} \chi_d(q)\log q = \sum_{n<H} \chi_d(n)\Lambda(n) + O(H^{1/2})$$

and that

$$\sum_{n<m} \chi_d(n)\Lambda(n) = O(m^{1-\varepsilon}\log^3 p) \quad \text{for all } m < H.$$

Thus, using Abel's identity and (3) it follows that

$$\sum_{q<H} \chi_d(q) = O(H^{1-\varepsilon}\log^3 p). \tag{4}$$

Therefore,

$$\begin{aligned} T_p &= \sum_{\substack{d\mid p-1\\ d>1}} \beta_{d,p} \sum_{\chi_d \ (\mathrm{mod}\ p)} \Big| \sum_{q<H} \chi_d(q) \Big| \\ &\ll H^{1-\varepsilon}\log^3 p \sum_{\substack{d\mid p-1\\ d>1}} \beta_{d,p}\phi(d) = H^{1-\varepsilon}\log^3 p \Big(\sum_{\substack{d\mid p-1\\ \beta_{d,p}>0}} 1 \Big) \\ &= H^{1-\varepsilon}(\log^3 p)R = H^{1-\varepsilon/4}\lambda^{-1}(H^{-\varepsilon/2}\lambda)(H^{-\varepsilon/4}R)\log^3 p. \end{aligned}$$

Hence $T_p = O(\pi(H)/\lambda)$ whenever the following conditions hold: (i) $H^{-\varepsilon/2}\lambda < 1$, (ii) $H^{-\varepsilon/4}R < 1$ and (iii) $\log^3 p < H^{\varepsilon/4}$.

This completes the proof of the lemma.

We choose $R = (\log p)^A$, where A is a sufficiently large constant, and $\lambda > R^2$; the value of λ will be chosen in due course.

LEMMA 2.2.

$$\#S_1 \ll \log^{14} Y \exp\left(C\frac{\log\lambda \log Y}{\log H}\right).$$

Proof. Let $\varepsilon = 2\log\lambda/\log H$. Then

$$\varepsilon \geq \max\left(\frac{4\log R}{\log H}, \frac{2\log\lambda}{\log H}, \frac{12\log_2 p}{\log H}\right).$$

Further, for any $p \in S_1$, $T_p > \pi(H)/\lambda$. Therefore, by Lemma 2.1, it follows that

$$S_1 \subseteq \{p \leq Y : F_p(s) = 0 \text{ for some } s \text{ in the rectangle } 1-\varepsilon \leq \operatorname{Re} s \leq 1,\ -Y \leq \operatorname{Im} s \leq Y\}.$$

Using the estimate

$$\sum_{p\leq Y} \sideset{}{'}\sum_{\chi} N(\sigma, T, \chi) \ll (Y^2T)^{2(1-\sigma)/\sigma}(\log YT)^{14}$$

(here $\sum'_\chi$ = the sum over all primitive characters χ modulo p) for $4/5 \leq \sigma \leq 1$ (cf. Montgomery [5], p. 99), and also using our specific choice of ε, we see that

$$\begin{aligned} \sum_{Y<p\leq 2Y} \sum_{\chi \ (\mathrm{mod}\ p)} N(1-\varepsilon, Y, \chi) &\ll (Y^3)^{2\varepsilon/(1-\varepsilon)}(\log Y)^{14} \\ &\ll Y^{(C\log\lambda)/\log H}(\log Y)^{14}. \end{aligned}$$

Hence $\#S_1 \ll (\log Y)^{14}\exp(C\log\lambda\log Y/\log H)$, which proves the lemma.

3. Derivation of the asymptotic formula. In this section, we consider only those primes for which $F_p(s) \neq 0$ in $\operatorname{Re} s > 1 - \varepsilon$, with ε as chosen in Section 2. Given a prime p with this property, we obtain an asymptotic formula for the number of prime primitive roots $(\bmod\, p)$ which are less than H.

Notice that if $d \mid p-1$, then

$$\frac{1}{d} \sum_{\substack{\chi \,(\bmod\, p)\\ \operatorname{ord} \chi \mid d}} 1 = \begin{cases} 1 & \text{if } d \mid \operatorname{ind} q, \\ 0 & \text{otherwise}, \end{cases}$$

where "ind q" stands for the index of q with respect to a fixed primitive root mod$p$.

Let l denote a prime divisor of $p-1$. Then

$$\#\{q \le H : q \text{ is not a primitive root } (\bmod\, p)\}$$
$$\le \sum_{l \mid p-1} \frac{1}{l} \sum_{\operatorname{ord} \chi \mid l} \sum_{q \le H} \chi(q) = \pi(H) \sum_{l \mid p-1} \frac{1}{l} + \sum_{l \mid p-1} \frac{1}{l} \sum_{\chi_l} \sum_{q \le H} \chi_l(q).$$

We break each sum into two parts: (i) $l \le \log^2 p$, (ii) $l > \log^2 p$.

Lemma 3.1 below deals with the sum in (i) using Brun's sieve, and in Lemma 3.2 we estimate the sum in (ii) using Lemma 2.1. With notations as in [4], we state the following theorem, which is Brun's sieve in the form needed for our application (cf. [4], p. 57).

THEOREM 3.1. *Assume that the following conditions hold*:

(a)

$$1 \le \frac{1}{1 - \omega(p)/p} \le A_1$$

for some suitable constant $A_1 \ge 1$.

(b) *For suitable constants* $\kappa > 0$ *and* $A_2 \ge 1$,

$$\sum_{w < p < z} \frac{\omega(p) \log p}{p} \le \kappa \log \frac{z}{w} + A_2$$

if $2 \le w \le z$.

(c) $|R_d| \le \omega(d)$ *if* $\mu(d) \neq 0$ *and* $\omega(d) \neq 0$.

Let α *be a real number satisfying* $0 < \alpha e^{1+\alpha} \le 1$, *and let* b *be a positive integer. Then*

$$S(\mathcal{A}; \wp, z) \le XW(z)\Big\{1 + 2\frac{\alpha^{2b+1} e^{2\alpha}}{1 - \alpha^2 e^{2+2\alpha}} \exp\Big(\frac{(2b+3)c_1}{\alpha \log z}\Big)\Big\} + O\big(z^{2b + \{2.01/(e^{2\alpha/\kappa} - 1)\}}\big) \tag{5}$$

and

$$(6)\qquad S(\mathcal{A};\wp,z)\ge XW(z)\bigg\{1-2\frac{\alpha^{2b}e^{2\alpha}}{1-\alpha^2e^{2+2\alpha}}\exp\bigg(\frac{(2b+2)c_1}{\alpha\log z}\bigg)\bigg\} + O(z^{2b-1+\{2.01/(e^{2\alpha/\kappa}-1)\}})$$

where

$$c_1=\frac{A_2}{2}\bigg\{1+A_1\bigg(\kappa+\frac{A_2}{\log 2}\bigg)\bigg\}.$$

Remark 1. The constants implied by the use of the O-notation do not depend on b and α.

Remark 2. The replacement of the condition (c) of the theorem by the more general $|R_d|\le L\omega(d)$ changes the theorem only to the extent of introducing a factor L into the last error term in each of (5) and (6).

LEMMA 3.1 (Application of Brun's sieve). *Let p be a prime for which $F_p(s)$ is non-zero in $\operatorname{Re} s>1-(2\log\lambda/\log H)$. Let $\mathcal{A}=\{\operatorname{ind} q: q\le H\}$, $z=\log^2 p$, and $\wp=$ the set of all prime divisors l of $p-1$. Then*

$$S(\mathcal{A};\wp,z)=\frac{\phi(p-1)}{p-1}\pi(H)(1+O(\alpha^{B/\alpha}))$$

where α is a real number satisfying $0<\alpha e^{1+\alpha}\le 1$, $\alpha\gg 1/(\log z)^{1/2}$, and B is a constant.

Proof. With these choices of $\mathcal{A}$, $\wp$ and z, it follows that

$$\omega(p)=1\quad \text{if } p\in\wp,\quad X=\pi(H),\quad \kappa=1,$$

and

$$W(z)=\prod_{\substack{q\mid p-1\\ q<z}}\bigg(1-\frac{1}{q}\bigg).$$

We see that

$$\#\{q\le H: d\mid \operatorname{ind} q,\ d\mid p-1\}=\frac{1}{d}\sum_{q\le H}\sum_{\substack{\chi\,(\mathrm{mod}\,p)\\ \mathrm{ord}\,\chi\mid d}}\chi(q).$$

Hence,

$$|\mathcal{A}_d|=\frac{1}{d}\sum_{\substack{\chi\,(\mathrm{mod}\,p)\\ \mathrm{ord}\,\chi\mid d}}\sum_{q\le H}\chi(q)=\frac{1}{d}\pi(H)+\frac{1}{d}\sum_{\substack{\chi\ne\chi_0\\ \mathrm{ord}\,\chi\mid d}}\sum_{q\le H}\chi(q)$$
$$=\frac{1}{d}\pi(H)+\frac{1}{d}\sum_{\substack{t\mid d\\ t>1}}\sum_{\chi_t}\sum_{q\le H}\chi_t(q)$$

where χ_t runs through characters of order t. Therefore,

$$R_d = \frac{1}{d} \sum_{\substack{t|d \\ t>1}} \sum_{\chi_t} \sum_{q \le H} \chi_t(q).$$

Using (4), we get

$$|R_d| \ll \frac{1}{d} \sum_{t|d} \sum_{\chi_t} \Big| \sum_{q \le H} \chi_t(q) \Big| \ll \Big(\frac{1}{d} \sum_{t|d} \sum_{\chi_t} 1 \Big) H^{1-\varepsilon} \log^3 p$$
$$\ll \Big(\frac{1}{d} \sum_{t|d} \phi(t) \Big) H^{1-\varepsilon} \log^3 p = H^{1-\varepsilon} \log^3 p \ll \pi(H)/\lambda.$$

The last step follows as in the proof of Lemma 2.1. We take $b = [1/\alpha]$ in Theorem 3.1, and Brun's sieve then gives

$$S(\mathcal{A}; \wp, z) \le \pi(H) W(z) \Big\{ 1 + 2 \frac{\alpha^{2b+1} e^{2\alpha}}{1 - \alpha^2 e^{2+2\alpha}} \exp\Big(\frac{(2b+3)c_1}{\alpha \log z} \Big) \Big\} + O\Big(\frac{\pi(H)}{\lambda} z^{2b + \{2.01/(e^{2\alpha}-1)\}} \Big) \tag{7}$$

and

$$S(\mathcal{A}; \wp, z) \ge \pi(H) W(z) \Big\{ 1 - 2 \frac{\alpha^{2b} e^{2\alpha}}{1 - \alpha^2 e^{2+2\alpha}} \exp\Big(\frac{(2b+2)c_1}{\alpha \log z} \Big) \Big\} + O\Big(\frac{\pi(H)}{\lambda} z^{2b - 1 + \{2.01/(e^{2\alpha}-1)\}} \Big) \tag{8}$$

with

$$W(z) = \prod_{q|p-1} \Big(1 - \frac{1}{q} \Big) \prod_{\substack{q|p-1 \\ q \ge z}} \Big(1 - \frac{1}{q} \Big)^{-1}$$
$$= \frac{\phi(p-1)}{p-1} \Big(1 + O\Big(\frac{1}{\log p \log_2 p} \Big) \Big).$$

With our choice of b, we now estimate the error terms in (7). Similar estimates can be obtained for the inequality (8). The estimate for the first error term is

$$\frac{\alpha^{2b+1} e^{2\alpha}}{1 - \alpha^2 e^{2+2\alpha}} \exp \frac{(2b+3)c_1}{\alpha \log z} \ll \alpha^{B/\alpha}$$

whenever $\alpha^2 \gg 1/\log z$. Since α is small, the last O-term satisfies

$$\frac{\pi(H)}{\lambda} \exp((2b + \{2.01/(e^{2\alpha} - 1)\}) \log z) \ll \frac{\pi(H)}{\lambda} z^{B'/\alpha}$$

for a constant B'. We choose $\lambda > z^{B'/\alpha} = (\log p)^{2B'/\alpha}$. For our purposes, we take λ to satisfy $\log \lambda = (C' \log_2 p)/\alpha$, for a sufficiently large constant C'.

Using the estimates in (7) and (8), it follows that

$$S(\mathcal{A};\wp,z)=\frac{\phi(p-1)}{p-1}\pi(H)\biggl(1+O\biggl(\frac{1}{\log p\log_2 p}\biggr)\biggr)(1+O(\alpha^{B/\alpha}))+O\biggl(\frac{\pi(H)z^{B'/\alpha}}{\lambda}\biggr).$$

Therefore, we get

$$S(\mathcal{A};\wp,z)=\frac{\phi(p-1)}{p-1}\pi(H)(1+O(\alpha^{B/\alpha})),$$

which proves the lemma.

We now consider the sum in (ii).

LEMMA 3.2. *Let*

$$L=\sum_{l>\log^2 p}\frac{1}{l}\Bigl(\pi(H)+\sum_{\chi_l}\sum_{q\le H}\chi_l(q)\Bigr).$$

Then $L=O(\pi(H)/\log p)$.

Proof.

$$L=\pi(H)\sum_{l>\log^2 p}\frac{1}{l}+\sum_{l>\log^2 p}\frac{1}{l}\sum_{\chi_l}\sum_{q\le H}\chi_l(q).$$

Then

$$|L|\le\frac{\pi(H)}{\log p}+\sum_{l>\log^2 p}\frac{1}{l}\sum_{\chi_l}\Bigl|\sum_{q\le H}\chi_l(q)\Bigr|\ll\frac{\pi(H)}{\log p}+\frac{\pi(H)}{\lambda},$$

applying Lemma 2.1 to the second sum on the right with

$$\beta_{l,p}=\begin{cases}1/l & \text{if } l\mid p-1,\ l>\log^2 p,\\ 0 & \text{otherwise.}\end{cases}$$

Therefore, $L=O(\pi(H)/\log p)$.

Proof of Theorem 1.1. Lemmas 3.1 and 3.2 imply that for almost all primes p,

$$N(H,p)=\frac{\phi(p-1)}{p-1}\pi(H)(1+O(\alpha^{B/\alpha}))$$

where $\alpha\gg 1/(\log_2 p)^{1/2}$ and whenever $H\ge\exp((C\log_2 p)/\alpha)$ for some constant $C=C(B)$. Lemma 2.2 shows that the number of exceptional primes up to Y is

$$\ll(\log Y)^{14}\exp\biggl(\frac{C\log Y\log_2 Y}{\alpha\log H}\biggr).$$

This completes the proof of Theorem 1.1. ∎

Acknowledgements. This paper is the result of a suggestion made by Professor M. Ram Murty. I would like to thank him and Professor R. Balasubramanian for constant guidance and encouragement.

References

[1] D. A. Burgess and P. D. T. A. Elliott, *On the average value of the least primitive root*, Mathematika 15 (1968), 39–50.
[2] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Graduate Texts in Math. 74, Springer, New York, 1980.
[3] P. D. T. A. Elliott, *The distribution of primitive roots*, Canad. J. Math. 21 (1969), 822–841.
[4] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.
[5] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, Berlin, 1971.

THE INSTITUTE OF MATHEMATICAL SCIENCES
C.I.T. CAMPUS
MADRAS 600113, INDIA
E-mail: AMORA@IMSC.ERNET.IN

Received on 10.11.1993
and in revised form on 13.5.1994 (2518)