The density of power residues and non-residues in subintervals of \([1, \sqrt[4]{p}]\)

by

CLIPTON T. WHITMORE (Baton Rouge, La.)

Throughout this paper, \(p\) will denote an odd prime, and in the new section \(p\) will be assumed "sufficiently large".

The distribution of power residues and non-residues \((\text{mod } p)\), particularly in the interval \([1, \sqrt[4]{p}]\), has been an object of study since the time of Gauss ([1], art. 129). For the \(k\) classes of \(k\)th power residues and non-residues \((\text{mod } p)\), where \(k\mid p-1\), L. Rédei [3] has proved:

**Theorem A.** If \(k\mid (p-1)/2\), the density of any class in the interval \([1, \sqrt[4]{p}]\) is less than \(1 - (k-1)/k(2+\sqrt[4]{2})\).

**Theorem B.** For \(4\mid p+1\), the density of the quadratic residues and also that of the non-residues in the interval \([1, \sqrt[4]{p}\sqrt[8]{3}]\) is greater than \(1/(8+4\sqrt[8]{2})\) (\(= 1/14,928 \ldots\)).

Theorem A has the corollary:

**Theorem A'.** For \(4\mid p-1\), the density of the quadratic residues and also that of the non-residues \((\text{mod } p)\) in the interval \([1, \sqrt[4]{p}]\) is greater than \(1/(4+2\sqrt[4]{2})\) (\(= 1/6,828 \ldots\)).

The purpose of this article is to exhibit results similar to those of Rédei, but valid for shorter intervals, and for all sufficiently large (odd) primes \(p\). The technique used is elementary except for the use of the well-known ([5], p. 131) formula:

\[
\sum_{j=1}^{q} \varphi(j) = 3q^{1/2} + O(q \log q).
\]

**Theorem.** Let \(d\) be a positive integer, such that \(d\mid p-1\) and \(d \geq 2\). Let \(h\) be such that \(g = h\sqrt[p]{p}\) is a positive integer and

\[
1 > h^2 > p^{3/4}d.
\]

Denote by \(C_d\) the set of \(d\)-th power residues \((\text{mod } p)\) and define the classes \(C_{1}, C_{2}, \ldots, C_{d-1}\) by \(x, y \in C_d\) if \(x\) and \(y\) are prime to \(p\) and their quotient

\text{Acta Arithmetica XIV}.
is congruent an element of \( C_\ell \mod p \). If \( \nu_\ell \) is the number of elements of \( C_\ell \) in \([1, q]\), we have:

\[
\nu_\ell /q = \delta_\ell = \left(1 + (d-1)^{-1}[1 - 6d/(\sigma^2(d-1))] + 1/[1 - 6d/(d-1)^2]\right)^{1/2}/d + o(1).
\]

**Proof.** Let the number of distinct, reduced fractions \( a/b \) \((a, b) = 1,\) with \( a, b \) integers of \([1, q]\) be denoted by \( A \). Then

\[
A = 2\sum_{\ell=1}^{\infty} \phi(\ell) - 1 = 6q^2/\pi^2 + O(q \log q),
\]

where \( \phi \) is Euler's function.

Let us define \( \eta_\ell \) for \( \ell \geq d \) by \( \eta_\ell = \nu_\ell \) if \( \ell = j \mod d \). One may then form

\[
\sum_{\ell=1}^{d} \eta_\ell\eta_{\ell+1}
\]

fractions which are congruent elements of \( C_\ell \mod p \) and which have numerator and denominator chosen from \([1, q]\). Not all of these are reduced.

Since the \( A \) fractions \( a/b \) enumerated in (1) have \( 1 \leq a, b \leq q < \sqrt{p} \), and \((a, b) = 1\), no two are congruent \( \mod p \). Even if these fractions represent all \((p-1)/d\) elements of \( C_\ell \), they will still represent \( A - (p-1)/d\) elements of \( C_\ell \cup C_{\ell+1} \cup \ldots \cup C_{\ell-1} \). Further, since \( p \) is large, and by the lower bound on \( \kappa \), we have:

\[
A - (p-1)/d > 0,
\]

and certainly:

\[
\sum_{\ell=1}^{d} \sum_{\eta_\ell \in C_\ell} \eta_\ell\eta_{\ell+1} \geq A - (p-1)/d.
\]

There is the additional condition:

\[
\sum_{\ell=1}^{d} \eta_\ell = q.
\]

We may divide (3) through by \( q \) to obtain

\[
\sum_{\ell=1}^{d} \delta_\ell = 1,
\]

and (2) by \( q^2 \) so that:

\[
\sum_{\ell=1}^{d-1} \sum_{\ell=1}^{d} \delta_\ell\delta_{\ell+1} \geq \kappa (d-1),
\]

where

\[
\kappa = (A/q^2 - (p-1)/d\eta^2)/(d-1).
\]

The density of power residues and non-residues

We attempt a solution to (4) and (5) (with "\( = n \)" by setting

\[
\delta_1 = u, \quad \delta_2 = \delta_3 = \ldots = \delta_d = v.
\]

Then (4), (5) become:

\[
u + (d-1)\nu = 1, \quad 2uv + (d-2)\nu^2 = \kappa,
\]

which may be solved:

\[
u = (1 + (d-1)(1 - \delta_0)/d)^{1/2}/d,
\]

\[
v = (1 - (1 - \delta_0)^2)/d.
\]

(5) may be written:

\[
\left(\sum_{\ell=1}^{d} \delta_\ell^2 \right) - \left(\sum_{\ell=1}^{d} \delta_\ell \right) \geq \kappa (d-1),
\]

and by (4):

\[
\sum_{\ell=1}^{d} \delta_\ell^2 \leq 1 - (d-1)\kappa.
\]

Let us attempt to find real numbers \( a_1, ..., a_d \) such that:

\[
\delta_1 = u + a_1; \quad \delta_2 = v + a_2; \quad \delta_3 = \ldots = \delta_d = v,
\]

then because of (4) and the equations for \( u \) and \( v \):

\[
\sum_{\ell=1}^{d} a_\ell = 0,
\]

and (8) becomes:

\[
u^2 + (d-1)\nu^2 + 2u a_1 + 2v \sum_{\ell=1}^{d} a_\ell + \sum_{\ell=1}^{d} a_\ell^2 \leq 1 - (d-1)\kappa.
\]

By (6) and (7), (11) becomes:

\[
2u a_1 + 2v \sum_{\ell=1}^{d} a_\ell + \sum_{\ell=1}^{d} a_\ell^2 \leq 0,
\]

so:

\[
2u a_1 + 2v \sum_{\ell=1}^{d} a_\ell \leq 0.
\]

By (10) this is \( 2u a_1 - 2v a_1 \leq 0 \), but \( a_1 - v > 0 \), so \( a_1 \leq 0 \). Hence, by (9) and (6), we have the desired result for \( \delta_1 \). However, the argument is entirely the same for each of the remaining \( \delta_0 \)s, so the theorem is established.

Probably the most interesting special cases of this theorem are obtained when \( d = 2 \) and \( q = \sqrt{p} \). The following corollaries treat these and will furnish an example of how the theorem may be applied.
Corollary 1. If $h$ is such that 

$$1 > h^4 > \pi^2/12$$

and $q = h \sqrt{p}$ is a positive integer, and $s$ denotes the number of quadratic residues or non-residues (mod $p$) in $[1, q]$, then:

$$s/q > (1 - (1 - 12/\pi^2) + 1/h^2)^{1/2} + o(1).$$

Proof. In the theorem, $d = 2$ and $n$ necessarily is 1. Since $1 - \delta_1 = \delta_1, 1 - \delta_0 = \delta_0$, we have:

$$
\delta_1, \delta_0 > 1 + \left(1 - 12/\pi^2 + 1/\delta_1^{1/2}\right)^{1/2} + o(1),
$$

which is the corollary.

Corollary 2. The density of quadratic residues or non-residues in $[1, \sqrt{p}]$ is $> 0.42$.

Proof. Choose $h = \sqrt{p}/\sqrt{p}$ in Corollary 1 so that:

$$1 < 1/h^2 < 1 + 1/\sqrt[p]{p} + 1/\sqrt[p]{p},$$

and observe that:

$$\lim_{p \to \infty} 2/\sqrt[p]{p} + 1/\sqrt[p]{p} = 0,$$

so these terms may be absorbed into the $o(1)$. The rest is computation.

Note: The author wishes to express his appreciation to A. Schinzel for pointing out a superficial hypothesis in the theorem to him. Professor Schinzel also indicated a way of strengthening the theorem’s conclusion, once this hypothesis was removed.

References


Reçu par la Rédaction le 31. 5. 1967