SMALL PRIME kTH POWER RESIDUES FOR $k = 2, 3, 4$: A RECIPROCITY LAWS APPROACH

KÜBRA BENLİ AND PAUL POLLACK

ABSTRACT. Nagell proved that for each prime $p \equiv 1 \pmod 3$, $p > 7$, there is a prime $q < 2p^{1/2}$ that is a cubic residue modulo p. Here we show that for each fixed $\epsilon > 0$, and each prime $p \equiv 1 \pmod 3$ with $p > p_0(\epsilon)$, the number of prime cubic residues $q < p^{1/2+\epsilon}$ exceeds $p^{\epsilon/30}$. Our argument, like Nagell's, is rooted in the law of cubic reciprocity; somewhat surprisingly, character sum estimates play no role. We use the same method to establish related results about prime quadratic and biquadratic residues. For example, for all large primes p, there are more than $p^{1/9}$ prime quadratic residues $q < p$.

1. Introduction

For each prime p and each integer $k \geq 2$, let $r_k(p)$ denote the smallest prime kth power residue modulo p. Clearly, any prime congruent to 1 modulo p is a kth power residue, and so $r_k(p)$ exists for all pairs k, p. Almost a full century ago, I. M. Vinogradov conjectured that $r_2(p) = O_\epsilon(p^\epsilon)$ for each $\epsilon > 0$ [13], and it is widely believed that the same is true for $r_k(p)$, for every fixed k. (The general conjecture is known under the assumption of the Generalized Riemann Hypothesis; see, e.g., a recent paper of Lamzouri, Li, and Soundararajan [5, Theorem 1.4], who present explicit upper bounds improving earlier estimates of Bach and Sorenson [1].) The jumping-off point for this note is an unconditional upper bound for $r_k(p)$ published by Elliott in 1974 [3].

Theorem A. *Fix an integer $k \geq 2$, and fix $\epsilon > 0$. For all large primes $p \equiv 1 \pmod k$,*

$$r_k(p) < p^{\frac{k-1}{4}+\epsilon}. \tag{1}$$

The restriction to primes $p \equiv 1 \pmod k$ is a natural one, since the set of kth powers modulo p coincides with the set of $\gcd(k, p-1)$th powers.

In nascent form, the method of proof of Theorem A goes back to Linnik and A. I. Vinogradov [12], who showed Theorem A when $k = 2$. The key components are (1) Burgess's character sum bound, and (2) lower bounds on $|L(1, \chi)|$ for nonprincipal Dirichlet characters χ mod p of order dividing k. Note that Theorem A is of interest only for fairly small values of k, as $\frac{k-1}{4}$ eventually exceeds the exponent in known versions of Linnik's theorem.

For odd values of k, Elliott observes (op. cit.) that the proof of Theorem A can be modified to give a slightly sharper upper bound on $r_k(p)$. (The improvement comes from our possessing better lower bounds on $|L(1, \chi)|$ for complex χ vis-à-vis real χ.) As an example, he states that for primes $p \equiv 1 \pmod 3$,

$$r_3(p) \leq cp^{\frac{1}{2}} \exp(c' \sqrt{\log p \cdot \log\log p})$$

for certain constants $c, c' > 0$. It does not seem to be widely known that Nagell published a still sharper upper bound for $r_3(p)$ already in 1952 [7], namely

$$r_3(p) < 2p^{\frac{1}{2}} \qquad \text{once } p > 7. \tag{2}$$

Remarkably, Nagell's proof of (2) is free of any trappings of analysis, relying instead on the algebraic theory of cubic residues developed by Gauss, Jacobi, and Eisenstein.

2010 *Mathematics Subject Classification.* 11A15 (primary), 11N36 (secondary).

This note explores further consequences of Nagell's method for the distribution of prime kth power residues, for $k = 2, 3, 4$.

To set the stage, observe that the $k = 2$ case of Theorem A guarantees at least one prime quadratic residue below $p^{1/4+\epsilon}$. The second author showed in [9] that there are in fact *many* prime quadratic residues below this bound: For any $\epsilon > 0$ and $A > 0$,

$$\#\{\text{primes } q < p^{\frac{1}{4}+\epsilon}\colon q \text{ is a quadratic residue mod } p\} > (\log p)^A \tag{3}$$

for all primes $p > p_0(\epsilon, A)$. Our first theorem is an analogous — but in one sense superior — result for prime cubic residues.

Theorem 1. *Let $\epsilon > 0$. For all primes $p \equiv 1 \pmod 3$, $p > p_0(\epsilon)$, we have that*

$$\#\{\textit{primes } q < p^{\frac{1}{2}+\epsilon} : q \textit{ is a cubic residue mod } p\} > p^{\frac{1}{30}\epsilon}.$$

This surpasses (3) in that the number of power residues produced exceeds a certain power of p, not merely an arbitrary power of $\log p$. By contrast, the analytic method of [9] when applied to this problem gives only a weaker lower bound of

$$p^{c \log\log\log p/\log\log p}$$

for some absolute positive constant c.

Our second theorem concerns biquadratic (i.e., fourth power) residues. For an odd prime q, let $q^* = (-1)^{(q-1)/2} q$, so that $q^* = \pm q$ and $q^* \equiv 1 \pmod 4$.

Theorem 2. *Let $\epsilon > 0$. For all primes $p \equiv 1 \pmod 4$, $p > p_0(\epsilon)$, we have that*

$$\#\{\textit{primes } q < p^{\frac{1}{2}+\epsilon} : q^* \textit{ is a biquadratic residue modulo } p\} > p^{\frac{1}{50}\epsilon}.$$

If $p \equiv 1 \pmod 8$, then -1 is a biquadratic residue modulo p. Consequently, q and q^* are either both biquadratic residues or both biquadratic nonresidues. So in this case, Theorem 2 implies a power-of-p lower bound on the number of prime biquadratic residues $q < p^{1/2+\epsilon}$. In comparison, Theorem A only guarantees a single prime biquadratic residue below the significantly larger value $p^{3/4+\epsilon}$. (However, the bound of Theorem A applies also when $p \equiv 5 \pmod 8$.)

As our last application, we revisit the problem of showing that there are many small prime quadratic residues modulo an odd prime p. In [9], "small" was taken to mean "not much larger than $p^{1/4}$". Here we show that for the more relaxed problem where $p^{1/4}$ is replaced by $p^{1/2}$ we can once again establish a power-of-p lower bound.

Theorem 3. *Suppose that $0 < \epsilon \le \frac{1}{2}$. For all primes $p > p_0(\epsilon)$, we have that*

$$\#\{\textit{primes } q < p^{\frac{1}{2}+\epsilon} : q \textit{ is a quadratic residue modulo } p\} > p^{\frac{1}{25}\epsilon}.$$

As was the case for Theorem 1, the proofs of Theorems 2 and 3 are character-free. It would be interesting to investigate the possibility of obtaining stronger results by injecting character sum estimates into the method.

2. Many small prime cubic residues: Proof of Theorem 1

The following consequence of the law of cubic reciprocity is due to Z.-H. Sun (see [10, (1.6) and Corollary 2.1]). Recall that for each prime $p \equiv 1 \pmod 3$, there are integers L, M, uniquely determined up to sign, with

$$4p = L^2 + 27M^2. \tag{4}$$

Proposition 4. *Let p be a prime with $p \equiv 1 \pmod 3$, and let L, M be integers satisfying $4p = L^2 + 27M^2$. Let q be a prime, $q \ne 2, 3$, or p. Then*

$$q \textit{ is a cubic residue mod } p \iff q \mid L(x^2-1) - M(x^3 - 9x) \quad \textit{for some } x \in \mathbb{Z}.$$

Remark. Taking $x = 0$ and $x = 1$, we deduce from Proposition 4 that if a prime $q \neq 2, 3$ divides LM, then q is a cubic residue modulo p. In fact, the restriction to $q \neq 2, 3$ is unnecessary. (See [6, Chapter 7] or [8, Chapter 2] for details and background.) When $p > 7$, (4) implies that $|LM| > 1$. Now taking any prime q dividing LM produces a cubic residue with $q < 2p^{1/2}$. This was essentially Nagell's proof of (2).

Proof of Theorem 1. Let p be a large prime with $p \equiv 1 \pmod 3$, and write $4p = L^2 + 27M^2$ with $L, M > 0$. Let

$$f_0(x) := L(x^2 - 1) + M(x^3 - 9x) \in \mathbb{Z}[x].$$

As preparation for sieving the values of f_0, we record some observations on the number of roots of f_0 modulo primes q. Modulo $q = 2$, there is always at least one root, since $f_0(1) = -8M$, and there are two roots whenever L is even, since $f_0(0) = -L$. Modulo $q = 3$, the polynomial f_0 has at most two roots, since $3 \nmid f_0(0)$ (for if $3 \mid L$, then $3^2 \mid L^2 + 27M^2 = 4p$). Now suppose that $q > 3$. Since $\gcd(L, M)^2 \mid L^2 + 27M^2 = 4p$, it must be that

$$\gcd(L, M) = 1 \text{ or } 2. \tag{5}$$

Since f_0 has leading coefficient M and constant term $-L$, (5) implies that f_0 does not reduce to the zero polynomial mod q, and so f_0 has at most three roots modulo q. Collecting the results of this paragraph, we see in particular that f_0 has no fixed prime divisor except possibly $q = 2$.

We sidestep the case when f_0 has 2 as a fixed prime divisor by means of the following device. From (5), $2^5 \nmid \gcd(L, 8M)$; hence, we may choose $n_0 \in \{0, 1\}$ with $2^5 \nmid f_0(n_0)$. Let e be the largest integer for which $2^e \mid f_0(n_0)$, so that $e \in \{0, 1, 2, 3, 4\}$. Put

$$f(x) = \frac{1}{2^e} f_0(2^5 x + n_0).$$

Then $f(x) \in \mathbb{Z}[x]$ and all the values of f at integer inputs are odd. Since 2^5 is invertible modulo every odd prime q, the above results concerning f_0 imply that f has at most two roots modulo $q = 3$ and at most three roots modulo each prime $q > 3$.

Now let

$$\mathscr{A} = \{f(n) : n \leq p^{\epsilon/4}\}.$$

(Here and below, n is understood to run only over positive integers.) Since f has no fixed prime divisors and at most three roots modulo every prime $q > 3$, the fundamental lemma of the sieve shows that there is an absolute constant $\eta > 0$ such that

$$\#\{n \leq p^{\epsilon/4}, f(n) \text{ has no prime divisor less than } p^{\eta\epsilon/4}\} \gg_\epsilon p^{\epsilon/4}/(\log p)^3$$

provided only that p is sufficiently large in terms of ϵ. In fact, by the sieve of Diamond–Halberstam–Richert, we can (and will) take $\eta = 1/7$. (The sieve we use is Theorem 9.1 on p. 104 of [2]. The relevant numerological fact is that the sifting limit, β_3, is smaller than 7; see Table 17.1, p. 227.) Put

$$\mathscr{E} = \{n \leq p^{\epsilon/4} : f(n) \text{ has no prime divisor less than } p^{\epsilon/28}\},$$

and let

$$\mathscr{Q} = \{\text{primes } q : q \mid f(n) \text{ for some } n \in \mathscr{E}\},$$

so that

$$\#\mathscr{E} \gg_\epsilon p^{\epsilon/4}/(\log p)^3 \qquad \text{and} \qquad \min \mathscr{Q} \geq p^{\epsilon/28}.$$

It is easy to see that $f(n) > 1$ for all positive integers n. Thus,

$$\sum_{n \in \mathscr{E}} 1 \leq \sum_{n \in \mathscr{E}} \sum_{\substack{q \mid f(n) \\ q \text{ prime}}} 1.$$

Reversing the order of summation and using our lower bound on $\#\mathscr{E}$, we deduce that

$$\sum_{q\in\mathscr{Q}} \sum_{\substack{n\le p^{\epsilon/4}\\ q\mid f(n)}} 1 \gg_\epsilon p^{\epsilon/4}/(\log p)^3 \tag{6}$$

for large p. On the other hand, for each $q\in\mathscr{Q}$, the number of $n\le p^{\epsilon/4}$ for which $q\mid f(n)$ is at most $3p^{\epsilon/4}/q+O(1)$. Thus,

$$\begin{aligned}\sum_{q\in\mathscr{Q}} \sum_{\substack{n\le p^{\epsilon/4}\\ q\mid f(n)}} 1 &\le 3p^{\epsilon/4}\sum_{q\in\mathscr{Q}}\frac{1}{q}+O(\#\mathscr{Q})\\ &\le 3p^{\epsilon/4}\cdot p^{-\epsilon/28}\#\mathscr{Q}+O(\#\mathscr{Q}).\end{aligned}$$

If we suppose that $\#\mathscr{Q}\le p^{\epsilon/29}$, then this contradicts (6) (for large p). Hence,

$$\#\mathscr{Q}>p^{\epsilon/29}.$$

Take any $q\in\mathscr{Q}$ with q not dividing $6LM$. This non-divisibility condition excludes only $O(\log p)$ values of q, and so (for large p) there are still at least $p^{\epsilon/30}$ choices of q. We have that $q\mid f(n)$ for some $n\le p^{\epsilon/4}$, so that if we set $m=2^5n+n_0$, then $q\mid f_0(m)$. Hence,

$$q\mid L((-m)^2-1)-M((-m)^3-9(-m)).$$

By Proposition 4, q is a cube modulo p.

We will be finished if we show that each $q\in\mathscr{Q}$ is smaller than $p^{1/2+\epsilon}$. But this is easy: q divides a nonzero integer of the form $f_0(m)$ where $1\le m\le 2^5p^{\epsilon/4}+1$. For every positive integer m,

$$|f_0(m)|\le\max\{|L|,|M|\}(|m^3-9m|+|m^2-1|)\ll p^{\frac{1}{2}}m^3.$$

Thus, $|f_0(m)|$ and q are both smaller than $p^{1/2+\epsilon}$ (for large p). □

3. Biquadratic residues: Proof of Theorem 2

For the proof of Theorem 2, we replace Proposition 4 with the following corollary to the biquadratic reciprocity law. Recall that each prime $p\equiv 1\pmod 4$ admits a representation $p=L^2+4M^2$, with the integers L,M uniquely determined up to sign.

Proposition 5. *Let p be a prime with $p\equiv 1\pmod 4$, and let L,M be integers satisfying $p=L^2+4M^2$. Let q be an odd prime, $q\ne p$. Then*

q^* is a biquadratic residue mod p $\Longleftrightarrow$

$$q\mid M(x^4-6x^2+1)-2L(x^3-x)\quad\textit{for some } x\in\mathbb{Z}.$$

Proposition 5 is again due to Sun (compare with Theorem 2.2 and Corollary 3.2 of [11]).

Proof of Theorem 2. The proof closely parallels that of Theorem 1. This time, we let L,M be positive integers with $L^2+4M^2=p$, and we put

$$f_0(x)=M(x^4-6x^2+1)+2L(x^3-x)\in\mathbb{Z}[x].$$

If $2\mid M$, then $q=2$ is clearly a fixed prime divisor of f_0. Noting that n^3-n is always a multiple of 3, we see that when $3\mid M$ the prime $q=3$ is also a fixed divisor of f_0. Now suppose that $q\ge 5$. Since $\gcd(L,M)^2\mid L^2+4M^2=p$, it is clear that $\gcd(L,M)=1$. The constant term of f_0 is M while the x^3-coefficient is $2L$; since $q\ge 5$ and $\gcd(L,M)=1$, at least one of M and $2L$ is not a multiple of q. Hence, f_0 does not reduce to the zero polynomial modulo q, and so f_0 has at most four roots modulo q.

As before, fixed prime divisors can be avoided by restricting the the allowed substitutions for x to a suitable arithmetic progression. Let 2^e be the highest power of 2 dividing $f_0(0) = M$ and let $3^{e'}$ be the highest power of 3 dividing M. If $e \geq 3$, then $2^2 \parallel f_0(2) = -7M + 12L$ (since in that case, $2 \nmid L$, and so $2^2 \parallel 12L$). Similarly, if $e' \geq 2$, then $3 \parallel f_0(2)$. Set

$$m = \begin{cases} 0 & \text{if } 2^3 \nmid M, \\ 2 & \text{if } 2^3 \mid M, \end{cases} \quad \text{and} \quad m' = \begin{cases} 0 & \text{if } 3^2 \nmid M, \\ 2 & \text{if } 3^2 \mid M. \end{cases}$$

Let n_0 be a positive integer solution to the simultaneous congruences

$$n_0 \equiv m \pmod{2^3}, \quad n_0 \equiv m' \pmod{3^2}$$

with $n_0 \leq 2^3 \cdot 3^2$. If v, v' are defined by the conditions that $2^v \parallel f_0(n_0)$ and $3^{v'} \parallel f_0(n_0)$, we have $v \in \{0, 1, 2\}$ and $v' \in \{0, 1\}$. Put

$$f(x) = \frac{1}{2^v 3^{v'}} f_0(2^3 3^2 x + n_0).$$

Then $f(x) \in \mathbb{Z}[x]$ and all the values assumed by f are coprime to 6. Since $2^3 3^2$ is invertible modulo every prime $q \geq 5$, our earlier discussion of f_0 implies that f has at most four roots modulo all these q.

Applying the sieve in the same manner as in the proof of Theorem 1 shows that the number of primes q dividing $f(n)$ for some $n \leq p^{\epsilon/5}$ is at least $p^{\epsilon/46}$, for all large p. (We use the entry for β_4 in Table 17.1 of [2] this time, since now f can have up to four roots modulo a prime number q. Note that $\beta_4 < 9.1$, and $5 \cdot 9.1 < 46$.) Arguing as above, but now using Proposition 5 in place of Proposition 4, we see that q^* is a biquadratic residue modulo p for all such q not dividing $2LM$. Since this last condition eliminates only $O(\log p)$ primes, the number of remaining values of q is at least $p^{\epsilon/50}$ (for large p). Finally, it is easy to see that $|f(n)| < p^{1/2+\epsilon}$ for all $n \leq p^{\epsilon/5}$, so that each $q < p^{1/2+\epsilon}$. □

4. Small quadratic residues redux: Proof of Theorem 3

Proof of Theorem 3. Suppose first that $p \equiv 1 \pmod 4$. Let $r = \lfloor \sqrt{p} \rfloor$, and let $f(x) = (x + r)^2 - p$. Then f has no fixed prime divisor, and f has at most two roots modulo every prime. Applying the DHR sieve in a now familiar way, we find that

$$\#\{\text{odd primes } q : q \mid f(n) \text{ for some } n \leq p^{0.95\epsilon}\} > p^{2\epsilon/9}$$

for sufficiently large p. (The relevant sifting limit this time, β_2, is ≈ 4.27, and $0.95/4.27 > 2/9$.) For $n \leq p^{0.95\epsilon}$, the integer $f(n)$ is positive and smaller than $p^{1/2+\epsilon}$; thus, each prime q counted above is smaller than $p^{1/2+\epsilon}$. Moreover, for any of these q, the shape of f makes it obvious that p is a square modulo q. By quadratic reciprocity, q is a square modulo p. This completes the proof of the theorem, in slightly stronger form, when $p \equiv 1 \pmod 4$.

We have to work harder when $p \equiv 3 \pmod 4$. Consider the reduced positive definite binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $p^* = -p$; note that such forms are necessarily primitive. Let $h = h(-p)$ be the corresponding class number. A simple counting argument shows that (at least) one of our h forms has $a \gg h/\log(2h)$. To see this, note that a determines b in $O(d(a))$ ways, since b satisfies $b^2 \equiv -p \pmod a$ and $|b| \leq a$. Moreover, c is determined by a and b via $b^2 - 4ac = -p$. Hence, if A is the largest value of a above, then

$$h \ll \sum_{m \leq A} d(m) \ll A \log 2A;$$

consequently, $A \gg h/\log(2h)$, as claimed.

By Siegel's theorem, we have $h > p^{1/2-\epsilon/3}$ for all large p. Hence, one of the above forms has $a > p^{1/2-\epsilon/2}$. Since $|b| \le a \le c$,

$$ac = \frac{b^2+p}{4} \le \frac{ac+p}{4},$$

so that

$$ac \le \frac{p}{3}.$$

Thus,

$$c \le \frac{p}{3a} < p^{1/2+\epsilon/2}.$$

The rest of the argument follows the usual lines, with $f_0(x) = ax^2+bx+c$. Since $\gcd(a,b,c)=1$, the reduction of f_0 is nonzero modulo every prime q, and so f_0 has at most two roots modulo q. In particular, $q=2$ is the only possible fixed prime divisor. Notice that if $2^2 \mid c = f_0(0)$ and $2^2 \mid 4a+2b+c = f_0(2)$, then $2 \mid b$; since $\gcd(a,b,c)=1$, this forces a to be odd, so that $a+b+c = f_0(1)$ is also odd. So we can choose an $n_0 \in \{0,1,2\}$ for which $2^2 \nmid f_0(n_0)$. Define e by the condition that $2^e \parallel f_0(n_0)$, so that $e=0$ or 1, and let

$$f(x) = \frac{1}{2^e} f_0(2^2x+n_0).$$

Then $f(x) \in \mathbb{Z}[x]$, f assumes only odd values, and f has at most two roots modulo every prime. Application of the sieve shows that

$$\#\{\text{odd primes } q : q \mid f(n) \text{ for some } n \le p^{\epsilon/5}\} > p^{\epsilon/25}$$

for large p. (We use the crude estimate $5 \cdot 4.27 < 25$.) Each of these q divides a nonzero integer $f_0(m)$ for some positive integer $m < p^{0.21\epsilon}$ (say). Thus,

$$q \le |f_0(m)| \le am^2 + |b|m + c \le c(m^2+m+1) \le p^{1/2+0.5\epsilon}\cdot p^{0.43\epsilon} < p^{1/2+\epsilon}.$$

Moreover, since the discriminant of f_0 is p^*, we may conclude that p^* is a square modulo q. By quadratic reciprocity, q is a square modulo p. □

Remark. Our Theorems 1 and 2 are effective in the technical sense; given $\epsilon > 0$, there is no theoretical obstacle to computing the value of $p_0(\epsilon)$. The same is true for Theorem 3 in those cases when $p \equiv 1 \pmod 4$; however, when $p \equiv 3 \pmod 4$, the invocation of Siegel's theorem means that we have no way of estimating the required lower bound on p. It seems interesting to note that for the simpler problem of counting prime quadratic residues smaller than p (the specific case $\epsilon = 1/2$ of Theorem 3), effectivity is easily restored. One simply applies our sieve argument to $f_0(x) = x^2 + x + \frac{1-p^*}{4}$. In this way, one can show that for all primes p larger than an effectively computable absolute constant, there are more than $p^{1/9}$ prime quadratic residues $q < p$. Here 9 could be replaced with any number larger than $2 \cdot 4.27$. (In addition to being effective, the exponent $1/9$ is better — i.e., larger — than the one that comes directly out of the proof of Theorem 3.)

Acknowledgements

Our interest in this area was sparked by a `MathOverflow` posting of "GH from MO" [4]. We thank GH for the inspiration. We also thank the referee for helpful comments.

References

[1] E. Bach and J. Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. **65** (1996), 1717–1735.
[2] H. G. Diamond and H. Halberstam, *A higher-dimensional sieve method*, Cambridge Tracts in Mathematics, vol. 177, Cambridge University Press, Cambridge, 2008.
[3] P. D. T. A. Elliott, *The least prime kth-power residue*, J. London Math. Soc. (2) **3** (1971), 205–210.

[4] GH from MO (`http://mathoverflow.net/users/11919/gh-from-mo`), *Given a prime p how many primes $\ell < p$ of a given quadratic character mod p?*, MathOverflow, URL: `http://mathoverflow.net/q/52393` (version: 2014-09-03).
[5] Y. Lamzouri, X. Li, and K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Math. Comp. **84** (2015), 2391–2412, errata in **86** (2017), 2551–2554.
[6] F. Lemmermeyer, *Reciprocity laws: From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.
[7] T. Nagell, *Sur les restes et les non-restes cubiques*, Ark. Mat. **1** (1952), 579–586.
[8] P. Pollack, *Not always buried deep: A second course in elementary number theory*, American Mathematical Society, Providence, RI, 2009.
[9] ———, *Bounds for the first several prime character nonresidues*, Proc. Amer. Math. Soc. **145** (2017), 2815–2826.
[10] Z.-H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291–335.
[11] ———, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), 361–377.
[12] A. I. Vinogradov and U. V. Linnik, *Hypoelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR **168** (1966), 259–261 (Russian).
[13] I. M. Vinogradov, *On the distribution of quadratic residues and nonresidues*, J. Phys.-Mat. ob-va Permsk Univ. **2** (1919), 1–16 (Russian).

Department of Mathematics, University of Georgia, Athens, GA 30601
E-mail address: `kubra.benli25@uga.edu`
E-mail address: `pollack@uga.edu`