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 $\left(1, \frac{p-1}{2}\right)$. we show that as $p \to \infty$,

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

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

$$\left\lfloor \sqrt{\left(k+\frac{1}{2}\right)p} \right\rfloor - \left\lfloor \sqrt{kp} \right\rfloor \quad k = 0,1,2, \ldots \frac{p-3}{4} \tag{1}$$

where the brackets " $\lfloor\ \rfloor$ " denote the floor function

We can rewrite (1) as

$$\sqrt{\left(k+\frac{1}{2}\right)p} - \left\{\sqrt{\left(k+\frac{1}{2}\right)p}\right\} - \sqrt{kp} + \left\{\sqrt{kp}\right\} \tag{2}$$

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

Hence $$N_p\left(1, \frac{p-1}{2}\right) = \sum_{0}^{\frac{p-3}{4}} \sqrt{\left(k+\frac{1}{2}\right)p} - \left\{\sqrt{\left(k+\frac{1}{2}\right)p}\right\} - \sqrt{kp} + \left\{\sqrt{kp}\right\} \tag{3}$$

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

We do this by showing that $p\to\infty$, $f_p(k)=\left\{\sqrt{kp}\right\}$ *and* $g_p(k)=\left\{\sqrt{\left(k+\frac{1}{2}\right)p}\right\}$ 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 ∞ *as* $k\to\infty$.

(3) $f'_p(k)$ is monotone decreasing to 0 as $k\to\infty$

(4) $kf'_p(k)$ *tends to* ∞ *as* $k\to\infty$

As $p\to\infty$, $\sum_{0}^{\frac{p-3}{4}} f_p(k)$ *and* $\sum_{0}^{\frac{p-3}{4}} g_p(k)$ *will* $\to\frac{p-3}{8}$ *so their difference will* $\to 0$

Lemma 2. We now need to evaluate $h_p(k)=\sum_{o}^{\frac{p-3}{4}}\left(\sqrt{\left(k+\frac{1}{2}\right)p}-\sqrt{kp}\right)$ *as* $p\to\infty$ (4)

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

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

$$h_p(k)=\frac{p^{\frac{1}{2}}}{4}\sum_{k=1}^{\frac{p-3}{4}}\frac{1}{k^{\frac{1}{2}}}+2\sqrt{2} \qquad (6)$$

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

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

adding $2\sqrt{2}$ to (7) gives us

$$2\sqrt{k} - 2 + 2\sqrt{2} < 2\sqrt{2} + 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \dots \frac{1}{\sqrt{k}} < 2\sqrt{k} - 1 + 2\sqrt{2} \qquad (8)$$

Letting $k = \frac{p-3}{4}$, in (8), multiplying by $\frac{p^{\frac{1}{2}}}{4}$ and taking the limit as $p \to \infty$, we get

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

which together with Lemma 1 is the desired result.

References

1

1. A. L. Whiteman, *Theorems On Quadratic Residues*, Bulletin of The American Mathematical Society Vol. 47 (1941) pp514-516.

2. G. Polya & G. Szego, *Problems & Theorems In Analysis, Volume 1*, Springer 1998, p90, Problem 174

3. P.P. Korovkin, *Inequalities*, Little Mathematics Library, Mir Publishers, Moscow