On the least prime primitive root

Junsoo Ha

Stanford University, Department of Mathematics, 450 Serra Mall, Stanford, 94305 CA, United States

1. Introduction and statement of the result

Linnik’s theorem states that the least prime in an arithmetic progression \( (a, q) = 1 \) is bounded by \( cq^L \) for some constants \( c \) and \( L \). Over the years, the exponent \( L \), also known as Linnik’s Constant, has been constantly reduced by many authors. One of the most significant results is due to Heath-Brown [1], who achieved \( L = 5.5 \) with his careful investigation on the distribution of the zeros of Dirichlet \( L \)-functions, and recently Xylouris [7] improved the result to \( L = 5.18 \). In the special case that the modulus \( q \) is a prime, Meng [5] achieved \( L = 4.5 \).

It is a natural question to ask whether we may find the least prime that belongs to a certain set of residue classes. In particular, finding the least prime primitive root is among those challenging problems. We denote by \( g^*(q) \) the least prime that is a primitive
root \pmod q, where q is either a prime power or twice a prime power. Linnik’s bound remains valid, and thus

$$g^*(p) \ll p^L$$

(1.1)

for Linnik’s Constant \(L\); for example, \(L = 4.5\) in Meng [5] is admissible when \(p\) is a prime.

Estimation of \(g^*(p)\) is studied by Martin [3,4]. Due to the abundance of primitive roots, it is expected that \(g^*(p) \ll (\log p)^C\). Martin [3] proved that this is true for almost all moduli; precisely, he showed

$$g^*(p^e) \ll (\log p)^{C(\epsilon)}$$

(1.2)

holds for all except \(O(Y^\epsilon)\) primes \(p \leq Y\) and all positive integers \(e\).

If we assume Generalized Riemann Hypothesis, Shoup [6] showed that

$$g^*(p) \ll 4r^4(\log 2r)^2(\log p)^2$$

(1.3)

where \(r = \omega(p - 1)\) and \(p\) is a prime. On the other hand, if there is a Siegel zero that is sufficiently close to 1, Martin [4] also proved that

$$g^*(p) \ll p^{3/4+\epsilon}.$$  

(1.4)

A related problem is to find the least almost-prime primitive root. Let \(g_2^*(q)\) be the least \(P_2\) (numbers that have at most two prime factors, counted with multiplicity) primitive root. In this problem, Martin [4] achieved the uniform bound

$$g_2^*(q) \ll p^{1/2+1/873}$$

(1.5)

where \(q = p\) or \(p^2\) and \(p\) is a prime.

However, less is known in the literature on the uniform bound of \(g^*(q)\) other than Linnik’s bound. In this paper, we prove the following.

**Theorem 1.1.** Let \(q = p^e\) or \(2p^e\) where \(p\) is an odd prime and \(e\) is a positive integer and let \(g^*(q)\) be the least prime primitive root \pmod q. Then

$$g^*(q) \ll p^{3.1}.$$  

(1.6)

If we assume further that \(\gcd(p - 1, 3 \cdot 5 \cdot 7) = 1\), we have a slightly better bound.

**Theorem 1.2.** Let \(q = p^e\) or \(2p^e\) and suppose \((p - 1, 3 \cdot 5 \cdot 7) = 1\). Then we have

$$g^*(q) \ll p^{2.8}.$$  

