On Burgess' estimate, quadratic residues and non-residues

Weite Pi
Student number: 1006626974

1 Introduction and early results.

Various problems have been proposed regarding quadratic residues and non-residues modulo an odd prime p. To start with, I shall consider two of them, namely:

(1) The bound for the least quadratic non-residue $(\mathrm{mod}\, p)$;

(2) The bound for the maximum number of consecutive quadratic residues or non-residues $(\mathrm{mod}\, p)$.

Let p be an odd prime and denote by $n_1(p)$ the least quadratic non-residue $(\mathrm{mod}\, p)$. It was conjectured by Vinogradov that $n_1(p) = O(p^{\varepsilon})$ for every $\varepsilon > 0$. This is reasonable, since there are half quadratic residues and half non-residues $(\mathrm{mod}\, p)$ in $[1, p-1]$. In 1918, Pólya **[1]** and Vinogradov **[2]** independently proved that

$$\left| \sum_{n=N+1}^{N+H} \left(\frac{n}{p}\right) \right| < p^{\frac{1}{2}} \log p,$$

where $(\frac{\cdot}{p})$ is the Legendre symbol. This is the Pólya-Vinogradov inequality. Because of the fundamental importance of this result, we sketch a proof using Fourier transform and the Gaussian sum below:

Proof (sketch). Let $\chi(n) := (\frac{n}{p})$ for some prime p, and define the Gaussian sum $G(n,\chi) := \sum_{k=0}^{p-1} \chi(k) e^{\frac{2\pi i k n}{p}}$ for $n \in \mathbb{Z}$. We can write $\chi(n)$ as a Fourier series

$$\chi(n) = \sum_{k=0}^{p-1} \widehat{\chi}(k) e^{\frac{2\pi i k n}{p}},$$

where the Fourier coefficients are defined by

$$\widehat{\chi}(k) := \frac{1}{p} \sum_{n=0}^{p-1} \chi(n) e^{\frac{-2\pi i k n}{p}} = \frac{1}{p} G(-k, \chi).$$

One can prove that $G(n,\chi) = \overline{\chi}(n) \cdot G(1,\chi)$ for any Dirichlet character χ and $n \in \mathbb{Z}$ (this requires some work if $\gcd(n,p) > 1$). Thus one obtains $\chi(n) = \frac{G(1,\chi)}{p} \sum_{k=0}^{p-1} \overline{\chi}(-k) e^{\frac{2\pi i k n}{p}}$, and that

$$\sum_{n=1}^{H} \chi(n) = \frac{G(1,\chi)}{p} \sum_{k=1}^{p-1} \overline{\chi}(-k) \sum_{n=1}^{H} e^{\frac{2\pi i k n}{p}}.$$

It can be shown in this case that $|G(1,\chi)| = \sqrt{p}$ (this again requires some work), and that for $1 \le k \le \frac{p}{2}$ one has $|\sum_{n=1}^{H} e^{\frac{2\pi i k n}{p}}| \le \frac{p}{2k}$, by the convexity of the sine function in $(0, \frac{\pi}{2})$. Let $f(k) = \sum_{n=1}^{H} e^{\frac{2\pi i k n}{p}}$, one

then has

$$\left|\sum_{n=1}^{H}\chi(n)\right| \le \frac{|G(1,\chi)|}{p}\cdot 2\sum_{1\le k\le p/2}|f(k)| \le \frac{|G(1,\chi)|}{p}\cdot 2\sum_{1\le k\le p/2}\frac{p}{2k} < \sqrt{p}\log p.$$

This argument still holds if we shift n by N, and the result follows. □

Combining this with a counting argument (we shall show this trick later) which exploits the complete multiplicativity property of the Legendre symbol and uses the asymptotic formula for the sum of reciprocals of primes, Vinogradov showed that

$$n_1(p) = O(p^{\frac{1}{2\sqrt{e}}}(\log p)^2).$$

It is worth noting that Vinogradov gave another proof of this result in **[3]** and **[4]**, after a general theorem concerning the distribution of residues and non-residues of higher powers. This theorem is elementary but hardly simple; the key idea is to utilize the average property of fractional parts and the least positive residues $(\mathrm{mod}\, p)$ in an arithmetic progression. The proof used two different ways to calculate the number of numbers of certain forms that, in a sense, described higher power residues. Using this result, he obtained the following

Theorem 1.1 If p is a prime and n a divisor of $p-1$ distinct from 1, the least non-residue of n-th powers modulo p is less than $p^{1/2k}(\log p)^2$ for all sufficiently large p, where $k = e^{\frac{n-1}{n}}$.

Davenport and Erdős showed in **[5]** the following elementary

Lemma 1.2 Let $\chi(n)$ be a non-principle character modulo p, and h an integer with $0 < h < p$. Then

$$\sum_{x}\left|\sum_{n=1}^{h}\chi(x+n)\right|^2 = ph - h^2,$$

where the outer sum is over a complete set of residues $(\mathrm{mod}\, p)$.

Using this identity, they obtained a minor improvement of Vinogradov's result on $n_1(p)$, namely, that $n_1(p) = O((p^{\frac{1}{2}}\log p)^{\frac{1}{\sqrt{e}}})$. This identity also leads to an estimate on the bound for the maximum number of consecutive quadratic residues or non-residues. Denote by M this maximum number; let $h = \left[\frac{1}{2}M\right]$ in the lemma, one then obtains

$$M = O(p^{\frac{1}{2}}).$$

In the same paper, Davenport and Erdős also gave an estimate on $\sum_x |S_h(x)|^{2r}$ for $0 < h < p$, where

$$S_h(x) = \sum_{n=1}^{h}\left(\frac{x+n}{p}\right),$$

and the sum is over a complete set of residues $(\mathrm{mod}\, p)$. The idea is to expand and divide the sum into two parts, using combinatorial method to estimate the major contribution, and invoke an asyptomtic

formula for the other. This estimate played an important role in the following result by Burgess. It also leads to a theorem saying that the distribution of the sum $S_h(x)$ for large p is *normal*, provided h is taken to be a function of p satisfying appropriate conditions; see *Theorem 5* of **[5]**.

2 Burgess' estimate on character sums.

Significant improvements of the results on the two problems are obtained by Burgess in 1957. In his paper **[6]**, he proved the following

Theorem 2.1 Let δ and ϵ be any fixed positive numbers. Then, for all sufficiently large p and any N, one has

$$\left|\sum_{n=N+1}^{N+H}\left(\frac{n}{p}\right)\right| < \epsilon H,$$

provided $H > p^{\frac{1}{4}+\delta}$. In this theorem, the magnitude of p for the result to hold only depends on δ and ϵ.

The starting point of this result is just the above estimate on $S_h(x)$, strengthened by a deep theorem of A. Weil's that is an analogue of the Riemann Hypothesis; see **[7]**. The result is

$$\sum_x \big(S_h(x)\big)^{2r} < (2r)^r p h^r + r(2p^{\frac{1}{2}}+1)^{2r}$$

for any positive integer r. We shall use multiple times the following consequence of this theorem:

Lemma 2.2 (A. Weil) Let $f(x)$ be a polynomial of degree k with integral coefficients and highest coefficient 1. Suppose that $f(x)$ is square-free $(\mathrm{mod}\, p)$. Then

$$\left|\sum_x\left(\frac{f(x)}{p}\right)\right| \le (k-1)p^{\frac{1}{2}},$$

where the summation is over a complete set of residues $(\mathrm{mod}\, p)$.

It should be noted that in **[6]**, this lemma is stated only for odd k, but one sees later in the proof that the result holds for even k as well (in fact, the result is even stronger in this case). To complete the proof of *Theorem 2.1,* the key observation is that, the set $\{1, 2, \cdots, p\}$ contains not only translates of $\{1, 2, \cdots, H\}$, but more images of $\{1, 2, \cdots, H\}$ under *affine transformations*. To be more specific, we have already obtained a bound for $\sum_x |S_h(x)|^{2r}$, where the sum is over a *complete* set of residues $(\mathrm{mod}\, p)$. Now we want to choose some disjoint subsets of $\{1, 2, \cdots, p\}$, such that if the estimate is false, the sum on these subsets is large enough for a contradiction. It turned out that these subsets can be chosen as the images of affine transformations of $\{1, 2, \cdots, H\}$: one can group the terms in the sum $|\sum_{n=N+1}^{N+H}(\frac{n}{p})|$ by modulo a prime q, which gives affine transformations of scaling $\frac{1}{q}$. If $|\sum_{n=N+1}^{N+H}(\frac{n}{p})|$ is large, it tells us that the sum over images related to q is large. Summing again over q where q are primes ranging between some interval dependent on p, and comparing the result with the bound for $\sum_x |S_h(x)|^{2r}$, one would arrive at a contradiction. The fact that q's are mutually coprime is essential for these images to be disjoint.

In short, the proof used an amplification trick that turns the 'local' magnitude of $|\sum_{n=N+1}^{N+H}(\frac{n}{p})|$ into the 'global' magnitude of $\sum_x |S_h(x)|^{2r}$.

An immediate consequence of this theorem is that $M = O(p^{\frac{1}{4}+\delta})$ for large p. This estimate is better than Davenport and Erdős's previous result. On the other hand, we show the following estimate by applying this theorem to Vinogradov's original method. We shall also return this argument in Section 3.

Theorem 2.3 Let $n_1(p)$ denote the least positive quadratic non-residue $(\mathrm{mod}\, p)$. Then one has

$$n_1(p) < p^{\frac{1}{4\sqrt{e}}+\varepsilon}$$

as $p \to \infty$, for every $\varepsilon > 0$. (Note that we distinguish ε and ϵ below when they denote different small positive numbers.)

Proof. Since $\frac{1}{4}e^{-\frac{1}{2}} > \frac{1}{8}$, we can take $H = [p^{\frac{1}{4}+\delta}]$ and suppose that $H < n_1(p)^2$, for some small positive number δ. Then, every quadratic non-residue $(\mathrm{mod}\, p)$ less than H must have some quadratic non-residue prime factor, and this prime factor is at least $n_1(p)$. Thus one has

$$\sum_{n=1}^{H}\left(\frac{n}{p}\right) = H - 2\sum_{n_1(p)\le q\le H}\left[\frac{H}{q}\right] > H\Big(1 - 2\sum_{n_1(p)\le q\le H}\frac{1}{q}\Big),$$

where the sum is over prime numbers. From *Theorem 2.1,* it follows that for every $\epsilon > 0$,

$$1 - 2\sum_{n_1(p)\le q\le H}\frac{1}{q} < \epsilon,$$

that is,

$$\sum_{n_1(p)\le q\le H}\frac{1}{q} > \frac{1}{2}(1-\epsilon).$$

By a prime number estimate, the left sum is

$$\log\log H - \log\log n_1(p) + o(1)$$

as $p \to \infty$. Let $n_1(p) = H^{\frac{1}{\beta}}$, one sees that $\beta > \exp(\frac{1}{2} - \epsilon)$ and the result follows. □

This is by far the sharpest estimate on Problem (1).

Some details of Burgess' proof.

Here I shall discuss three fine points of Burgess' original proof that I spent some time thinking over. The first is how to apply *Lemma 2.2* to the case where k is even. We consider the sum

$$S = \sum_x \left(\frac{(x+u_1)(x+u_2)\cdots(x+u_k)}{p}\right),$$

where $1 \le k \le 2r$ for some positive integer r and u_i are mutually incongruent $(\mathrm{mod}\, p)$. Burgess wrote that 'the transformation from x to y defined by $(x+u_1)y \equiv 1 \ (\mathrm{mod}\, p)$ changes the sum S into a similar

sum with $k-1$ factors ...,' but I have only succeeded after making a shift in S: since the sum is taking over a complete set of residues $(\mathrm{mod}\, p)$, one can write

$$S = \sum_x \left(\frac{(x+u_1)(x+u_2)\cdots(x+u_k)}{p} \right) = \sum_{x\neq 0} \left(\frac{x\cdot(x+u_2-u_1)\cdots(x+u_k-u_1)}{p} \right).$$

Since k is even, one has

$$\begin{aligned} |S| &= \left| \prod_{2\leq j\leq k} \left(\frac{(u_j-u_1)^{-1}}{p} \right) \cdot \sum_{x\neq 0} \left(\frac{x^{-k}\cdot x\cdot(x+u_2-u_1)\cdots(x+u_k-u_1)}{p} \right) \right| \\ &= \left| \sum_{x\neq 0} \left(\frac{(x^{-1}+(u_2-u_1)^{-1})(x^{-1}+(u_3-u_1)^{-1})\cdots(x^{-1}+(u_k-u_1)^{-1})}{p} \right) \right|. \end{aligned}$$

Thus the transformation from x to y by $x\cdot y \equiv 1 \ (\mathrm{mod}\, p)$ indeed turns S into a similar sum with $k-1$ factors, with an error term of at most 1.

The second point is as follows: for I some interval related to p and any positive integer h, one has

$$\sum_{z\in I} \left(\frac{z}{p}\right) = h^{-1} \sum_{m=1}^{h} \sum_{n\in I} \left(\frac{n}{p}\right) = h^{-1} \sum_{m=1}^{h} \left(\sum_{n\in I} \left(\frac{n+m}{p}\right) + \phi(m) \right),$$

where $|\phi(m)| \leq 2m$. The aim is to transform the sums on intervals I into those of the form $S_h(n)$. It took me a while to see why $\phi(m)$ satisfies this inequality; at first I tried to compare $(\frac{n}{p})$ with $(\frac{n+m}{p})$, but they seem unrelated for general n, which made me think that $|\phi(m)|$ is related to the length of I. The 'key' observation, however, lies in the simple fact that I is an *interval,* and thus $\sum_{n\in I}(\frac{n}{p})$ and $\sum_{n\in I}(\frac{n+m}{p})$ differ by at most $2m$ terms. It is the particular structure of I that makes the estimate on $\phi(m)$ possible.

The last point is on the transition between the inequality

$$\sum_I \sum_{n\in I} |S_h(n)|^{2r} > \left(\frac{1}{4}\epsilon HQh\right)^{2r} \left(p^{\frac{1}{4}}Q\cdot 3p^{-\frac{1}{4}}H\right)^{1-2r}$$

and

$$\sum_x |S_h(x)|^{2r} > \left(\frac{1}{12}\epsilon\right)^{2r} HQh^{2r}.$$

Here $S_h(x) = \sum_{m=1}^{h}(\frac{x+m}{p})$ and $Q = \pi(p^{\frac{1}{4}}) - \pi(\frac{1}{2}p^{\frac{1}{4}})$. It is shown that the intervals I are disjoint, but one might worry about their behaviors after modulo p. Nevertheless, the intervals $I = I(q,t)$, where q is a prime in some interval related to p and $0 \leq t < q$, are of the form

$$\frac{N+tp}{q} < z \leq \frac{N+H+tp}{q},$$

where $p^{\frac{1}{4}+\delta} < H < p^{\frac{1}{2}+\delta}$ and $\frac{1}{2}p^{\frac{1}{4}} < q < p^{\frac{1}{4}}$. Examine the proof, one sees that the integer N is irrelevant to the estimate, so we may assume $N=0$. Now all integers n in some I satisfy $0 < n \leq 2p^{\frac{1}{4}+\delta} + p < 3p$. Thus every residue class is counted at most three times in $\sum_I \sum_{n\in I} |S_h(n)|^{2r}$, and the second inequality follows.

3 Applications of Burgess' estimate to related problems.

In this section, I shall explore the following two problems, both on quadratic non-residues, by applying Burgess' method and result to them:

(3) The bound for the least positive integer n such that n and $n+1$ are *both* quadratic non-residues modulo p;

(4) The bound for $n_2(p)$, the *second prime* quadratic non-residue $(\mathrm{mod}\, p)$.

We start with Problem (3). First, one would ask whether n is well-defined, i.e., whether such n exists for large p. This is easily guaranteed. On the one hand, one may argue by contradiction: suppose for large p, there is no integer n such that both n and $n+1$ are quadratic non-residues $(\mathrm{mod}\, p)$. Since in a complete set of residues $(\mathrm{mod}\, p)$, there are exactly half quadratic residues and half non-residues, it follows that quadratic residues and non-residues must occur alternatively. Thus 4 would be a quadratic non-residue for $p \geq 5$, leading to a contradiction. This shows that n exists for such p.

P. D. Elliot gave another argument in **[8]** of this result. The proof is of some interest, as the method is 'classical' and also gives a concrete example of how *Lemma 2.2* can be applied to an even degree, so we give it below:

Proof. Consider the reduced residue classes $(\mathrm{mod}\, p)$ as a multiplicative group. To begin with,

$$\sum_{x=1}^{p-2}\Big(\frac{x\cdot(x+1)}{p}\Big)=\sum_{x=1}^{p-2}\Big(\frac{1+x^{-1}}{p}\Big)=\sum_{y=1}^{p-2}\Big(\frac{1+y}{p}\Big)=-1.$$

If we denote by $N(p)$ the number of consecutive quadratic non-residues in the interval $[1, p-1]$, one then has

$$N(p)=\frac{1}{4}\sum_{x=1}^{p-2}\Big(-1+\big(\frac{x}{p}\big)\Big)\Big(-1+\big(\frac{x+1}{p}\big)\Big)=\frac{1}{4}\Big(p-2+\big(\frac{-1}{p}\big)\Big).$$

Thus $N(p)>0$ for $p\geq 5$, i.e., the integer n exists for $p\geq 5$. □

From this result, it is natural to consider similar problems as follows:

(5) For any positive integer k, is there a prime p such that $1, 2, \cdots, k$ are all quadratic residues modulo p?

(6) For any positive integer k, is there a bound $N(k)$ such that for primes $p > N(k)$, there exist k consecutive integers which are all quadratic residues (or non-residues) modulo p?

For Problem (5), the answer is affirmative: one can give a simple proof using Dirichlet's theorem. The first observation is that we only need to guarantee, for each positive integer k, there exists a prime p such that the first k *primes* are all quadratic residues $(\mathrm{mod}\, p)$. This is due to the complete multiplicativity of the Legendre symbol. We construct such p for some positive integer k.

Denote by p_r the r-th prime. It is well known that $(\frac{2}{p})=1$ if and only if p is of the form $8n\pm 1$. Let the prime p be large enough and of the form $8n+1$; thus $\frac{p-1}{4}$ is an even integer. By the Quadratic Reciprocity Law, one has

$$\Big(\frac{p_r}{p}\Big)\Big(\frac{p}{p_r}\Big)=(-1)^{\frac{(p-1)(p_r-1)}{4}}=1,\ \text{for}\ 2\leq r\leq k.$$

Thus, in order that p_r is a quadratic residue modulo p, it suffices that p is a quadratic residue modulo p_r. One is then lead to consider the sequence $8m\cdot\prod_{r=2}^{k}p_r+1$ for $m\in\mathbb{N}$. By Dirichlet's theorem, there

are infinitely many primes in it, and thus we are done.

For Problem (6), the answer is also positive. To obtain such a bound $N(k)$, we use the previous *Lemma 2.2.* For a prime p, consider the sum

$$\sum_{x=1}^{p-k}\Big(1+\epsilon(\frac{x}{p})\Big)\Big(1+\epsilon(\frac{x+1}{p})\Big)\cdots\Big(1+\epsilon(\frac{x+k-1}{p})\Big),$$

where $\epsilon\in\{\pm 1\}$. Expanding this sum, one obtains

$$p-k+\sum_{n=1}^{k}\sum_{a_i}\sum_{x=1}^{p-k}\epsilon^n\Big(\frac{(x+a_1)(x+a_2)\cdots(x+a_n)}{p}\Big),$$

where the second sum is taken over all possible sets of mutually different a_i. By *Lemma 2.2,* for every such set we have

$$\left|\sum_{x=1}^{p-k}\epsilon^n\Big(\frac{(x+a_1)(x+a_2)\cdots(x+a_n)}{p}\Big)\right|\le (n-1)p^{\frac{1}{2}}+k,$$

and thus

$$\left|\sum_{a_i}\sum_{x=1}^{p-k}\epsilon^n\Big(\frac{(x+a_1)(x+a_2)\cdots(x+a_n)}{p}\Big)\right|\le \binom{k}{n}\Big((n-1)p^{\frac{1}{2}}+k\Big).$$

It follows that

$$\sum_{x=1}^{p-k}\Big(1+\epsilon(\frac{x}{p})\Big)\Big(1+\epsilon(\frac{x+1}{p})\Big)\cdots\Big(1+\epsilon(\frac{x+k-1}{p})\Big)\ge p-k-\sum_{n=1}^{k}\binom{k}{n}\Big((n-1)p^{\frac{1}{2}}+k\Big).$$

The right hand side is a quadratic polynomial in $p^{\frac{1}{2}}$ with coefficients only related to k. Thus, there exists $N(k)$ such that the polynomial is positive when $p>N(k)$. On the other hand, if we denote by $M_{\pm}(p,k)$ the number of k consecutive quadratic residues (and non-residues, respectively) in the interval $[1,p-1]$, one sees easily that

$$M_{\pm}(p,k)=\frac{1}{2^k}\left|\sum_{x=1}^{p-k}\Big(1+\epsilon(\frac{x}{p})\Big)\Big(1+\epsilon(\frac{x+1}{p})\Big)\cdots\Big(1+\epsilon(\frac{x+k-1}{p})\Big)\right|,$$

depending on the choice of ϵ. It follows that $M_{\pm}(p,k)>0$ when $p>N(k)$, that is, there exist at least k consecutive integers that are all quadratic residues (or non-residues).

Working more carefully, one can prove the following theorems in **[9]**. *Theorem 3.3* gives an explicit bound for $N(k)$. The difference in odd and even cases is due to the fact that the result of *Lemma 2.2* is stronger for even integers; see **[6]**.

Theorem 3.1 For every odd integer $k\ge 1$, each prime p satisfying the inequality

$$p>k+(k-1)p^{\frac{1}{2}}+\sum_{j=1}^{(k-1)/2}\big(k-2j+1+(2j-2)p^{\frac{1}{2}}\big)\left(\binom{k}{2j-1}+\binom{k}{2j}\right)$$

has k consecutive quadratic residues and k consecutive quadratic non-residues in any complete set of residues $(\mathrm{mod}\, p)$.

Theorem 3.2 For every even integer $k \geq 2$, each prime p satisfying the inequality

$$p > k + \sum_{j=1}^{k/2} \big(k - 2j + 1 + (2j-2)p^{\frac{1}{2}}\big) \left(\binom{k}{2j-1} + \binom{k}{2j} \right)$$

has k consecutive quadratic residues and k consecutive quadratic non-residues in any complete set of residues $(\mathrm{mod}\, p)$.

Theorem 3.3 If we define integers B_k and C_k as follows

$$B_k = (k-3) \cdot 2^{k-1} + 2,\ C_k = (k+1) \cdot 2^{k-1} - 1,\ k \geq 2,$$

then any primes p such that

$$p > \frac{1}{4}\big(B_k + (B_k^2 + 4C_k)^{\frac{1}{2}}\big)^2$$

has k consecutive quadratic residues and k consecutive quadratic non-residues in any complete set of residues $(\mathrm{mod}\, p)$.

Remark. One easily sees that by modifying the above argument, we can show that for a positive integer k and a prescribed sequence $\theta = (\epsilon_1, \epsilon_2, \cdots, \epsilon_k)$ where $\epsilon_i \in \{\pm 1\}$, there exists a bound $N_\theta(k)$ such that for primes $p > N_\theta(k)$, one can find a sequence of k consecutive integers $\alpha+1, \alpha+1, \cdots, \alpha+k$ in the interval $[1, p-1]$, satisfying

$$\left(\frac{\alpha+i}{p}\right) = \epsilon_i,\ \ 1 \leq i \leq k.$$

Moreover, if we denote by $M_\theta(p,k)$ the number of such sequences, *Lemma 2.2* not only tells us that $M_\theta(p,k) > 0$ for large p and every θ, but also shows

$$M_\theta(p,k) = \frac{p}{2^k} + O_k(p^{\frac{1}{2}}). \qquad (*)$$

One sees that this the expected number of times: the complete multiplicativity property of the Legendre symbol becomes 'invisible' when we deal with short sequences in an additive way. Thus one may, in a sense, view $(\frac{\cdot}{p})$ as 'random' sequences here. Since there are 2^k possibilities of θ, the main term of M_θ should be $\frac{p}{2^k}$, as in $(*)$. The error term $O_k(p^{\frac{1}{2}})$ is also 'optimal': on the one hand, the Central Limit Theorem shows that randomly distributed sequences in $[1, p-1]$ exhibit fluctuations of size $p^{\frac{1}{2}}$ in global statistics, and thus it is hard to get an error term of size less than $p^{\frac{1}{2}}$; on the other, one can actually prove that for sufficiently large N,

$$\sum_{p=2}^{N} \big(M_\theta(p,k) - \frac{p}{2^k}\big)^2 \sim \sum_{p=2}^{N} p\,,$$

where the sum is taken over primes p. One sees then the error terms should indeed be as big as $p^{\frac{1}{2}}$.

Before proceeding, we shall take a look at Problem (4) also. The first idea of bounding $n_2(p)$ that came to my mind is to modify Vinogradov's trick as shown in the proof of *Theorem 2.3.* Indeed, using the same argument, one has

$$\sum_{n=1}^{H} \left(\frac{n}{p}\right) = H - 2\left[\frac{H}{n_1(p)}\right] - 2 \sum_{n_2(p) \leq q \leq H} \left[\frac{H}{q}\right] > H\Big(1 - \frac{2}{n_1(p)} - 2 \sum_{n_2(p) \leq q \leq H} \frac{1}{q}\Big),$$

and thus

$$\sum_{n_2(p)\le q\le H}\frac{1}{q}>\frac{1}{2}(1-\epsilon)-\frac{1}{n_1(p)}.$$

Applying the same asymptotic formula to the left hand side, one obtains

$$n_2(p)<p^{\frac{1}{4}e^{-\frac{1}{2}+\frac{1}{n_1(p)}}+\varepsilon}$$

for large p and every $\varepsilon>0$.

This estimate depends, however, heavily on $n_1(p)$ which behave differently for each prime. For example, if $n_1(p)=2$, this gives an estimate of $n_2(p)<p^{\frac{1}{4}+\varepsilon}$. Recall that the exponent for the *first* prime quadratic non-residue is $\frac{1}{4}e^{-\frac{1}{2}}=0.152\cdots$, this estimate does not seem sharp enough.

We can slightly refine the above argument. Since we are looking for a bound for $n_2(p)$, one is lead to minimize the effect of $n_1(p)$ on the estimate. Thus, it is natural to consider the sum

$$\sum_n\left(\frac{n}{p}\right)\ \text{taken over}\ 1\le n\le H,\ n_1(p)\nmid n$$

rather than $\sum_{n=1}^{H}(\frac{n}{p})$. Then every quadratic non-residue in the sum has a quadratic non-residue prime factor that is at least $n_2(p)$. Proceeding this way, one obtains the bound

$$n_2(p)<p^{\frac{1}{4}e^{-\frac{1}{2}+\frac{1}{2n_1(p)}}+\varepsilon}$$

for large p and every $\varepsilon>0$. Now this estimate gives for every prime p a bound $n_2(p)<p^{\frac{1}{4}e^{-\frac{1}{4}}+\varepsilon}$, and for primes of the form $8k\pm3$, the bound becomes $n_2(p)<p^{\frac{1}{4}e^{-\frac{1}{3}}+\varepsilon}$.

Still, this estimate has the disadvantage of hinging on $n_1(p)$. In fact, one may reasonably guess that the second prime non-residue does not exceed the first too much, and conjecture that $n_2(p)<p^{\frac{1}{4}e^{-\frac{1}{2}}+\varepsilon}$ for every $\varepsilon>0$ as well. In the following, we return to Problem (3) and obtain a bound for the least positive consecutive quadratic non-residues modulo a prime p (which we shall denote by $\alpha(p)$ and $\alpha(p)+1$ afterwards), and this conjecuture would follow as a corollary.

The first attempt in this direction is done by P. D. Elliot. He showed in [**8**] the following

Lemma 3.4 Let p be an odd prime. For any $H>1$ let $N(H)$ denote the number of pairs of integers $\alpha,\alpha+1\le H$ which are both quadratic non-residues (mod p). Let $'$ denote summation over integers which have a fixed parity. Then, if for both parities

$$\left|\sum_{n\le H}{}'\left(\frac{n}{p}\right)\right|\le\frac{1}{20}H$$

for a value of H satisfying $49\le H<p$, we have $N(H)\ge\frac{1}{48}H-1>0$.

We first show that combined with Burgess' *Theorem 2.1,* this gives an estimate

$$\alpha(p)=O_\varepsilon(p^{\frac{1}{4}+\varepsilon}),$$

and then sketch the proof of *Lemma 3.4.*

Proof. Let $H = p^{\frac{1}{4}+\delta}$ for a large prime p and a small $\delta > 0$; we show that the two inequalities are satisfied. For the sum over even integers, one has

$$\left|\sum_{n\le H}{}' \left(\frac{n}{p}\right)\right| = \left|\sum_{m\le[\frac{H}{2}]} \left(\frac{2}{p}\right)\cdot\left(\frac{m}{p}\right)\right| = \left|\sum_{m\le[\frac{H}{2}]} \left(\frac{m}{p}\right)\right| \le \epsilon\cdot\left[\frac{H}{2}\right] \le \frac{1}{20}H$$

by *Theorem 2.1,* on choosing a suitable ϵ. For the sum over odd integers, one has

$$\left|\sum_{n\le H}{}' \left(\frac{n}{p}\right)\right| = \left|\sum_{n\le H}{}' \left(\frac{-1}{p}\right)\cdot\left(\frac{n}{p}\right)\right| = \left|\sum_{n\le H}{}' \left(\frac{p-n}{p}\right)\right|,$$

returning to the even case since p is odd. □

Proof of Lemma 3.4 (sketch). Intuitively, this lemma is true because of the meta-theorem: 'If there is not enough quadratic non-residues, then there would be too many quadratic residues,' and the additional assumption on summing over parities allows us to replace 'quadratic non-residues' with '*consecutive* quadratic non-residues,' as is shown in the following.

From the hypothesis, one can deduce that

$$\left|\sum_{\substack{n\le H\\(\frac{n}{p})=\eta}}{}' 1 - \frac{1}{2}\sum_{n\le H}{}' 1\right| \le \frac{1}{2}\epsilon H, \qquad (\star)$$

where $\epsilon \ge \frac{1}{20}$ and η takes one of the values ± 1. This inequality holds uniformly in η and both parities. We now consider two cases according to the value $(\frac{2}{p})$. We shall treat the case $(\frac{2}{p}) = 1$, and the case $(\frac{2}{p}) = -1$ can be dealt with similarly.

Let $e_1, e_2, \cdots, e_m$ be even quadratic non-residues $(\mathrm{mod}\, p)$ not exceeding H in ascending order. The key idea is to consider the distances between e_i and e_{i+1}, and discuss the distribution of quadratic residues and non-residues in those intervals. Clearly, the number of intervals $(e_i, e_{i+1}]$ of length 2 is at most $N(\frac{1}{2}H)$. We consider next the remaining intervals (that is, intervals of length at least 4) that do *not* contain any pair of non-residues. Let there be M of them; by the assumption, each contains at least 3 quadratic *residues*.

Applying $(\star)$ to count m and the total number of residues not exceeding H, one has $m \ge \big(\frac{1}{4}-\frac{1}{2}\epsilon\big)H-1$ and $3M \le \big(\frac{1}{2}+\epsilon\big)H$, respectively. On the other hand, we have the estimate

$$N(H) \ge (m-1) - N\big(\frac{1}{2}H\big) - M.$$

Putting these together, and observing that trivially $N(H) \ge N\big(\frac{1}{2}H\big)$, one obtains

$$N(H) \ge \big(\frac{1}{24} - \frac{5}{12}\epsilon\big)H - 1.$$

Taking $\epsilon = \frac{1}{12}$ yields the result. □

P. D. Elliot remarked, however, that 'the bound on $\alpha(p)$ which is implied here is very poor.' One may in fact conjecture that $\alpha(p) = O(p^{\varepsilon})$ for every $\varepsilon > 0$, the reason being similar to that of Vinogradov's conjecture on the bound for $n_1(p)$. The bound for $\alpha(p)$ also leads to an estimate on $n_2(p)$: since $\alpha(p)$ and $\alpha(p)+1$ are coprime and both quadratic non-residues, it follows that they have two different quadratic non-residue prime factors $q_1, q_2 \leq \alpha(p)+1$. Hence one has

$$n_2(p) \leq \alpha(p) + 1 = O_{\varepsilon}(p^{\frac{1}{4}+\varepsilon}).$$

But this estimate is even weaker than our first estimate on $n_2(p)$, which again supports P. D. Elliot's claim.

Significant improvement of the above result was obtained by A. Hildebrand in **[10]**. He showed in this paper the following

Theorem 3.5 Let $\alpha(p)$ be as above. Then for sufficiently large p and every $\varepsilon > 0$, one has

$$\alpha(p) \leq p^{\frac{1}{4}e^{-\frac{1}{2}}+\varepsilon}.$$

Thus, one has the same bound for $\alpha(p)$ as for $n_1(p)$. Since trivially $\alpha(p) \geq n_1(p)$, any further improvement would seem very difficult. To prove this result, we first introduce two lemmas. One can found them in **[11]** and **[12]**, but as neither is particularly difficult, it is possible to work out the proofs oneself.

Lemma 3.6 For every positive integer r, there exist positive integers $t_1 < t_2 < \cdots < t_r$ such that

$$t_j - t_i = \gcd(t_i, t_j), \ \ 1 \leq i < j \leq r.$$

Proof. Let $N_1 = 1$, and $N_{k+1} = 2\prod_{j=1}^{k}\sum_{i=j}^{k} N_i$ for $k \geq 1$. Then by construction, one sees that $(\sum_{i=j}^{k} N_i) \,|\, N_{k+1}$ for $1 \leq j \leq k$. In particular, $N_k \,|\, N_{k+1}$ for all $k \geq 1$.

For a positive integer $r \geq 2$, let $t_r = N_r$ and $t_i = N_r - \sum_{j=i}^{r-1} N_j$ for $1 \leq i \leq r-1$. One can verify directly that

$$(t_j - t_i) \,|\, t_j, \ \ 1 \leq i < j \leq r,$$

which is equivalent to $t_j - t_i = \gcd(t_i, t_j), \ 1 \leq i < j \leq r$. □

Lemma 3.7 Let $\alpha(p), n_1(p)$ and $n_2(p)$ be as above. Then one has $\alpha(p) \leq (n_1(p)-1)n_2(p)$.

Proof. By Bezout's theorem, there exist integers $1 \leq a < n_2(p), 1 \leq b < n_1(p)$ such that

$$|a \cdot n_1(p) - b \cdot n_2(p)| = 1.$$

It follows from the definition of $n_1(p)$ that b is a quadratic residue $(\mathrm{mod}\, p)$; thus $b \cdot n_2(p)$ is a quadratic non-residue. If $n_1(p) \nmid a$, then a is also a quadratic residue and $a \cdot n_1(p)$ a non-residue, and we are done. If $n_1(p) \,|\, a$, one can let $\widehat{a} = n_2(p) - a$ and $\widehat{b} = n_1(p) - b$. Then $\widehat{a}$ and $\widehat{b}$ still satisfy the same conditions,

but now $n_1(p) \nmid \widehat{a}$, so one can apply the above argument to $\widehat{a}$ and $\widehat{b}$. □

The main idea of the proof of *Theorem 3.5* is to first give a criterion, as in *Lemma 3.8,* for a set of positive integers to contain a pair of consecutive integers up to some positive integer. Next, we show that for some suitable positive integer N, the set $A(p,N) := \{1 \le n \le N : \ (\frac{n}{p}) = -1\}$ satisfies the criterion, and thus contains two consecutive quadratic non-residues $(\mathrm{mod}\, p)$. We shall sketch the proof of *Theorem 3.5* first and then prove *Lemma 3.8.*

Lemma 3.8 For every $\epsilon \in (0,1]$ there exist positive integers $N_0(\epsilon)$ and $k_0(\epsilon)$ with the following property: If $N \ge N_0(\epsilon)$ and A is a set of positive integers satisfying

$$\sum_{\substack{n\le N \\ n\equiv l \bmod k \\ n\in A}} 1 \ge \epsilon\frac{N}{k}, \ \text{ for } \ 1 \le k \le k_0(\epsilon),\ 0 \le l \le k-1 \tag{i}$$

and

$$\Big\{\frac{n}{d} :\ n \in A,\ d \,|\, n,\ d \le k_0(\epsilon)\Big\} \subset A, \tag{ii}$$

then A contains a pair of consecutive integers $\le N$.

Proof of Theorem 3.5 (sketch). Let $\epsilon > 0$ be given and p is a large prime. We may assume for the proof that $0 < \epsilon < \frac{1}{100}$. This condition guarantees some of the estimates related to ϵ afterwards.

Let $N_1 = [p^{\frac{1+\epsilon}{4}}]$ and $N_2 = [p^{\frac{1}{4}e^{-\frac{1}{2}}+\epsilon}]$. Our aim is to find some $N \le N_2$ and apply *Lemma 3.8* to the set $A := A(p,N)$ described above. We want to count quadratic non-residues according to their prime factors. For this purpose, we construct the following sum over primes q:

$$S(x) = \sum_{\substack{q\le x \\ q\in A}} \frac{1}{q}.$$

We need to estimate the sum as in condition (i). The key is to obtain a lower bound for $S(N_2)$. Intuitively, Burgess' estimate guarantees that $S(N_1)$ is 'big' since there should be sufficiently many quadratic non-residues not exceeding N_1, and thus $S(N_2)$ would not be too small as well. To be more specific, *Theorem 2.1* as well as a counting argument suggests

$$\frac{1}{2}N_1(1-\epsilon) \le \sum_{\substack{n\le N_1 \\ n\in A}} 1 \le \sum_{\substack{q\le N_1 \\ q\in A}} \sum_{\substack{n\le N_1 \\ q\,|\,n}} 1 \le N_1 S(N_1),$$

where q denotes a prime number. Thus, one has $S(N_1) \ge \frac{1}{2}(1-\epsilon)$. On the other hand, trivially $S(N_1) - S(N_2) \le \sum_{N_2 < q \le N_1} \frac{1}{q}$, and a prime number estimate yields

$$S(N_1) - S(N_2) \le \frac{1}{2} - \log\frac{1+4\epsilon\sqrt{e}}{1+\epsilon} + O(\frac{1}{\log p}).$$

Taking note that $0 < \epsilon \le \frac{1}{100}$, one has $S(N_1) - S(N_2) \le \frac{1}{2} - 3\epsilon$ for sufficiently large p. Combining the results, one sees that

$$S(N_2) \ge \frac{5}{2}\epsilon.$$

It can be seen in the following that one also requires some upper bound on $S(N)$ to show that condition (i) holds. One way of doing this is to assume $n_1(p) > p^{\frac{\epsilon}{2}}$ first, so that $S(p^{\frac{\epsilon}{2}}) = 0$. From this and the bound on $S(N_2)$, we conclude that there exists $p^{\frac{\epsilon}{2}} \leq N \leq N_2$ such that

$$\frac{5}{2}\epsilon \leq S(N) \leq \frac{5}{2}\epsilon + \frac{1}{2} < \frac{4}{7}.$$

For $k \leq p^{\frac{\epsilon}{2}}$ (this guarantees k is coprime with every $q \in A$) and $0 \leq l \leq k-1$, using Inclusion-Exclusion Principle and a prime number estimate, one has

$$\begin{aligned}
\sum_{\substack{n\leq N\\ n\equiv l \bmod k\\ n\in A}} 1 &\geq \sum_{\substack{q\leq N\\ q\in A}} \sum_{\substack{n\leq N\\ n\equiv l \bmod k\\ q\,|\,n}} 1 - \sum_{\substack{q,q'\leq N\\ q,q'\in A}} \sum_{\substack{n\leq N\\ n\equiv l \bmod k\\ qq'\,|\,n}} 1 \\
&\geq \frac{N}{k} S(N)\big(1-S(N)\big) - \sum_{q\leq N} 1 - \sum_{\substack{q,q'\leq N\\ qq'\leq N}} 1 \\
&\geq N\Big(\frac{15}{14}\cdot\frac{\epsilon}{k} + O_\epsilon\Big(\frac{\log\log(N+2)}{\log N}\Big)\Big).
\end{aligned}$$

For sufficiently large p, one has $k \leq k_0(\epsilon)$ and that the last expression is $\geq \epsilon\frac{N}{k}$; condition (i) is fulfilled. On the other hand, condition (ii) holds for $p \geq k_0(\epsilon)^{\frac{2}{\epsilon}}$ because of the assumption $n_1(p) > p^{\frac{\epsilon}{2}}$ and the complete multiplicativity of the Legendre symbol. Thus this case is done for large p.

It remains to deal with the case where $n_1(p) \leq p^{\frac{\epsilon}{2}}$. The proof is more technical here, so we merely outline the main idea. Applying *Lemma 3.7*, it suffices to show that $n_2(p) \leq N_3 := [p^{\frac{1}{4}e^{-\frac{1}{2}}+\frac{\epsilon}{2}}]$. If this is not true, then the second prime non-residue is 'big', and one would expect that there wouldn't be 'enough' quadratic non-residues within some range. Indeed, consider the quadratic non-residues up to N_1, they have at most one prime factor $> N_3$ since $N_3^2 > N_1$. By a sieve argument, one can show

$$\sum_{\substack{n<N_1\\ n\in A}} 1 \leq N_1\big(\frac{1}{2} - \frac{\epsilon}{4}\big),$$

that is, the number of quadratic non-residues up to N_1 is relatively 'small'. It follows that

$$\sum_{n\leq N_1}\left(\frac{n}{p}\right) = N_1 - 2\sum_{\substack{n\leq N_1\\ n\in A}} 1 \geq \frac{\epsilon}{2}N_1,$$

contradicting *Theorem 2.1.* □

Proof of Lemma 3.8. For a given $0 < \epsilon \leq 1$, put $r = [\frac{2}{\epsilon}] + 1$ and choose positive integers $t_1, t_2, \cdots, t_r$ as in *Lemma 3.6.* Let $t = \prod_{i=1}^r t_i$. We prove the lemma with

$$N_0(\epsilon) = \left[\frac{2t}{\epsilon}\right] + 1 \ \ , k_0(\epsilon) = t.$$

Let $N \geq N_0(\epsilon)$ and a set $A \subset \mathbb{N}$ satisfying (i) and (ii) be given. The key is to consider the sets

$$B_i = \{n \leq N : \ t\,|\,n,\ n - t_i \in A,\ \ 1 \leq i \leq r\}.$$

If $B_i \cap B_j$ is nonempty for some $i < j$, then by the properties $t_j - t_i = \gcd(t_i, t_j)$ and (ii), one can show that $\frac{n-t_i}{\gcd(t_i,t_j)}$ and $\frac{n-t_j}{\gcd(t_i,t_j)}$ are consecutive integers $\leq N$ and both contained in A. Thus, it suffices to

prove that this is always the case. We proceed by contradiction and suppose all B_i are disjoint. Then one has

$$\sum_{i=1}^{r} |B_i| = \left| \bigcup_{i=1}^{r} B_i \right| \leq \sum_{\substack{n \leq N \\ t \mid n}} 1 \leq \frac{N}{t}.$$

On the other hand, condition (i) gives for each $i \leq r$

$$|B_i| = \sum_{\substack{n \leq N - t_i \\ n \equiv -t_i \bmod t \\ n \in A}} 1 \geq \sum_{\substack{n \leq N \\ n \equiv -t_i \bmod t \\ n \in A}} 1 - 1 \geq \epsilon \frac{N}{t} - 1.$$

Taking note that $r = [\frac{2}{\epsilon}] + 1$ and summing this over $1 \leq i \leq r$, we arrive at a contradiction. □

Following the same argument earlier, one obtains the bound $\alpha(p) < p^{\frac{1}{4}e^{-\frac{1}{2}}+\varepsilon}$ for every $\varepsilon > 0$, proving our conjecture on Problem (4).

4 Further discussions.

At this point, one can continue on problems such as the bound for $\beta(p)$, the least positive integer such that $\beta(p), \beta(p)+1, \beta(p)+2$ are all quadratic non-residues $(\bmod p)$. A. Weil's *Lemma 2.2* still gives an estimate (we shall explain below), but further improvement appears quite difficult, as is remarked by R. Hudson in **[13]**. P. D. Elliot's method does not generalize well, and I have yet to come up with a similar criterion as *Lemma 3.8* that shows a set contains three consecutive integers.

One can, however, obtain a sharper bound for $\gamma(p)$, defined as the least positive integer such that $\gamma(p), \gamma(p)+1, \gamma(p)+2$ are all quadratic *residues* $(\bmod p)$. We only state the result here; one can find the idea of the proof in R. Hudson's paper **[14]**. Note that this estimate is much weaker than those on $\alpha(p)$ and $n_2(p)$.

Theorem 4.1 For all primes $p > 17$, one has $\gamma(p) < 270.5\, p^{\frac{1}{4}} \log p + 62$.

Now we shall give a final remark on why Fourier transform would work in the proof of Pólya-Vinogradov inequality and in more general situations.

Let $f(n)$ be a function from $\mathbb{Z}/p\mathbb{Z}$ to the complex numbers. The key idea is that, when bounding $|\sum_{n=1}^{N} f(n)|$ for some $1 \leq N \leq p-1$, one can write it as the sum over a complete set of residues $(\bmod p)$ combined with a cutoff function, namely

$$\left| \sum_{n=1}^{N} f(n) \right| = \left| \sum_{n=1}^{p-1} f(n) \cdot \delta_N \right|,$$

where δ_N is the characteristic function of the set $\{1, 2, \cdots, N\}$. If we consider the space $L^2(\mathbb{Z}/p\mathbb{Z})$ with the inner product defined as the sum of pointwise products, then one can show that the discrete Fourier transform

$$\mathcal{F} : L^2(\mathbb{Z}/p\mathbb{Z}) \to L^2(\mathbb{Z}/p\mathbb{Z}), \quad f \mapsto \widehat{f}$$

is an automorphism *preserving inner products.* Thus, one obtains

$$\left|\sum_{n=1}^{p-1} f(n)\cdot\delta_N\right| = \left|\sum_{n=1}^{p-1} \widehat{f}(n)\cdot\widehat{\delta_N}\right|.$$

Generally speaking, the Fourier transform of a cutoff function is both small and predictable; thus to obtain a bound for $|\sum_{n=1}^{N} f(n)|$, one only needs to bound $\widehat{f}(n)$ in various ways (pointwise, in L^2 norms, etc.) which is often achievable. In the Pólya-Vinogradov inequality case, this leads to the Gaussian sum, which is bounded by $O(\sqrt{p})$.

In the problem of estimating $\beta(p)$ mentioned above, one is led to consider the sum

$$S(p,N) = \sum_{x=1}^{N}\left(1-\left(\frac{x}{p}\right)\right)\left(1-\left(\frac{x+1}{p}\right)\right)\left(1-\left(\frac{x+2}{p}\right)\right).$$

Expanding this, one gets a constant term N plus sums of single, pairwise product, and triple product of Legendre symbols, respectively. If we let

$$f_1(n)=\left(\frac{n}{p}\right),\ f_2(n)=\left(\frac{n\cdot(n+1)}{p}\right),\ f_3(n)=\left(\frac{n\cdot(n+2)}{p}\right),\ f_4(n)=\left(\frac{n\cdot(n+1)\cdot(n+2)}{p}\right),$$

one can then apply the above argument and derive an estimate for $S(p,N)$, as A. Weil's result would give bounds for $\widehat{f_i}(n)$, $1\le i\le 4$. One may, in the end, obtain a bound of $\beta(p)=O(p^{\frac{3}{4}})$, but this is obviously not sharp enough compared with our previous results.

References.

[**1**] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste,* Göttinger Nachrichten (1918) 21-29.

[**2**] I. M. Vinogradov, *Sur la distribution des résidues et des non-résidus des puissances,* Journal Physico-Math. Soc. Univ. Perm., No. 1 (1918), 94-96.

[**3**] I. M. Vinogradov, *On a general theorem concerning the distribution of the residues and non-residues of powers,* Trans. Amer. Math. Soc., 29 (1927), 209-217.

[**4**] I. M. Vinogradov, *On the bound of the least non-residue of n-th powers,* Trans. Amer. Math. Soc., 29 (1927), 218-226.

[**5**] H. Davenport and P. Erdős, *The distribution of quadratic and higher residues,* Publicationes Mathematicae (Debrecen), 2 (1952), 252-265.

[**6**] D. A. Burgess, *The distribution of quadratic residues and non-residues,* Mathematika 4 (1957) 106-112.

[**7**] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent,* Actualités Math. et Sci., No. 1041 (1945), Deuxième partie, §IV.

[**8**] P. D. Elliot, *On the mean value of $f(p)$,* Proc. London Math. Soc., (3) 21 (1970) 28-96.

[**9**] D. Buell and R. Hudson. *On runs of consecutive quadratic residues and quadratic nonresidues,* BIT Numerical Mathematics, 24 (1984), 243-247.

[**10**] A. Hildebrand, *On the least pair of consecutive quadratic non-residues,* The Michigan Mathematical Journal, 34 (1987), 57-62.

[**11**] A. Hildebrand, *On a conjecture of Balog,* Proc. Amer. Math. Soc., 95 (1985), 517-523.

[**12**] R. Hudson, *The least pair of consecutive character non-residues,* J. Reine Angew. Math., 281 (1976), 219-220.

[**13**] R. Hudson, *On the first occurrence of certain patterns of quadratic residues and non-residues,* Israel J. Math., 44 (1983) 23-32.

[**14**] R. Hudson, *Totally multiplicative sequences with values ± 1 which exclude four consecutive values of 1,* J. Reine Angew. Math., 271 (1974), 218-220.