Journal of Number Theory 170 (2017) 10–16

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the least square-free primitive root modulo p

Stephen D. Cohen [a], Tim Trudgian [b,*,1]

[a] School of Mathematics and Statistics, University of Glasgow, Scotland, United Kingdom

[b] Mathematical Sciences Institute, The Australian National University, ACT 0200, Australia

ARTICLE INFO

Article history:
Received 8 February 2016
Received in revised form 8 June 2016
Accepted 8 June 2016
Available online 2 August 2016
Communicated by David Goss

Keywords:
Character sums
Primitive roots
Square-free integers

ABSTRACT

Let $g^{\square}(p)$ denote the least square-free primitive root modulo p. We show that $g^{\square}(p) < p^{0.96}$ for all p.

1. Introduction

Let $\hat{g}(p)$ denote the least prime primitive root modulo p. By Dirichlet's theorem on primes in arithmetic progressions, it is clear that $\hat{g}(p)$ exists. Nevertheless, it is not known whether $\hat{g}(p) < p$ for all p, or even for all sufficiently large p. The best unconditional result (by Ha [3]) says that $\hat{g}(p) \ll p^{3.1}$. On assuming the Generalised Riemann Hypothesis it is known [7] that $\hat{g}(p) \ll (\log p)^{6+\epsilon}$, and, recently, it was shown in [5] that $\hat{g}(p) < \sqrt{p} - 2$ for all $p > 2791$.

* Corresponding author.
E-mail addresses: Stephen.Cohen@glasgow.ac.uk (S.D. Cohen), timothy.trudgian@anu.edu.au (T. Trudgian).

[1] Supported by Australian Research Council DECRA Grant DE120100173.

http://dx.doi.org/10.1016/j.jnt.2016.06.011
0022-314X/

In this article we consider the broader (and easier) case of square-free primitive roots. An integer n is said to be *square-free* if for all primes $l|n$ we have $l^2 \nmid n$. Let $g^{\square}(p)$ denote the least square-free primitive root modulo p, and let $N^{\square}(p,x)$ denote the number of square-free primitive roots modulo p that do not exceed x. Shapiro [6, p. 355] showed that

$$N^{\square}(p,x) = \frac{\phi(p-1)}{p-1}\left\{\frac{6}{\pi^2}x + O(2^{\omega(p-1)}p^{1/4}(\log p)^{1/2}x^{1/2})\right\}, \tag{1}$$

where $\omega(n)$ is the number of distinct prime factors of n. This shows that $N^{\square}(p,p^{1/2+\epsilon}) > 0$ for any positive ϵ and for all sufficiently large p. Equivalently, this means that $g^{\square}(p) \ll p^{1/2+\epsilon}$.

The error term in (1) has been improved by Liu and Zhang [4, Thm 1.1], who showed

$$N^{\square}(p,x) = \frac{\phi(p-1)}{p-1}\left\{\frac{6}{\pi^2}x + O\left(p^{9/44+\epsilon}x^{1/2+\epsilon}\right)\right\}, \tag{2}$$

whence one has that $g^{\square}(p) \ll p^{9/22+\epsilon}$. Instead of focusing on (2), we seek a version of (1) in order to bound $g^{\square}(p)$ explicitly. We do this in the following theorem.

Theorem 1. *We have $g^{\square}(p) < p^{0.96}$ for all primes p. In particular all primes p possess a square-free primitive root less than p.*

We note that using (1) does not allow one to show that $g^{\square}(p) \ll p^{1/2}$. However, based on computational evidence, the bound in (2) and recent work in [2,5] it seems reasonable to extrapolate, as below.

Conjecture 1. *For all $p > 409$ we have $g^{\square}(p) < \sqrt{p} - 2$.*

The outline of this paper is as follows. In §2 we collect the necessary results to make (1) explicit. In §3 we introduce a sieving inequality. We also carry out some rudimentary computations, which prove Theorem 1. Finally, in §4 we discuss a related problem on square-full primitive roots. Throughout this article we write $n = \square -$ free to indicate that n is a square-free integer.

2. Preliminary results

The following establishes an indicator function on primitive roots.

$$f(n) := \frac{\phi(p-1)}{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\chi\in\Gamma_d}\chi(n) = \begin{cases}1 & \text{if } n \text{ is a primitive root mod } p\\ 0 & \text{otherwise,}\end{cases} \tag{3}$$

where $\sum_{\chi\in\Gamma_d}$ denotes a sum over all Dirichlet characters modulo p of order d. We therefore have