ON THE LEAST PRIMITIVE ROOT EXPRESSIBLE AS A SUM OF TWO SQUARES

Christopher Ambrose[1]
Mathematisches Institut, Georg-August Universität Göttingen, Göttingen, Deutschland
ambrose@uni-math.gwdg.de

Received: 2/11/13, Accepted: 7/18/13, Published: 9/26/13

Abstract

For a positive integer n, a λ-root modulo n is an integer q coprime to n which has maximal order in $(\mathbb{Z}/n\mathbb{Z})^*$. We establish upper bounds for $s^*(n)$, the least λ-root modulo n which is expressible as a sum of two squares, in particular proving that for $\varepsilon > 0$, and n large enough there always exists a λ-root q modulo n in the range $1 \leq q \leq n^{\frac{1}{2}+\varepsilon}$ such that q is a sum of two squares.

1. Introduction and Statement

According to a folklore conjecture, all but finitely many primes p admit a positive *prime* primitive root q modulo p which is smaller than p, a problem that has not been resolved yet. Writing $g^*(p)$ for the least prime primitive root q, Martin [3] showed $g^*(p) \ll (\log p)^{B(\varepsilon)}$ for all but $O(Y^\varepsilon)$ primes $p \leq Y$, and Shoup [6] proved $g^*(p) \ll (\log p)^6$ for all p, conditionally on GRH (his result is stated for primitive roots, but it holds for prime primitive roots, too). Further information on this topic, and related problems is provided in [5].

In this paper we are interested in unconditional results valid for all primes, and therefore weaken the condition that the primitive root be a prime. Instead, as a natural variation, we ask for the smallest primitive root expressible as a sum of two squares. From a sieve-theoretic point of view this may be regarded as half way towards prime primitive roots. As it amounts to no extra effort, we treat the case of arbitrary moduli n. Of course, $(\mathbb{Z}/n\mathbb{Z})^*$ may not have a primitive root in general. Therefore we define a λ-root modulo n to be an integer coprime to n of maximal order in $(\mathbb{Z}/n\mathbb{Z})^*$. We write $s^*(n)$ for the smallest λ-root modulo n expressible as a sum of two squares, and prove the following unconditional result.

[1]The author wants to thank the Volkswagen Foundation for their support and Valentin Blomer for fruitful discussions and comments on earlier versions of this work.

Theorem 1. *For a positive integer n let n_c denote the largest odd cube-free divisor of n. Then, for any $\varepsilon > 0$ we have*

$$s^*(n) \ll_\varepsilon n_c^{\frac{1}{2}+\varepsilon}.$$

The proof of Theorem 1 uses ideas of Martin [4] who treated the case of almost-primitive roots. It is based on a semi-linear lower bound sieve and Burgess' bound for short character sums. The semi-linear sieve is applicable because primes represented by $x^2 + y^2$ have density $1/2$ in the set of all primes. We thus note that, as a generalization of Theorem 1, our method also works if one considers λ-roots represented by any binary quadratic form of class number 1.

The necessary notations and results from sieve theory will be provided in Section 2. In Section 3 we develop a sieve setting appropriate to our problem and note some preliminary results which are needed in the sequel. Finally, in Section 4 we proceed with the proof of Theorem 1.

Throughout this paper, $\mathbb{N}$ shall denote the set of positive integers. For any $n \in \mathbb{N}$ we denote by $\varphi(n)$ the order, and by $\lambda(n)$ the exponent of $(\mathbb{Z}/n\mathbb{Z})^*$. By $\mathrm{rad}(n)$, and $\omega(n)$ we mean the largest squarefree divisor, and the number of distinct prime divisors of n, respectively.

2. The Semi-Linear Sieve

As usual in sieve theory we denote by $\mathcal{A}$ a set of positive integers, and for any $d \in \mathbb{N}$ we let $\mathcal{A}_d := \{a \in \mathcal{A} \mid a \equiv 0 \ (d)\}$. For a set $\mathcal{P}$ of rational primes, and a positive parameter z we let $\mathcal{P}(z)$ be the product of all primes $p \in \mathcal{P}$ smaller than z. The predominant goal in sieve theory consist of estimating the quantity

$$\mathcal{S}(\mathcal{A}, z) := \sharp\{a \in \mathcal{A} \mid (a, \mathcal{P}(z)) = 1\}.$$

To this end one assumes that for any $d \in \mathbb{N}$ one has an asymptotic formula

$$\sharp\,\mathcal{A}_d = g(d)X + r_d \tag{1}$$

for the size of $\mathcal{A}_d$. Here the so called density function $g(d)$ is a multiplicative function, and X is a real parameter which serves as an approximation to the size of $\mathcal{A}$. The remainder terms r_d are intended to be rather small (at least on average over d). In a probabilistic sense one may then expect that X multiplied with

$$V(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} (1 - g(p))$$

yields a good approximation for $\mathcal{S}(\mathcal{A}, z)$. This is indeed true under appropriate assumptions, and we state the following result which is a special case of a beta sieve

of sieve dimension $\kappa = \frac{1}{2}$ (cf. [2, p.207,275]). Since we are merely interested in lower bounds for $\mathcal{S}(\mathcal{A}, z)$ we omit the upper bound version.

Theorem 2. *Assume that the function $g(d)$ in (1) satisfies*

$$\prod_{\substack{w\le p<z\\ p\in\mathcal{P}}} (1-g(p))^{-1} \le \left(\frac{\log z}{\log w}\right)^{\frac{1}{2}} \left(1+\frac{L}{\log w}\right) \tag{2}$$

for all $2 \le w \le z$, with some constant $L \ge 1$. Then, for $s \ge 1$ we have

$$\mathcal{S}(\mathcal{A}, z) \ge XV(z)\left\{f(s) + O\left((\log D)^{-\frac{1}{6}}\right)\right\} + O\left(\sum_{\substack{d\mid\mathcal{P}(z)\\ d<D}} |r_d|\right), \tag{3}$$

where $s = \log D/\log z$, and the first implied constant depends on L. For $1 \le s \le 3$ the function $f(s)$ is given by

$$f(s) = \sqrt{\frac{e^\gamma}{\pi s}} \log\left(1 + 2(s-1) + 2\sqrt{s(s-1)}\right)$$

with γ denoting the Euler-Mascheroni constant.

3. Description of the Method and Preliminary Results

We now translate our problem into an appropriate sieve setting in order to make Theorem 2 applicable. From now on, let n be a fixed positive integer, $x > 0$ a real parameter, and set

$$\mathcal{A} := \{1 \le a < x \mid a \text{ is a } \lambda\text{-root modulo } n,\ a \equiv 1\ (4)\}.$$

Furthermore $\mathcal{P}$ will be the set of primes $p \equiv 3\ (4)$. Then we aim to bound

$$\mathcal{S}(\mathcal{A}, z) := \sharp\{a \in \mathcal{A} \mid (a, \mathcal{P}(z)) = 1\}$$

from below for a suitable choice of the parameters z and x. Indeed, if $\mathcal{S}(\mathcal{A}, z) \ge 1$ for $z > \sqrt{x}$, there exists a λ-root modulo n less than x which is expressible as a sum of two squares, since an odd number in $\mathcal{A}$ must have an even number of prime divisors in $\mathcal{P}$.

Before we can apply Theorem 2 to our problem, it is essential to derive an asymptotic formula for $\sharp\,\mathcal{A}_d$ as in (1). Therefore we let $\gamma(k)$ denote the characteristic function of λ-roots modulo n, i.e. $\gamma(k) = 1$, if k is a λ-root modulo n, and $\gamma(k) = 0$, otherwise. Since $\gamma(k)$ is periodic with period n, and with support inside the set of integers coprime to n, it admits a unique expression as a linear combination of Dirichlet characters modulo n. This linear combination has been determined in Lemma 4 and 5 of [4] which we summarize in the following lemma.

Lemma 3. *Let G be the subgroup of Dirichlet characters modulo n given by*

$$G = \left\{ \chi^{\frac{\lambda(n)}{\mathrm{rad}(\lambda(n))}} \mid \chi \pmod n \right\}.$$

For every prime p dividing $\varphi(n)$, let $m(p)$ denote the number of independent characters of order p in G. For every character χ modulo n let $\sigma(\chi)$ denote its order. Then, for any integer k we have

$$\gamma(k) = \sum_{\chi(n)} c_\chi \chi(k),$$

where the coefficients c_χ are given by

$$c_\chi = \begin{cases} \prod\limits_{p \mid \sigma(\chi)} \left(\frac{-1}{p^{m(p)}} \right) \prod\limits_{\substack{p \mid \varphi(n) \\ p \nmid \sigma(\chi)}} \left(1 - \frac{1}{p^{m(p)}} \right), & \text{if } \chi \in G, \\ 0, & \text{otherwise,} \end{cases}$$

and satisfy the equation

$$\sum_{\chi(n)} |c_\chi| = 2^{\omega(\varphi(n))} c_0,$$

where $c_0 := c_{\chi_0}$, and χ_0 is the principal character modulo n.

The error term in the asymptotic formula for $\sharp\, \mathcal{A}_d$, which we proceed to prove in the subsequent section, involves short sums of consecutive values of characters $\chi \in G$. To this end we state the following result (cf. Lemma 7 in [4]) which yields appropriate estimates for such sums, and is based on a more general result of Burgess (cf. [1]).

Lemma 4. *For every $G \ni \chi \neq \chi_0$, $M, N \geq 1$, and $0 < \eta < 1$ we have*

$$\sum_{M < k \leq M+N} \chi(k) \ll N \left(\frac{n_c^{1/4+\eta}}{N} \right)^\eta.$$

4. Proof of Theorem 1

We begin with the deduction of an asymptotic formula for $\sharp\, \mathcal{A}_d$.

Lemma 5. *For a positive integer $d \leq x$ we have*

$$\sharp\, \mathcal{A}_d = g(d) X + r_d, \tag{4}$$

where $X := \frac{c_0 x \varphi(2n)}{4n}$ with c_0 as in Lemma 3, and $g(d)$ is a multiplicative function given by

$$g(d) = \begin{cases} 0, & \text{if } (d, 2n) > 1, \\ \frac{1}{d}, & \text{otherwise.} \end{cases}$$

For any $0 < \eta \leq 1$, $\varepsilon > 0$, and $D \leq x$ the remainder terms r_d satisfy

$$\sum_{\substack{d|\mathcal{P}(z)\\ d<D}} |r_d| \ll_{\varepsilon,\eta} X n_c^{\varepsilon} \left(\frac{n_c^{1/4+\eta}}{x}\right)^{\eta} D^{\eta}.$$

Proof. If $(d,n) > 1$ or $2 \mid d$ we clearly have $\mathcal{A}_d = \varnothing$. For d odd and $(d,n) = 1$ we deduce by Lemma 3

$$\begin{aligned}
\sharp\mathcal{A}_d &= \sum_{\substack{k\leq x\\ k\equiv 1\ (4)\\ k\equiv 0\ (d)}} \gamma(k)\\
&= \sum_{\substack{k\leq x/d\\ kd\equiv 1\ (4)}} \sum_{\chi\in G} c_\chi \chi(kd)\\
&= c_0\chi_0(d) \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)}} \chi_0(k) + \sum_{\substack{\chi\in G\\ \chi\neq\chi_0}} c_\chi\chi(d) \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)}} \chi(k). \qquad (5)
\end{aligned}$$

By Möbius inversion the first sum in (5) equals

$$\begin{aligned}
\sum_{\substack{k\leq x/d\\ k\equiv d\ (4)\\ (k,n)=1}} 1 &= \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)}} \sum_{\substack{f|k\\ f|n}} \mu(f)\\
&= \sum_{f|n} \mu(f) \sum_{\substack{lf\leq x/d\\ lf\equiv d\ (4)}} 1\\
&= \frac{x}{4d} \sum_{\substack{f|n\\ 2\nmid f}} \frac{\mu(f)}{f} + O\left(2^{\omega(n)}\right)\\
&= \frac{x}{4d}\frac{\varphi(2n)}{n} + O\left(2^{\omega(n)}\right). \qquad (6)
\end{aligned}$$

The second sum in (5) can be estimated using Lemma 3 and 4. If $d_0 \equiv d\ (4)$ with $d_0 \in \{1,3\}$, and m is an integer satisfying $4m \equiv 1\ (n)$, we obtain

$$\begin{aligned}
\sum_{\substack{\chi\in G\\ \chi\neq\chi_0}} c_\chi\chi(d) \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)}} \chi(k) &\ll \sum_{\substack{\chi\in G\\ \chi\neq\chi_0}} |c_\chi| \left|\chi(m) \sum_{0\leq l\leq \frac{x}{4d}-\frac{d_0}{4}} \chi(4l+d_0)\right|\\
&\ll \sum_{\substack{\chi\in G\\ \chi\neq\chi_0}} |c_\chi| \left|\sum_{0\leq l\leq \frac{x}{4d}-\frac{d_0}{4}} \chi(l+md_0)\right|\\
&\ll c_0 2^{\omega(\varphi(n))} \frac{x}{d}\left(\frac{d}{x} n_c^{1/4+\eta}\right)^{\eta}.
\end{aligned}$$

By (5) and (6) the remainder term r_d is therefore

$$\ll c_0 2^{\omega(n)} + c_0 2^{\omega(\varphi(n))} \frac{x}{d} \left(\frac{d}{x} n_c^{1/4+\eta} \right)^{\eta} \ll_{\varepsilon} \frac{1}{d} \frac{c_0 x \varphi(2n)}{4n} n_c^{\varepsilon} \left(\frac{d}{x} n_c^{1/4+\eta} \right)^{\eta},$$

since $d \leq x$ and $\eta \leq 1$. Using the definition of X, we finally deduce

$$\sum_{\substack{d \mid \mathcal{P}(z) \\ d<D}} |r_d| \leq \sum_{d<D} |r_d| \ll_{\varepsilon} X n_c^{\varepsilon} \left(\frac{n_c^{1/4+\eta}}{x} \right)^{\eta} \sum_{d<D} d^{\eta-1} \ll_{\eta} X n_c^{\varepsilon} \left(\frac{n_c^{1/4+\eta}}{x} \right)^{\eta} D^{\eta}.$$

□

Using Theorem 2, and the preceding lemma we may now prove the following modified version of Theorem 1.

Theorem 6. *For a positive integer n, and x a positive real parameter, let $\mathcal{S}(\mathcal{A})$ denote the number of odd λ-roots q modulo n in the range $0 < q < x$, such that q is expressible as a sum of two squares, and set $X := \frac{c_0 x \varphi(2n)}{4n}$. Then, for any $0 < \eta < \frac{1}{2}$ there exists $x_0(\eta) \geq 1$ such that*

$$\mathcal{S}(\mathcal{A}) \gg_{\eta} \frac{X}{\sqrt{\log x}}$$

holds, whenever $x > \max\{x_0(\eta), n_c^{\frac{1}{2}+\frac{5\eta}{1-2\eta}}\}$.

Proof. Inserting the multiplicative function $g(d)$ from Lemma 5 into the definition of $V(z)$ one can easily verify that (2) is satisfied, and $V(z) \sim \frac{c_n}{\sqrt{\log z}}$ holds with some constant $c_n \geq 1$ depending on n (cf. [2, p.277f]). Hence Theorem 2 is applicable. If $z > \sqrt{x}$, we clearly have

$$\begin{aligned} \mathcal{S}(\mathcal{A}) &\geq \mathcal{S}(\mathcal{A}, z) \\ &\gg \frac{X}{\sqrt{\log x}} \left\{ f(s) + O\left((\log D)^{-\frac{1}{6}} \right) \right\} + O_{\eta,\varepsilon} \left(X n_c^{\varepsilon} \left(\frac{n_c^{1/4+\eta}}{x} \right)^{\eta} D^{\eta} \right) \end{aligned}$$

by Theorem 2 and Lemma 5. Now we define $D := \frac{x^{1-\eta}}{n_c^{2\eta+1/4}}$, and set $\varepsilon = \eta^2$. With these choices the above error term becomes $o(X/\sqrt{\log x})$. If we choose x according to the condition

$$x > n_c^{\frac{1}{2}+\frac{5\eta}{1-2\eta}},$$

we obtain $D > x^{1/2}$, and hence $f(s) > 0$. This completes the proof. □

Finally, Theorem 1 is a simple consequence of the previous theorem. Indeed, for any $0 < \eta < \frac{1}{2}$ Theorem 6 implies that $\mathcal{S}(\mathcal{A})$ is positive, whenever

$$x > x_0(\eta) n_c^{\frac{1}{2}+\frac{5\eta}{1-2\eta}}$$

is satisfied. Since $\mathcal{S}(\mathcal{A})$ is a counting function, it must therefore be ≥ 1, and Theorem 1 follows.

References

[1] D. A. Burgess, *On character sums and L-series. II*, Proc. Lond. Math. Soc. (3) **13** (1963), 524–536.

[2] J. Friedlander and H. Iwaniec, *Opera de cribro*, vol. 57 of Amer. Math. Soc. Colloq. Publ., Amer. Math. Soc., Providence, RI, 2010.

[3] G. Martin, *The least prime primitive root and the shifted sieve*, Acta Arith. **80** (1997), 277–288.

[4] G. Martin, *Uniform bounds for the least almost-prime primitive root*, Mathematika **45** (1998), 191–207.

[5] P. Moree, *Artin's primitive root conjecture—a survey*, Integers **12** (2012), 1305–1416.

[6] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. **58** (1992), 369–380.