THE LEAST PRIME QUADRATIC NONRESIDUE IN A PRESCRIBED RESIDUE CLASS MOD 4

PAUL POLLACK

Abstract. For all primes $p \geq 5$, there is a prime quadratic nonresidue $q < p$ with $q \equiv 3 \pmod 4$. For all primes $p \geq 13$, there is a prime quadratic nonresidue $q < p$ with $q \equiv 1 \pmod 4$.

1. Introduction

Let p be an odd prime. It is easy to see that there is always a prime in the interval $[2, p-1]$ that is a quadratic nonresidue modulo p. Indeed, since a product of squares is a square, the least quadratic nonresidue modulo p is necessarily prime. Since there is *some* quadratic nonresidue less than p (in fact, there are $\frac{p-1}{2}$ of them), the claim follows. With a bit more work, one can show that whenever $p > 3$ there is an *odd* prime quadratic nonresidue less than p. (This statement, accompanied by a clever elementary proof, appears as Lemma 5.8 in [9].) In this note, we show that both of the coprime residue classes modulo 4 contain quadratic nonresidues smaller than p once $p \geq 13$.

Theorem 1. *For every prime $p \geq 5$, there is a prime quadratic nonresidue $q \equiv 3 \pmod 4$ with $q < p$.*

Theorem 2. *For every prime $p \geq 13$, there is a prime quadratic nonresidue $q \equiv 1 \pmod 4$ with $q < p$.*

In both of these theorems, the lower bound on p is easily seen to be sharp.

These theorems are complementary to those of Gica [6], who proved the analogous results for prime quadratic *residues* (by methods different from those used here). Specifically, if $p \geq 19$, then there is a prime quadratic residue $q < p$ with $q \equiv 3 \pmod 4$, while if $p \geq 41$, then there is a prime quadratic residue $q < p$ with $q \equiv 1 \pmod 4$. Again, the bounds are sharp.

Theorems 1 and 2 are primarily of interest as examples of numerically explicit results; from an asymptotic perspective, sharper results are already available. For $r = 1$ or 3, let $n_r(p)$ denote the least prime quadratic nonresidue modulo p lying in the progression r modulo 4. One can deduce from the machinery of [11] that $n_3(p) \leq p^{\frac{1}{4}+o(1)}$, as $p \to \infty$. The same methods give $n_1(p) \leq p^{\frac{1}{2}+o(1)}$, but in fact Friedlander showed already in 1973 that $n_1(p) \leq p^{\frac{1}{2\sqrt{e}}+o(1)}$ [4].

In view of the results "at infinity" just described, one might guess that the proofs of Theorems 1 and 2 should be entirely routine. This is not so. A major obstacle is that the estimate on $n_3(p)$ quoted above is ineffective; the method of [11] does not allow one to determine, even in principle, an explicit p_0 for which $n_3(p) < p$ once $p > p_0$. As regards $n_1(p)$, the methods of [11] and [4] *are* effective. But the proof of Theorem 2 still presents challenges. For example, the Burgess-type character sum estimates in $\mathbb{Z}[i]$ proved in [4] have not (as far as I know) ever been made numerically explicit. It would not be difficult to use the method of [11], in conjunction with an explicit version of the

2010 *Mathematics Subject Classification.* 11A15 (primary), 11E16, 11L40 (secondary).

Key words and phrases. quadratic nonresidue, genus theory, binary quadratic forms, Pólya–Vinogradov inequality.

classical Burgess bound (e.g., that proved in [13]), to find *some* value of p_0 such that $n_1(p) < p$ for all $p > p_0$. However, p_0 would be large enough that it would be far from routine to check Theorem 2 in the remaining range $[13, p_0]$.

Our approach to these problems is as follows: We avoid character sum analysis altogether in the proof of Theorem 1. Instead, we appeal to classical results on binary quadratic forms (all of which were known already to Gauss). The proof of Theorem 2 goes through character sum estimates, but the Burgess bounds are eschewed in favor of the Pólya–Vinogradov inequality, for which we have explicit versions with remarkably agreeable leading terms.

Notation. The letters p, q, and ℓ are reserved for prime variables unless otherwise noted. It is convenient to adopt the following modified O-notation: $f = \mathcal{O}^*(g)$ indicates that $|f| \le g$ for all values of the arguments under consideration.

2. Proof of Theorem 1

We first dispose of those cases when $p \equiv 3 \pmod 4$. Since $p \ge 5$ is assumed, we in fact have $p \ge 7$, so that $p - 4 \ge 3$. Since $p - 4 \equiv 3 \pmod 4$, there is a prime $q \mid p - 4$ with $q \equiv 3 \pmod 4$. By quadratic reciprocity,

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{4}{q}\right) = -1,$$

and so q is our desired prime.

To prove Theorem 1 when $p \equiv 1 \pmod 4$, we appeal to the reduction theory and genus theory of binary quadratic forms; useful references for this material are the books of Cox [1] and Flath [3]. For primes $p \equiv 1 \pmod 4$, the genus characters associated to the discriminant $-4p$ are the Legendre symbol $\left(\frac{\cdot}{p}\right)$ and χ, the nontrivial Dirichlet character modulo 4. By Gauss's theorem on the existence of genera (cf. Theorem 3.6(ii) on [3, p. 158]), there is a primitive, positive definite binary quadratic form F of discriminant $-4p$ such that for any integer a coprime to $4p$ represented by F,

$$\left(\frac{a}{p}\right) = -1 \quad \text{and} \quad \chi(a) = -1. \tag{1}$$

(For the discriminant $-4p$, there are exactly two genera, and the condition (1) characterizes the forms F in the nonprincipal genus.)

Applying Gauss–Lagrange reduction, we can assume $F(x, y) = Ax^2 + Bxy + Cy^2$, where $|B| \le A \le C$. Since $B^2 - 4AC = -4p$, the integer B is even. Moreover, $A > 1$: Indeed, if $A = 1$, then $B = 0$, and $C = p$, so that F is the "principal form" $X^2 + pY^2$. But F is not in the principal genus! Thus, $A \ge 2$. Now

$$C = \frac{1}{4}\frac{B^2}{A} + \frac{p}{A} \le \frac{1}{4}A + \frac{p}{A}.$$

Since

$$4p = 4AC - B^2 \ge 4A^2 - A^2 = 3A^2,$$

we have that $A \le \sqrt{4p/3}$. The expression $\frac{1}{4}t + \frac{p}{t}$ is decreasing as a function of the real variable t for $t \in [2, \sqrt{4p/3}]$, and we conclude that

$$C \le \left(\frac{1}{4}t + \frac{p}{t}\right)\Big|_{t=2} = \frac{p+1}{2}.$$

As $A \le C$, the same upper bound holds for A. (This upper bound also follows from $A \le \sqrt{4p/3}$.) In particular, neither A nor C is a multiple of p.

Since B is even and $Ax^2 + Bxy + Cy^2$ is primitive, at least one of A or C is odd. Pick an odd integer from $\{A, C\}$, say a. Then a is prime to $4p$, and a is represented by

F. Thus, (1) holds. Since $\chi(a) = -1$, we have $a \equiv 3 \pmod 4$, and so there is a prime $q \mid a$ with $q \equiv 3 \pmod 4$. Then

$$-4p = B^2 - 4ac \equiv B^2 \pmod q,$$

so that

$$1 = \left(\frac{-4p}{q}\right) = \left(\frac{-4}{q}\right)\left(\frac{p}{q}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Hence, $\left(\frac{q}{p}\right) = -1$. Since $q \le a \le \frac{p+1}{2} < p$, the prime q has the properties claimed in Theorem 1.

Remarks.

(i) In the (easier) case $p \equiv 3 \pmod 4$, sharper results have been obtained by Nagell [10]: If $p \equiv 3 \pmod 8$ and $p > 3$, one can find a $q \equiv 3 \pmod 4$ with $\left(\frac{q}{p}\right) = -1$ and $q < 2\sqrt{p} + 1$. When $p \equiv 7 \pmod 8$, one can find such a $q < 2\sqrt{p} - 1$.

(ii) In the case $p \equiv 1 \pmod 4$, our proof shows that there is a nonresidue $q \equiv 3 \pmod 4$ with $q \le \frac{p+1}{2}$. One can do a bit better for large p — while maintaining effectivity! — as follows. Let h be the number of classes of primitive, positive definite forms of discriminant $-4p$, so that each of the two corresponding genera is comprised of $\frac{1}{2}h$ inequivalent forms. By a straightforward counting argument, we can show that each genus contains a reduced form $Ax^2 + Bxy + Cy^2$ with $A \gg h/\log h$: If $Ax^2 + Bxy + Cy^2$ is a reduced form of discriminant $-4p$, then $B^2 \equiv -4p \pmod A$. Given A, the number of B satisfying this congruence with $|B| \le A$ is $O(d(A))$, where $d(\cdot)$ is the number-of-divisors function. Moreover, since $B^2 - 4AC = -4p$, the integers B and A determine C. Thus, the number of possible forms with $A \le T$ is $\ll \sum_{A \le T} d(A) \ll T \log T$. Now taking T as the maximum value of A for all reduced forms in the genus, we deduce that $T \log T \gg \frac{1}{2}h$, so that $T \gg h/\log h$.

Choose a form $G(x, y) = Ax^2 + Bxy + Cy^2$ in the nontrivial genus with $A \gg h/\log h$. Since $|B| \le A \le \sqrt{4p/3}$, we have $AC = (B^2 + 4p)/4 \le 4p/3$, and so

$$A \le C \le \frac{4p}{3A} \ll \frac{p \log h}{h}.$$

Following our proof of Theorem 1 reveals that there is a prime quadratic nonresidue $q \equiv 3 \pmod 4$ with $q \le \max\{A, C\} \ll p \log h/h$. The lower bound $h \gg_\epsilon (\log p)^{1-\epsilon}$ of Goldfeld–Gross–Zagier (see [8, Chapter 23]) thus yields $q \ll_\epsilon p/(\log p)^{1-\frac{1}{2}\epsilon}$, where the implied constant is effectively computable for each $\epsilon > 0$.

3. Proof of Theorem 2

We continue to use χ to denote the nontrivial Dirichlet character modulo 4. Let $r(n) := \sum_{de=n} \chi(d)$, so that $r(n)$ is multiplicative in n and

$$r(n) = \frac{1}{4}\#\{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 = n\}$$

(see [7, Theorem 278, p. 314]). We begin with an estimate for the partial sums of $r(n)$ over odd n.

Lemma 3. *For all real $x \ge 1$,*

$$\sum_{\substack{n \le x \\ n \text{ odd}}} r(n) = \frac{x}{2} \cdot \frac{\pi}{4} + \mathcal{O}^*\left(\frac{7}{4}\sqrt{x} + \frac{5}{4}\right).$$

Proof. Inserting the definition of $r(n)$ and interchanging the order of summation, we find that $\sum_{n\le x,\ n \text{ odd}} r(n) = \sum_{de\le x,\ d,e \text{ odd}} \chi(d)$. Applying Dirichlet's hyperbola method,

$$\sum_{\substack{de\le x\\ d,e \text{ odd}}} \chi(d) = \sum_{\substack{d\le \sqrt{x}\\ d \text{ odd}}} \chi(d) \sum_{\substack{e\le x/d\\ e \text{ odd}}} 1 + \sum_{\substack{e\le \sqrt{x}\\ e \text{ odd}}} \sum_{\substack{d\le x/e\\ d \text{ odd}}} \chi(d) - \sum_{\substack{d,e\le \sqrt{x}\\ d,e \text{ odd}}} \chi(d)$$
$$= \sum\nolimits_1 + \sum\nolimits_2 - \sum\nolimits_3,$$

say. Since χ is supported on odd integers, and since the partial sums of $\chi(\cdot)$ are all 0 or 1,

$$\left|\sum\nolimits_2\right| \le \sum_{\substack{e\le \sqrt{x}\\ e \text{ odd}}} 1 \le \frac{1+\sqrt{x}}{2}; \tag{2}$$

similarly,

$$\left|\sum\nolimits_3\right| = \left|\sum_{\substack{d\le \sqrt{x}\\ d \text{ odd}}} \chi(d)\right| \cdot \left|\sum_{\substack{e\le \sqrt{x}\\ e \text{ odd}}} 1\right| \le \frac{1+\sqrt{x}}{2}. \tag{3}$$

We turn now to $\sum_1$. Noting that the number of odd natural numbers not exceeding t, for real $t \ge 1$, is $t/2 + \mathcal{O}^*(1/2)$, we have that

$$\sum\nolimits_1 = \sum_{\substack{d\le \sqrt{x}\\ d \text{ odd}}} \chi(d) \sum_{\substack{e\le x/d\\ e \text{ odd}}} 1 = \sum_{\substack{d\le \sqrt{x}\\ d \text{ odd}}} \chi(d) \left(\frac{x}{2d} + \mathcal{O}^*\left(\frac{1}{2}\right)\right)$$
$$= \frac{x}{2} \sum_{d\le \sqrt{x}} \frac{\chi(d)}{d} + \mathcal{O}^*\left(\frac{1+\sqrt{x}}{4}\right).$$

Since $\sum_{d\ge 1} \chi(d)/d = \pi/4$, we also have that

$$\sum_{d\le \sqrt{x}} \frac{\chi(d)}{d} = \frac{\pi}{4} - \sum_{d>\sqrt{x}} \frac{\chi(d)}{d} = \frac{\pi}{4} + \mathcal{O}^*\left(\frac{1}{\sqrt{x}}\right),$$

using in the last step that the nonzero terms $\chi(d)/d$ are alternating in sign and decreasing in absolute value. Substituting this estimate above reveals that

$$\sum\nolimits_1 = \frac{x}{2}\cdot\frac{\pi}{4} + \mathcal{O}^*\left(\frac{1+3\sqrt{x}}{4}\right). \tag{4}$$

Combining (2), (3), and (4) yields the lemma. □

Remark. As pointed out by the referee, the $\mathcal{O}^*$ term could be improved to $\frac{5}{4}\sqrt{x} + \frac{3}{4}$ by taking account of the fact that $\sum_2$ and $\sum_3$ are nonnegative.

Motivated by Lemma 3, we let

$$\mathrm{RSUM}^+(x) = \frac{x}{2}\cdot\frac{\pi}{4} + \frac{7}{4}\sqrt{x} + \frac{5}{4}, \quad \text{and} \quad \mathrm{RSUM}^-(x) = \frac{x}{2}\cdot\frac{\pi}{4} - \frac{7}{4}\sqrt{x} - \frac{5}{4}.$$

To proceed, we also require an estimate for the partial sums of $r(n)$ when weighted by the Legendre symbol $\left(\frac{n}{p}\right)$. We derive a suitable bound from the following explicit version of the Pólya–Vinogradov inequality due to Frolenkov and Soundararajan (see [5, Theorem 2]).

Proposition 4. *Let χ be a primitive Dirichlet character modulo m, where $m \ge 1200$. For all $M \in \mathbb{Z}$ and $N \in \mathbb{Z}^+$,*

$$\left|\sum_{n=M+1}^{M+N} \chi(n)\right| \le \mathrm{PV}(m),$$

where

$$\mathrm{PV}(m) := \frac{2}{\pi^2}\sqrt{m}\log m + \sqrt{m}.$$

In fact, when $\chi(-1) = -1$, one can replace $\frac{2}{\pi^2}$ by the smaller constant $\frac{1}{2\pi}$. We will not need this, however.

It is useful to observe that the estimate of Proposition 4 continues to hold with the sum on n restricted to odd values. When m is even, this claim is trivial, since in that case χ is supported on odd n. If m is odd, write "$\frac{1}{2}$" for an inverse of 2 modulo m, and note that $\chi(2j+1) = \chi(2)\chi(j+\frac{1}{2})$; thus, a sum over odd n has the same absolute value as an unrestricted sum on j taken over a different interval. Since the bound of Proposition 4 applies to sums over arbitrary intervals $[M+1, M+N]$, our assertion follows.

Lemma 5. *Let p be an odd prime, and let $M \geq 1$. Then*

$$\left|\sum_{\substack{n\leq pM\\ n\ odd}} \left(\frac{n}{p}\right) r(n)\right| \leq \mathrm{WRSUM}^+(p, M),$$

where

$$\mathrm{WRSUM}^+(p, M) := \frac{1+\sqrt{pM}}{2}\left(\mathrm{PV}(p) + \mathrm{PV}(4p)\right) + \mathrm{PV}(p)\cdot\mathrm{PV}(4p).$$

Proof. Inserting the definition of $r(n)$ and interchanging the order of summation, we find that $\sum_{n\leq pM,\ n \text{ odd}} \left(\frac{n}{p}\right) r(n) = \sum_{de\leq pM,\ d,e \text{ odd}} \left(\left(\frac{d}{p}\right)\chi(d)\cdot\left(\frac{e}{p}\right)\right)$. By the hyperbola method,

$$\sum_{\substack{de\leq pM\\ d,e \text{ odd}}} \left(\left(\frac{d}{p}\right)\chi(d)\cdot\left(\frac{e}{p}\right)\right) = \sum\nolimits_1 + \sum\nolimits_2 - \sum\nolimits_3,$$

where now

$$\begin{aligned}
\sum\nolimits_1 &= \sum_{\substack{d\leq\sqrt{pM}\\ d \text{ odd}}} \left(\frac{d}{p}\right)\chi(d) \sum_{\substack{e\leq pM/d\\ e \text{ odd}}} \left(\frac{e}{p}\right),\\
\sum\nolimits_2 &= \sum_{\substack{e\leq\sqrt{pM}\\ e \text{ odd}}} \left(\frac{e}{p}\right) \sum_{\substack{d\leq pM/e\\ d \text{ odd}}} \left(\frac{d}{p}\right)\chi(d),\\
\sum\nolimits_3 &= \sum_{\substack{d,e\leq\sqrt{pM}\\ d,e \text{ odd}}} \left(\frac{d}{p}\right)\chi(d)\cdot\left(\frac{e}{p}\right).
\end{aligned}$$

Now $\left(\frac{\cdot}{p}\right)$ is a primitive character of conductor p while $\left(\frac{\cdot}{p}\right)\cdot\chi(\cdot)$ is a primitive character of conductor $4p$. Applying Proposition 4 to the inner sums in $\sum_1$ and $\sum_2$ yields

$$\left|\sum\nolimits_1\right| \leq \frac{1+\sqrt{pM}}{2}\cdot\mathrm{PV}(p), \quad \text{and} \quad \left|\sum\nolimits_2\right| \leq \frac{1+\sqrt{pM}}{2}\cdot\mathrm{PV}(4p).$$

Writing $\sum_3$ as a product of two sums, we see that $|\sum_3| \leq \mathrm{PV}(p)\cdot\mathrm{PV}(4p)$. The lemma follows from combining these estimates for $\sum_1, \sum_2$, and $\sum_3$. □

We now prove Theorem 2.

Proof. A straightforward computation with `PARI/GP` shows that for every prime p with $13 \leq p < 3\cdot 10^{11}$, there is a prime $q \equiv 1 \pmod 4$ with $q < p$ and $\left(\frac{q}{p}\right) = -1$. (The

computation took roughly 6 hours running under `gp2c` on a Core i5-6200u machine.) So it is enough to prove the theorem under the assumption that $p \geq 3 \cdot 10^{11}$. We take

$$M := 60 \cdot (\log p)^2.$$

Using our lower bound on p, we find that

$$\mathrm{RSUM}^-(pM) \geq 7.8 \cdot \mathrm{WRSUM}^+(p, M).$$

(We used `Mathematica` to compute the minimum of $\mathrm{RSUM}^-(pM)/\mathrm{WRSUM}^+(p,M)$ for $p \geq 3 \cdot 10^{11}$.) So by Lemmas 3 and 5,

$$\left| \sum_{\substack{n \leq pM \\ n \text{ odd}}} \left(\frac{n}{p}\right) r(n) \right| \leq \frac{1}{7.8} \sum_{\substack{n \leq pM \\ n \text{ odd}}} r(n).$$

Hence,

$$\sum_{\substack{n \leq pM \\ n \text{ odd}}} r(n) \left(1 - \left(\frac{n}{p}\right)\right) \geq \frac{6.8}{7.8} \sum_{\substack{n \leq pM \\ n \text{ odd}}} r(n).$$

Considering the possibilities for $\left(\frac{n}{p}\right)$, we deduce that

$$\sum_{\substack{n \leq pM, \ \left(\frac{n}{p}\right) = -1 \\ n \text{ odd}}} r(n) \geq \frac{3.4}{7.8} \sum_{\substack{n \leq pM \\ n \text{ odd}}} r(n) - \frac{1}{2} \sum_{\substack{n \leq pM, \ p \mid n \\ n \text{ odd}}} r(n). \tag{5}$$

The sum being subtracted on the right-hand side of (5) is quite small. Indeed, since $pM < p^2$ for the values of p under consideration,

$$\sum_{\substack{n \leq pM, \ p \mid n \\ n \text{ odd}}} r(n) = r(p) \sum_{\substack{m \leq M \\ m \text{ odd}}} r(m) \leq 2 \cdot \mathrm{RSUM}^+(M).$$

(We used here that $r(p) = 0$ or 2.) In our range of p,

$$\mathrm{RSUM}^+(M) \leq \frac{1}{10000} \mathrm{RSUM}^-(pM).$$

(Indeed, this holds already for $p \geq 2 \cdot 10^4$.) Referring back to (5), and noting that $3.4/7.8 - 1/10000 > 0.4357$, we find that

$$\sum_{\substack{n \leq pM, \ \left(\frac{n}{p}\right) = -1 \\ n \text{ odd}}} r(n) \geq 0.4357 \sum_{\substack{n \leq pM \\ n \text{ odd}}} r(n). \tag{6}$$

To finish things off, we suppose for a contradiction that $\left(\frac{q}{p}\right) = 1$ for all primes $q < p$ with $q \equiv 1 \pmod 4$. Under this assumption, if $r(n) > 0$ for an odd number $n \leq pM$ with $\left(\frac{n}{p}\right) = -1$, then n must be divisible by some prime $q \equiv 1 \pmod 4$ with $q > p$. Moreover, writing $n = qk$, we have $r(n) = 2r(k)$. Therefore,

$$\begin{aligned} \sum_{\substack{n \leq pM, \ \left(\frac{n}{p}\right) = -1 \\ n \text{ odd}}} r(n) &\leq \sum_{\substack{p < q \leq pM \\ q \equiv 1 \pmod 4}} \sum_{\substack{n \leq pM, \ n \text{ odd} \\ q \mid n}} r(n) \\ &= 2 \sum_{\substack{p < q \leq pM \\ q \equiv 1 \pmod 4}} \sum_{\substack{k \leq pM/q \\ k \text{ odd}}} r(k). \end{aligned} \tag{7}$$

We claim that for every real $t \geq 6$,

$$\sum_{\substack{k \leq t \\ k \text{ odd}}} r(k) \leq \frac{1}{2} t.$$

It clearly suffices to verify this for integers t. For $t \geq 300$, it follows from Lemma 3, since $\mathrm{RSUM}^+(t)/t \leq 1/2$ in that range; for $6 \leq t < 300$, it is verified directly with a short computer program. Using this estimate to bound the inner sum in (7),

$$\sum_{\substack{n \leq pM,\ \left(\frac{n}{p}\right)=-1 \\ n \text{ odd}}} r(n) \leq 2 \left(\sum_{\substack{pM/5 < q \leq pM \\ q \equiv 1 \pmod 4}} 1 + \sum_{\substack{pM/6 < q \leq pM/5 \\ q \equiv 1 \pmod 4}} 3 + \frac{1}{2} pM \sum_{\substack{p < q \leq pM/6 \\ q \equiv 1 \pmod 4}} \frac{1}{q} \right).$$

To bound the sums on q, we use that for $\epsilon := 1/400$ and all $t \geq 10^{10}$,

$$\sum_{\substack{q \leq t \\ q \equiv 1 \pmod 4}} \log q = \frac{1}{2} t (1 + \mathcal{O}^*(\epsilon));$$

this is a result of Ramaré and Rumely [12] (see the entry for $k = 4, x_0 = 10^{10}$ in their Table 1). Thus,

$$\begin{aligned} \sum_{\substack{pM/5 < q \leq pM \\ q \equiv 1 \pmod 4}} 1 &\leq \frac{1}{\log(pM/5)} \sum_{\substack{pM/5 < q \leq pM \\ q \equiv 1 \pmod 4}} \log q \\ &\leq \frac{\frac{1}{2} pM(1+\epsilon) - \frac{1}{2}(pM/5)(1-\epsilon)}{\log(pM/5)} = \left(1 + \frac{3}{2}\epsilon\right) \frac{2pM/5}{\log(pM/5)}. \end{aligned}$$

Similarly,

$$\begin{aligned} \sum_{\substack{pM/6 < q \leq pM/5 \\ q \equiv 1 \pmod 4}} 1 &\leq \frac{1}{\log(pM/6)} \sum_{\substack{pM/6 < q \leq pM/5 \\ q \equiv 1 \pmod 4}} \log q \\ &\leq \frac{\frac{1}{2}(pM/5)(1+\epsilon) - \frac{1}{2}(pM/6)(1-\epsilon)}{\log(pM/6)} = (1 + 11\epsilon) \frac{pM/60}{\log(pM/6)}. \end{aligned}$$

Moreover,

$$\begin{aligned} \sum_{\substack{p < q \leq pM/6 \\ q \equiv 1 \pmod 4}} \frac{1}{q} &= \int_p^{pM/6} \frac{1}{t \log t} \, \mathrm{d}\left(\sum_{\substack{q \leq t \\ q \equiv 1 \pmod 4}} \log q \right) \\ &= \left(\frac{1}{t \log t} \sum_{\substack{q \leq t \\ q \equiv 1 \pmod 4}} 1 \right) \Bigg|_p^{pM/6} - \int_p^{pM/6} \left(\sum_{\substack{q \leq t \\ q \equiv 1 \pmod 4}} \log q \right) \mathrm{d}\left(\frac{1}{t \log t} \right); \end{aligned}$$

this is at most

$$\frac{1}{2}(1+\epsilon) \cdot \frac{1}{\log(pM/6)} - \frac{1}{2}(1-\epsilon) \cdot \frac{1}{\log p} + \frac{1}{2}(1+\epsilon) \int_p^{pM/6} \left(\frac{1}{t \log t} + \frac{1}{t \log(t)^2} \right) \mathrm{d}t,$$

which in turn equals

$$\begin{aligned} &\frac{1}{2}(1+\epsilon) \cdot \frac{1}{\log(pM/6)} - \frac{1}{2}(1-\epsilon) \cdot \frac{1}{\log p} \\ &\qquad + \frac{1}{2}(1+\epsilon) \cdot \left(\log\log(pM/6) - \log\log(p) + \frac{1}{\log p} - \frac{1}{\log(pM/6)} \right). \end{aligned}$$

Putting these estimates together, we see that

$$\sum_{\substack{n \leq pM,\ \left(\frac{n}{p}\right)=-1 \\ n \text{ odd}}} r(n) \leq 2 \cdot S(p), \tag{8}$$

where

$$S(p) := \left(1+\frac{3}{2}\epsilon\right)\cdot\frac{2pM/5}{\log(pM/5)} + (1+11\epsilon)\cdot\frac{pM/20}{\log(pM/6)} + \frac{1}{2}(1+\epsilon)\frac{pM/2}{\log(pM/6)} - \frac{1}{2}(1-\epsilon)\frac{pM/2}{\log p} + \frac{1}{4}pM(1+\epsilon)\cdot\left(\log\log(pM/6) - \log\log(p) + \frac{1}{\log p} - \frac{1}{\log(pM/6)}\right).$$

Comparing (8) and (6), we see that

$$S(p) \geq 0.21785\cdot \mathrm{RSUM}^-(pM). \tag{9}$$

Again using `Mathematica`, we see this inequality fails for $p \geq 3\cdot 10^{11}$. □

Remark for the skeptical. All of the inequalities asserted above can be verified with a finite number of high-precision calculations. In particular, there is no need to trust the output of `Mathematica`'s `Minimize` or `NMinimize` functions. The details are not particularly inspiring, so we discuss how this goes only for the key inequality (9) (meaning that we explain how to rigorously refute (9)). Simplifying,

$$\frac{S(p)}{pM} = \left(1+\frac{3}{2}\epsilon\right)\frac{2/5}{\log(pM/5)} + (1+11\epsilon)\frac{1/20}{\log(pM/6)} + \epsilon\frac{1/2}{\log p} + \frac{1}{4}(1+\epsilon)\log\left(1+\frac{\log(M/6)}{\log p}\right).$$

In our range of p, all four summands are easily checked to be decreasing as functions of the real variable p, so that $S(p)/pM$ is decreasing. On the other hand,

$$\frac{\mathrm{RSUM}^-(pM)}{pM} = \frac{1}{2}\cdot\frac{\pi}{4} - \frac{7}{4\sqrt{pM}} - \frac{5}{4pM},$$

which is positive and increasing in our range of p. Thus,

$$\frac{S(p)}{\mathrm{RSUM}^-(pM)} = \frac{S(p)}{pM}\cdot\frac{pM}{\mathrm{RSUM}^-(pM)}$$

is a product of positive, decreasing functions, so is decreasing. At $p = 3\cdot 10^{11}$,

$$\frac{S(p)}{\mathrm{RSUM}^-(pM)} < 0.2171.$$

It follows that (9) fails for all $p \geq 3\cdot 10^{11}$.

4. Concluding thoughts: Do we need character sums?

It is natural to wonder if the intricate analysis above is necessary to prove Theorem 2, especially as certain special cases of that theorem do admit algebraic treatments. For example, let $p \equiv 7 \pmod 8$. From work of Dickson [2], we can write $p = x^2+y^2+2z^2$ for some $x, y, z \in \mathbb{Z}$. (In fact, Dickson shows that $x^2+y^2+2z^2$ represents all integers not of the form $4^k(16m+14)$.) Since a sum of two squares cannot be 7 mod 8, it must be that z is odd, so that

$$x^2+y^2 = p-2z^2 \equiv 5 \pmod 8.$$

Any primes that appear to an odd power in an odd sum of two squares are 1 mod 4, and so are 1 or 5 mod 8. Since $x^2+y^2 \equiv 5 \pmod 8$, it follows that there is some prime $q \equiv 5 \pmod 8$ that divides x^2+y^2. Then

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{2z^2}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{z^2}{q}\right) = -\left(\frac{z}{q}\right)^2 = 0 \text{ or } -1.$$

But $q \leq p - 2z^2 < p$, so $\left(\frac{q}{p}\right) \neq 0$, and hence $\left(\frac{q}{p}\right) = -1$. So q is our desired prime. (Compare with the proof of [6, Theorem 1].) This argument can be extended somewhat, but the author has not so far succeeded in establishing all of Theorem 2 this way.

Acknowledgments

Research of the author is supported by NSF award DMS-1402268. He thanks David Jensen for suggesting the problem and Enrique Treviño for useful conversations. He also thanks the referee for a careful reading of the manuscript.

References

[1] D. A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013.
[2] L. E. Dickson, *Integers represented by positive ternary quadratic forms*, Bull. Amer. Math. Soc. **33** (1927), 63–70.
[3] D. E. Flath, *Introduction to number theory*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.
[4] J. B. Friedlander, *On characters and polynomials*, Acta Arith. **25** (1973/74), 31–37.
[5] D. A. Frolenkov and K. Soundararajan, *A generalization of the Pólya-Vinogradov inequality*, Ramanujan J. **31** (2013), 271–279.
[6] A. Gica, *Quadratic residues of certain types*, Rocky Mountain J. Math. **36** (2006), 1867–1871.
[7] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008.
[8] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.
[9] M. Köcher, *Elementare Abschätzungen für prime quadratische Reste und Nichtreste*, Ph.D. thesis, Universität Tübingen, 2002, available online at `https://publikationen.uni-tuebingen.de/xmlui/handle/10900/48414`.
[10] T. Nagell, *Sur les restes et les non-restes quadratiques suivant un module premier*, Ark. Mat. **1** (1950), 185–193.
[11] P. Pollack, *Prime splitting in abelian number fields and linear combinations of Dirichlet characters*, Int. J. Number Theory **10** (2014), 885–903.
[12] O. Ramaré and R. Rumely, *Primes in arithmetic progressions*, Math. Comp. **65** (1996), no. 213, 397–425.
[13] E. Treviño, *The Burgess inequality and the least kth power non-residue*, Int. J. Number Theory **11** (2015), 1653–1678.

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