ACTA ARITHMETICA
XIV (1968)

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

by

Clifton T. Whyburn (Baton Rouge, La.)

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

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

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

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

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* $(\bmod p)$ *in the interval $[1, \sqrt{p}]$ is greater than $1/(4+2\sqrt{2})$ $(= 1/6{,}828\ldots)$.*

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 {[2], p. 131} formula:

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

Theorem. *Let d be a positive integer, such that $d \mid p-1$ and $d \geqslant 2$. Let h be such that $q = h\sqrt{p}$ is a positive integer and*

$$1 > h^2 > \pi^2/6d.$$

Denote by C_0 the set of d-th power residues $(\bmod p)$ *and define the classes $C_1, C_2, \ldots, C_{d-1}$ by $x, y \in C_j$ if x and y are prime to p and their quotient*

icm©

is congruent an element of C_0 (mod$p$). *If* ν_i *is the number of elements of* C_i *in* $[1, q]$, *we have*:

$$\nu_i/q = \delta_i \leqslant \Big(1+(d-1)\big(1-6d/(\pi^2(d-1))+1/((d-1)h^2)\big)^{1/2}\Big)/d+o(1).$$

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

$$A = 2\sum_{j=1}^{q}\varphi(j)-1 = 6q^2/\pi^2+O(q\log q), \tag{1}$$

where φ is Euler's function.

Let us define ν_i for $i \geqslant d$ by $\nu_i = \nu_j$ if $i \equiv j$ (mod d). One may then form

$$\sum_{i=1}^{d} \nu_i\nu_{i+t}$$

fractions which are congruent elements of C_t (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 $1 \leqslant a, b \leqslant q < \sqrt{p}$, and $(a, b) = 1$, no two are congruent (mod$p$). Even if these fractions represent all $(p-1)/d$ elements of C_0, they will still represent $A-(p-1)/d$ elements of $C_1 \cup C_2 \cup \ldots \cup C_{d-1}$. Further, since p is large, and by the lower bound on h, we have:

$$A-(p-1)/d > 0,$$

and certainly:

$$\sum_{j=1}^{d-1}\sum_{i=1}^{d} \nu_i\nu_{i+j} \geqslant A-(p-1)/d. \tag{2}$$

There is the additional condition:

$$\sum_{i=1}^{d} \nu_i = q. \tag{3}$$

We may divide (3) through by q to obtain

$$\sum_{i=1}^{d} \delta_i = 1, \tag{4}$$

and (2) by q^2 so that:

$$\sum_{j=1}^{d-1}\sum_{i=1}^{d} \delta_i\delta_{i+j} \geqslant \varkappa(d-1), \tag{5}$$

where

$$\varkappa = \big(A/q^2-(p-1)/dq^2\big)/(d-1).$$

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

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

Then (4), (5) become:

$$u+(d-1)v = 1, \quad 2uv+(d-2)v^2 = \varkappa,$$

which may be solved:

$$u = \big(1+(d-1)(1-d\varkappa)^{1/2}\big)/d, \tag{6}$$

$$v = \big(1-(1-d\varkappa)^{1/2}\big)/d. \tag{7}$$

(5) may be written:

$$\Big(\sum_{j=1}^{d}\delta_j\Big)^2 - \sum_{j=1}^{d}\delta_j^2 \geqslant \varkappa(d-1),$$

and by (4):

$$\sum_{j=1}^{d}\delta_j^2 \leqslant 1-(d-1)\varkappa. \tag{8}$$

Let us attempt to find real numbers $a_1, \ldots, a_d$ such that:

$$\delta_1 = u+a_1; \quad \delta_i = v+a_i, \quad i = 2, \ldots, d, \tag{9}$$

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

$$\sum_{i=1}^{d} a_i = 0, \tag{10}$$

and (8) becomes:

$$u^2+(d-1)v^2+2ua_1+2v\sum_{i=2}^{d}a_i+\sum_{i=1}^{d}a_i^2 \leqslant 1-(d-1)\varkappa. \tag{11}$$

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

$$2ua_1+2v\sum_{i=2}^{d}a_i+\sum_{i=1}^{d}a_i^2 \leqslant 0,$$

so:

$$2ua_1+2v\sum_{i=2}^{d}a_i \leqslant 0.$$

By (10) this is $2ua_1-2va_1 \leqslant 0$, but $u-v > 0$, so $a_1 \leqslant 0$. Hence, by (9) and (6), we have the desired result for δ_1. However, the argument is entirely the same for each of the remaining δ'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 two corollaries treat these and will furnish an example of how the theorem may be applied.

COROLLARY 1. *If h is such that*

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

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*:

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

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

$$\delta_1, \delta_0 \geqslant 1-\big(1+(1-12/\pi^2+1/h^2)^{1/2}\big)/2+o(1),$$

which is the corollary.

COROLLARY 2. *The density of quadratic residues or non-residues in* $[1, [\sqrt{p}]]$ *is* $\geqslant .042$.

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

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

and observe that:

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

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 superfluous hypothesis in the theorem to him. Professor Schinzel also indicated a way of strengthening the theorem's conclusion, once this hypothesis was removed.

References

[1] K. F. Gauss, *Disquisitiones arithmeticae*, Yale University Press, 1966.
[2] T. Nagell, *Introduction to number theory*, Stockholm 1951.
[3] L. Rédei, *Über die Anzahl der Potenzreste* mod$p$ *im Intervall* $1, \sqrt{p}$, Nieuw Arch. Wisk. (2) 23 (1950), pp. 150-162.

Reçu par la Rédaction le 31. 5. 1967

LIVRES PUBLIÉS PAR L'INSTITUT MATHÉMATIQUE DE L'ACADÉMIE POLONAISE DES SCIENCES

Z. Janiszewski, Oeuvres choisies, 1962, p. 320, $ 5.00.
J. Marcinkiewicz, Collected papers, 1964, p. 673, $ 10.00.
S. Banach, Oeuvres, vol. I, 1967, p. 381, $ 10.00.

MONOGRAFIE MATEMATYCZNE

10. S. Saks i A. Zygmund, Funkcje analityczne, 3-ème éd., 1959, p. VIII+431, $ 4.00.
20. C. Kuratowski, Topologie I, 4-ème éd., 1958, p. XII+494, $ 8.00.
21. C. Kuratowski, Topologie II, 3-ème éd., 1961, p. IX+524, $ 8.00.
27. K. Kuratowski i A. Mostowski, Teoria mnogości, 2-ème éd. augmentée, 1966, p. 376, $ 5.00.
28. S. Saks and A. Zygmund, Analytic functions, 2-ème éd. augmentée, 1965, p. IX+508, $. 10.00.
30. J. Mikusiński, Rachunek operatorów, 2-ème éd., 1957, p. 375, $ 4.50.
31. W. Ślebodziński, Formes extérieures et leurs applications I, 1954, p. VI+154, $ 3.00.
34. W. Sierpiński, Cardinal and ordinal numbers, 2-ème éd., 1965, p. 492, $ 10.00.
35. R. Sikorski, Funkcje rzeczywiste I, 1958, p. 534, $ 5.50.
36. K. Maurin, Metody przestrzeni Hilberta, 1959, p. 363, $ 5.00.
37. R. Sikorski, Funkcje rzeczywiste II, 1959, p. 261, $ 4.00.
38. W. Sierpiński, Teoria liczb II, 1959, p. 487, $ 6.00.
39. J. Aczél und S. Gołąb, Funktionalgleichungen der Theorie der geometrischen Objekte, 1960, p. 172, $ 4.50.
40. W. Ślebodziński, Formes extérieures et leurs applications II, 1963, p. 271, $ 8.00.
41. H. Rasiowa and R. Sikorski, The mathematics of metamathematics, 1963, p. 520, $ 12.00.
42. W. Sierpiński, Elementary theory of numbers, 1964, p. 480, $ 12.00.
43. J. Szarski, Differential inequalities, 2-ème éd., 1967, p. 256, $ 9.00.
44. K. Borsuk, Theory of retracts, 1967, p. 251, $ 9.00.
45. K. Maurin, Methods of Hilbert spaces, 1967, p. 552, $ 12.00.
46. M. Kuczma, Functional equations in a single variable, 1968, p. 383, $ 9.00.

LES DERNIERS FASCICULES DES DISSERTATIONES MATHEMATICAE

LVI. A. Szybiak, Covariant differentiation of geometric objects, 1967, p. 1-41, $ 1.00.
LVII. J. Słomiński, Peano-algebras and quasi-algebras, 1968, p. 1-60, $ 1.50.
LVIII. A. Pełczyński, Linear extensions, linear averagings, and their applications to linear topological classification of spaces of continuous functions, 1968, p. 1-92, $ 2.50.
LIX. A. Śniatycki, An axiomatics of non-Desarguean geometry based on the half-plane as the primitive notion, 1968, p. 1-45, $ 1.00.
LX. S. Trybuła, Sequential estimations in processes with independent increments, 1968, p. 1-49, $ 1.00.