ON THE LEAST PRIMITIVE ROOT OF A PRIME p

P. ERDÖS

Vinogradoff[1] proved that the least primitive root of a prime p is less than $2^m p^{1/2} \log p$ for sufficiently large p; m denotes the number of different prime factors of $p-1$. Later he improved this to $2^m p^{1/2} \log\log p$.[2] Hua[3] improved this to $2^{m+1}p^{1/2}$. In the present note we are going to prove that the least primitive root is less than $p^{1/2}(\log p)^{17}$ for large p. This result is better than Hua's if $p-1$ has "many" prime factors, but worse if it has "few" prime factors. We shall use Brun's method. It is very likely that the least primitive root is $o(p^\epsilon)$ but I can not even prove that it is less than $cp^{1/2}$.

LEMMA 1. *Let $x<p$, $k \mid p-1$. Denote by $f_k(x)$ the number of kth power residues not exceeding x. Then $f_k(x)=x/k+O(p^{1/2}\log p)$.*

Denote by $\chi_0(a)$, $\chi_1(a)$, $\cdots$, $\chi_{k-1}(a)$ the characters for which $[\chi_i(a)]^k=1$. $\chi_0(a)$ is the principal character. Clearly $\sum_{i=0}^{k-1}[\chi_i(a)]=k$ if a is a kth power residue, and is 0 otherwise. Thus

$$\frac{1}{k}\sum_{i=0}^{k-1}\sum_{a=1}^{x}\chi_i(a) = f_k(x). \tag{1}$$

On the other hand by a well known result of Pólya[4]

$$\left|\sum_{a=1}^{x}\chi_i(a)\right| < p^{1/2}\log p \qquad (i \neq 0). \tag{2}$$

Thus combining (1) and (2) we obtain

$$f_k(x) = x/k + c(p^{1/2}\log p), \qquad |c| \leqq 1, \tag{3}$$

which proves the lemma.

Denote by $F(x)$ the number of primitive roots not exceeding x. We clearly have by the sieve of Eratosthenes $F(x)=\sum_{d\mid p-1}\mu(d)f_d(x)$. Hence clearly

$$F(x) > \left(x - \sum_{q\mid p-1}{}' f_q(x) + \sum_{q_1,q_2\mid p-1,q_1\neq q_2}{}' f_{q_1,q_2}(x) - \cdots\right) - \sum_{q\mid p-1,q>(\log p)^3} f_q(x) = \sum_1 - \sum_2,$$

Received by the editors April 11, 1944, and, in revised form, July 13, 1944.

[1] Landau, *Vorlesungen über Zahlentheorie*, vol. 2, p. 178.

[2] C. R. (Doklady) Acad. Sci. URSS (1936) pp. 7–11.

[3] Bull. Amer. Math. Soc. vol. 48 (1942) pp. 726–730.

[4] Landau, ibid. p. 178.

where the q's are primes and the dashes in $\sum_1$ indicate that the summation is extended over only the $q<(\log p)^3$. By (3)

$$\sum_2 < \sum_{q\mid p-1, q>(\log p)^3} \frac{x}{q} + 2p^{1/2}(\log p)^2 < \frac{4x}{(\log p)^2} \tag{4}$$

for $x>p^{1/2}(\log p)^4$, since the number of different prime factors of $p-1$ is less than $2\log p$.

Now we estimate $\sum_1$. Here we use Brun's method. If we replace $f_k(x)$ by x/k the error we make is less than $p^{1/2}\log p$ by (3). Thus following Brun's[5] reasoning (p. 23, equation 21) we obtain

$$\begin{aligned}\sum_1 &> x\cdot 0.3 \prod_{q\mid p-1, q<(\log p)^3}\left(1-\frac{1}{q}\right) - c_1(\log p)^{15}p^{1/2}\log p \\ &> c_2\frac{x}{\log\log p} - c_1 p^{1/2}(\log p)^{16}.^6\end{aligned} \tag{5}$$

We do not give the details since the argument follows literally from Brun's original argument. We make only the following remark. Put

$$A = x - \sum_{q_1\mid p-1}{}' \left[\frac{x}{q_1}\right] + \sum_{q_1,q_2\mid p-1, q_1\neq q_2}{}' \left[\frac{x}{q_1q_2}\right] - \cdots .$$

Then Brun obtains (p. 23, equation 21)

$$A > x\cdot 0.3 \prod_{q\mid p-1, q<(\log p)^3}\left(1-\frac{1}{q}\right) - c_1(\log p)^{15}.$$

The error term $c_1(\log p)^{15}$ comes from replacing in $(\log p)^{15}$ terms $[x/k]$ by x/k (see p. 22). Our error term $c_1p^{1/2}(\log p)^{16}$ comes from replacing in $(\log p)^{15}$ terms $f_k(x)$ by x/k. Thus we obtain from (4) and (5)

$$F(x) > c_2x/\log\log p - c_1p^{1/2}(\log p)^{16} - 4x/(\log p)^2 > 0$$

for $x>p^{1/2}(\log p)^{17}$, and p sufficiently large, which completes the proof.

PURDUE UNIVERSITY

---

[5] *Le crible d'Eratosthene et la theoreme de Goldbach*, Skrifter utgit av Videnskapsselskapets I. Christiania Matematich Naturvidenskabelig Klasse (1920) No. 3. See in particular p. 23, formula (21), and the preceding pages. The prime p_r in that formula is less than $(\log p)^3$ here.

[6] We have $\prod_{p<y}(1-1/p)>c/\log y$. See, for example, Hardy-Wright, *Theory of numbers*, p. 349.