Note On Quadratic Residues For Primes of the Form 4k+3

Louis D. Grey

Abstract. It is a well known result that for a prime of the form 4k+3, there are more quadratic residues than non residues in the interval \((1, \frac{p-1}{2})\) i.e. see [1]. Let \(N_p(1, \frac{p-1}{2})\) denote the number of quadratic residues in the interval \((1, \frac{p-1}{2})\). We show that as \(p \to \infty\),

\[
\frac{p}{4} + \left(\frac{\sqrt{2} - 1}{2}\right)p^{\frac{1}{2}} < N_p(1, \frac{p-1}{2}) < \frac{p}{4} + \frac{(2\sqrt{2} - 1)}{4}\frac{p^{\frac{1}{2}}}{2}.
\]

1. INTRODUCTION. The quadratic residues \(r_i\) are the residues of \(i^2 \pmod{p}\) \(i = 1, 2, \ldots, \frac{p-1}{2}\). \(r_i\) will lie in \((1, \frac{p-1}{2})\) if and only if \(i^2\) lies in one of the intervals

\[
\left[\sqrt{(k + \frac{1}{2})p} - \left\lfloor \sqrt{kp} \right\rfloor p \right] - \sqrt{kp} + \left\{ \sqrt{kp} \right\}
\]

where the brackets "[ ]" denote the floor function

We can rewrite (1) as

\[
\sqrt{(k + \frac{1}{2})p} - \left\lfloor \sqrt{(k + \frac{1}{2})p} \right\rfloor - \sqrt{kp} + \left\{ \sqrt{kp} \right\},
\]

where "\{\}" denote the fractional part of the entry.

Hence \(N_p(1, \frac{p-1}{2}) = \sum_{k=0}^{\frac{p-3}{4}} \sqrt{(k + \frac{1}{2})p} - \left\lfloor \sqrt{(k + \frac{1}{2})p} \right\rfloor - \sqrt{kp} + \left\{ \sqrt{kp} \right\}\)
Lemma 1. \( \lim_{p \to \infty} \sum_{k=0}^{p-3} \left( \sqrt{kp} - \sqrt{\left( k + \frac{1}{2} \right) p} \right) = 0 \)

We do this by showing that \( p \to \infty, \ f_p(k) = \sqrt{kp} \) and \( g_p(k) = \sqrt{\left( k + \frac{1}{2} \right) p} \) are uniformly distributed on \((0, 1)\).

This follows from the fact that \( f_p(k) \) and \( g_p(k) \) satisfy the following four conditions as shown in [2].

1. \( f_p(k) \) is continuously differentiable.
2. \( f_p(k) \) is monotone increasing to \( \infty \) as \( k \to \infty \).
3. \( f'_p(k) \) is monotone decreasing to \( 0 \) as \( k \to \infty \).
4. \( kf'_p(k) \) tends to \( \infty \) as \( k \to \infty \).

As \( p \to \infty, \sum_{k=0}^{p-3} f_p(k) \) and \( \sum_{k=0}^{p-3} g_p(k) \) will \( \to \frac{p-3}{8} \) so their difference \( \to 0 \).

Lemma 2. We now need to evaluate \( h_p(k) = \sum_{k=0}^{p-3} \left( \sqrt{\left( k + \frac{1}{2} \right) p} - \sqrt{kp} \right) \) as \( p \to \infty \)

Factoring out \( \frac{1}{k^2} \) \( p \) \( p^3 \) from (4) we get \( h_p(k) = \frac{1}{k^2} \ p^3 \sum_{k=1}^{p-3} \left( \frac{1 + \frac{1}{2(2k)^2}}{1} - 1 \right) + \left( \frac{p}{2} \right)^{\frac{1}{2}} \) (5)

Making use of the Bernoulli inequality \( (1 + x)^a \leq 1 + ax \) \( \text{where} \ x > -1, 0 < \alpha < 1 \) we get

\[
h_p(k) = \frac{p}{2} \sum_{k=1}^{p-3} \frac{1}{k^2} + 2 \sqrt{2} \] (6)

It can be shown i.e. [3] that the following inequality holds

\[
2 \sqrt{k} - 2 < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots \frac{1}{\sqrt{k}} < 2 \sqrt{k} - 1 \] (7)

adding \( 2 \sqrt{2} \) to (7) gives us
\[
2 \sqrt{k} - 2 + 2 \sqrt{2} < 2 \sqrt{2} + 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{k}} < 2 \sqrt{k} - 1 + 2 \sqrt{2} \quad (8)
\]

Letting \( k = \frac{p - 3}{4} \), in (8), multiplying by \( \frac{p^2}{4} \) and taking the limit as \( p \to \infty \), we get

\[
\text{as } p \to \infty \quad \frac{p}{4} + \left(\frac{\sqrt{2} - 1}{2}\right) p^\frac{1}{2} < N_p \left(1, \frac{p - 1}{2}\right) < \frac{p}{4} + \frac{\left(2 \sqrt{2} - 1\right)}{4} p^\frac{1}{2} \quad (9)
\]

which together with Lemma 1 is the desired result.

References

