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 $q \leq H$ which are primitive roots $\pmod{p}$. $N(\sigma, T, \chi)$ denotes the number of zeros of the Dirichlet $L$-function $L(s, \chi)$ in the rectangle $\sigma \leq \Re s \leq 1$, $-T \leq \Im s \leq T$.

For a given prime $p$, let

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

For any positive integer $k$, $\log_k x$ is defined as follows: $\log_1 x := \log x$ and for $k \geq 2$, 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 $\varepsilon$ 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

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

holds uniformly for $H \geq \exp(F \log \log p)$. 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 $\alpha$ be a real number satisfying $0 < \alpha e^{1+\alpha} \leq 1$. Then for almost all primes $p$, the following statement is true:

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

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

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

$$O\left( \exp \left( G \log Y \frac{\log_2 Y}{\log H} \right) \right)$$

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 $\varepsilon$ and $B$ be arbitrary constants. Then for almost all primes $p$, the following holds:

$$(2) \quad N(H, p) = \frac{\phi(p - 1)}{p - 1} \pi(H) \left( 1 + O\left( \frac{1}{(\log H)^{\varepsilon}} \right) \right)$$

whenever

$$H \geq \exp \left( C \log_2 p \log_3 p \right),$$

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 $H \geq Y^{\delta}$, for some $\delta$ 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

$$0 \leq \beta_{d, p} \leq 1/\phi(d).$$
Define
\[ T_p = \sum_{d \mid p-1} \beta_{d,p} \sum_{\chi_d \mod p} \left| \sum_{q \leq H} \chi_d(q) \right| \]
where \( \chi_d \) runs through the characters \( \mod p \) whose order is \( d \). Let
\[ g(p) = \sum_{d \mid p-1} \beta_{d,p} > 0. \]

Let \( \lambda, R \) be positive real numbers, \( Y \geq 3 \). Define
\[ S_1 = \{ p \leq Y : g(p) < R, T_p > \pi(H)/\lambda \}. \]

**Lemma 2.1.** If \( p \) is a prime for which \( L(s, \chi) \) does not vanish for any character \( \chi \) modulo \( p \) (that is, \( F_p(s) \neq 0 \)) in \( \Re s > 1 - \varepsilon \), and \( g(p) < R \), then \( T_p = O(\pi(H)/\lambda) \), provided \( \varepsilon \geq \max \left( \frac{4 \log R}{\log H} - \frac{2 \log \lambda}{\log H} + \frac{12 \log_2 p}{\log H} \right) \).

**Proof.** Let \( a \) and \( T \) be real numbers such that \( a > 1 \) and \( T \) is sufficiently large. By Perron’s formula, we have
\[
\sum_{n \leq H} \chi_d(n) \Lambda(n) = \frac{1}{2\pi i} \int_{\alpha-iT}^{\alpha+iT} \{ L'(s, \chi_d)/L(s, \chi_d) \} \frac{H^s}{s} ds + O\left( \frac{H^{a} \log^2 p T}{T} \right)
\]
since \( L'(s, \chi_d)/L(s, \chi_d) = O(\log^2 p T) \) in \( -1 < \Re s \leq 2 \), for a suitable choice of \( \Im s = T \). (See, for example, [2].) Choose \( a = 1 + 1/\log H \).

Since we are considering only primes \( p \) with \( F_p(s) \neq 0 \) in \( \Re s > 1 - \varepsilon \), moving the line of integration to \( \Re s = 1 - \varepsilon \) gives
\[
\sum_{n \leq H} \chi_d(n) \Lambda(n) = \frac{1}{2\pi i} \int_{1-\varepsilon-iT}^{1-\varepsilon+iT} \{ L'(s, \chi_d)/L(s, \chi_d) \} \frac{H^s}{s} ds + O\left( \frac{H \log^2 p T T}{T} \right)
\]
is a simple way of expressing the fact that
\[ \sum_{n \leq H} \chi_d(n) \Lambda(n) = O(H^{1-\varepsilon} \log^2 p T T). \]
In particular, choosing \( T = p \), we get
\[ (3) \sum_{n \leq H} \chi_d(n) \Lambda(n) = O(H^{1-\varepsilon} \log^3 p). \]
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
\( \sum_{q < H} \chi_d(q) = O(H^{1-\varepsilon} \log^3 p). \)

Therefore,
\[
T_p = \sum_{d \mid p-1} \beta_{d,p} \sum_{d > 1} \chi_{d, \text{mod } p} \left| \sum_{q < H} \chi_d(q) \right|
\ll H^{1-\varepsilon} \log^3 p \sum_{d \mid p-1} \beta_{d,p} \phi(d) = H^{1-\varepsilon} \log^3 p \left( \sum_{\beta_{d,p} > 0} 1 \right)
= H^{1-\varepsilon}(\log^3 p)R = H^{1-\varepsilon/4} \lambda^{-1}(H^{-\varepsilon/2}\lambda)(H^{-\varepsilon/4}R) \log^3 p.
\]

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 \( R = (\log p)^4 \), where \( A \) is a sufficiently large constant, and \( \lambda > R^2 \); the value of \( \lambda \) 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 \Re s \leq 1, \quad -Y \leq \Im s \leq Y \} \).

Using the estimate
\[
\sum_{p \leq Y} \sum_{\chi} N(\sigma, T, \chi) \ll (Y^2 T)^{2(1-\sigma)/\sigma} (\log YT)^{14}
\]
(here \( \sum_{\chi} \) is the sum over all primitive characters \( \chi \) modulo \( p \)) for \( 4/5 \leq \sigma \leq 1 \) (cf. Montgomery [5], p. 99), and also using our specific choice of \( \varepsilon \), we see that
\[
\sum_{Y < p \leq 2Y} \sum_{\chi \text{ (mod } p)} N(1 - \varepsilon, Y, \chi) \ll (Y^3)^{2\varepsilon/(1-\varepsilon)} (\log Y)^{14}
\ll Y^{C \log \lambda / \log H} (\log Y)^{14}.
\]

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 \( \text{Re } s > 1 - \varepsilon \), with \( \varepsilon \) as chosen in Section 2. Given a prime \( p \) with this property, we obtain an asymptotic formula for the number of prime primitive roots (mod \( p \)) which are less than \( H \).

Notice that if \( d | p - 1 \), then

\[
\frac{1}{d} \sum_{\chi \pmod{p} \atop \text{ord } \chi | d} 1 = \begin{cases} 
1 & \text{if } d | \text{ind } q, \\
0 & \text{otherwise},
\end{cases}
\]

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

\[
\#\{q \leq H : q \text{ is not a primitive root (mod } p)\} \leq \sum_{l|p-1} \frac{1}{l} \sum_{\text{ord } \chi | l} \sum_{q \leq H} \chi(q) = \pi(H) \sum_{l|p-1} \frac{1}{l} + \sum_{l|p-1} \frac{1}{l} \sum_{\chi \text{ } q \leq H} \chi(q).
\]

We break each sum into two parts: (i) \( l \leq \log^2 p \), (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) \[
1 \leq \frac{1}{1 - \omega(p)/p} \leq A_1
\]

for some suitable constant \( A_1 \geq 1 \).

(b) For suitable constants \( \kappa > 0 \) and \( A_2 \geq 1 \),

\[
\sum_{w < p < z} \frac{\omega(p) \log p}{p} \leq \kappa \log \frac{z}{w} + A_2
\]

if \( 2 \leq w \leq z \).

(c) \( |R_d| \leq \omega(d) \) if \( \mu(d) \neq 0 \) and \( \omega(d) \neq 0 \).

Let \( \alpha \) be a real number satisfying \( 0 < \alpha e^{1+\alpha} \leq 1 \), and let \( b \) be a positive integer. Then

\[
S(A; \varphi, z) \leq XW(z) \left\{ 1 + 2 \frac{\alpha^{2b+1} e^{2\alpha}}{1 - \alpha^2 e^{2+2\alpha}} \exp \left( \frac{(2b + 3)c_1}{\alpha \log z} \right) \right\}
+ O(z^{2b+(2.01/(e^{2\alpha/\alpha}-1))})
\]
and

\[
S(A; \wp, z) \geq X W(z) \left\{ 1 - 2 \frac{\alpha^{2b}e^{2\alpha}}{1 - \alpha^{2}e^{2+2\alpha}} \exp \left( \frac{(2b + 2)c_1}{\alpha \log z} \right) \right\}
\]

\[+ O(z^{2b-1 + (2.01/\epsilon^{2n/\alpha} - 1)}) \]

where

\[
c_1 = \frac{A_2}{2} \left\{ 1 + A_1 \left( \kappa + \frac{A_2}{\log 2} \right) \right\}.
\]

Remark 1. The constants implied by the use of the \(O\)-notation do not depend on \(b\) and \(\alpha\).

Remark 2. The replacement of the condition (c) of the theorem by the more general \(|R_d| \leq L \omega(d)\) 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 \(\text{Re} s > 1 - (2 \log \lambda / \log H)\). Let \(A = \{\text{ind } q : q \leq H\}\), \(z = \log^2 p\), and \(\wp = \) the set of all prime divisors \(l\) of \(p - 1\). Then

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

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

Proof. With these choices of \(A\), \(\wp\) and \(z\), it follows that

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

and

\[
W(z) = \prod_{\substack{q|p-1 \\text{\scriptsize such that } q \leq H}} \left( 1 - \frac{1}{q} \right).
\]

We see that

\[
\#\{q \leq H : d|q, \ d|p - 1\} = \frac{1}{d} \sum_{q \leq H} \sum_{\chi \pmod{p} \ \text{ord } \chi | d} \chi(q).
\]

Hence,

\[
|A_d| = \frac{1}{d} \sum_{\chi \pmod{p} \ \text{ord } \chi | d} \sum_{q \leq H} \chi(q) = \frac{1}{d} \pi(H) + \frac{1}{d} \sum_{\chi \neq \chi_0 \ \text{ord } \chi | d} \sum_{q \leq H} \chi(q)
\]

\[
= \frac{1}{d} \pi(H) + \frac{1}{d} \sum_{t|d} \sum_{\chi_t \neq \chi_0} \sum_{q \leq H} \chi_t(q)
\]
where $\chi_t$ runs through characters of order $t$. Therefore,

$$R_d = \frac{1}{d} \sum_{\substack{t \mid d \ \chi_t \sum_{q \leq H} \chi_t(q).}}$$

Using (4), we get

$$|R_d| \ll \frac{1}{d} \sum_{\substack{t \mid d \ \chi_t \sum_{q \leq H} \chi_t(q)}} \ll \left( \frac{1}{d} \sum_{\substack{t \mid d \ \chi_t}} \right) H^{1-\varepsilon} \log^3 p$$

$$\ll \left( \frac{1}{d} \sum_{\phi(t)} \right) H^{1-\varepsilon} \log^3 p = H^{1-\varepsilon} \log^3 p \ll \pi(H)/\lambda.$$

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

(7) $S(A; \varphi, z) \leq \pi(H) W(z) \left\{ 1 + 2 \frac{\alpha^{2b+1} e^{2\alpha}}{1 - \alpha^2 e^{2+2\alpha}} \exp \left( \frac{(2b+3)c_1}{\alpha \log z} \right) \right\}$

$$+ O \left( \frac{\pi(H)}{\lambda} z^{2b+\{2.01/(e^{2\alpha}-1)\}} \right)$$

and

(8) $S(A; \varphi, z) \geq \pi(H) W(z) \left\{ 1 - 2 \frac{\alpha^{2b} e^{2\alpha}}{1 - \alpha^2 e^{2+2\alpha}} \exp \left( \frac{(2b+2)c_1}{\alpha \log z} \right) \right\}$

$$+ O \left( \frac{\pi(H)}{\lambda} z^{2b-1+\{2.01/(e^{2\alpha}-1)\}} \right)$$

with

$$W(z) = \prod_{q \mid p-1} \left( 1 - \frac{1}{q} \right) \prod_{q \mid p} \left( 1 - \frac{1}{q} \right)^{-1}$$

$$= \frac{\phi(p-1)}{p-1} \left( 1 + O \left( \frac{1}{\log p \log_2 p} \right) \right).$$

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

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

whenever $\alpha^2 \gg 1/\log z$. Since $\alpha$ 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 $\lambda$ 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

\[
S(\mathcal{A}; \varphi, z) = \frac{\phi(p - 1)}{p - 1} \pi(H) \left(1 + O\left(\frac{1}{\log p \log_2 p}\right)\right) \left(1 + O\left(\alpha^{B/\alpha}\right)\right)
\]

\[
+ O\left(\frac{\pi(H) z^{B'/\alpha}}{\lambda}\right).
\]

Therefore, we get

\[
S(\mathcal{A}; \varphi, z) = \frac{\phi(p - 1)}{p - 1} \pi(H) \left(1 + O\left(\alpha^{B/\alpha}\right)\right),
\]

which proves the lemma.

We now consider the sum in (ii).

**Lemma 3.2.** Let

\[
L = \sum_{l > \log^2 p} \frac{1}{l} \left(\pi(H) + \sum_{\chi l \leq H} \chi_l(q)\right).
\]

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

**Proof.**

\[
L = \pi(H) \sum_{l > \log^2 p} \frac{1}{l} + \sum_{l > \log^2 p} \frac{1}{l} \sum_{\chi l \leq H} \chi_l(q).
\]

Then

\[
|L| \leq \frac{\pi(H)}{\log p} + \sum_{l > \log^2 p} \frac{1}{l} \sum_{\chi l \leq H} \chi_l(q) \leq \frac{\pi(H)}{\log p} + \frac{\pi(H)}{\lambda},
\]

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 \(p\),

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

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

\[
\ll (\log Y)^{14} \exp\left(\frac{C \log Y \log_3 Y}{\alpha \log H}\right).
\]

This completes the proof of Theorem 1.1. \(\blacksquare\)
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


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)