THE DISTRIBUTION OF QUADRATIC RESIDUES AND NON-RESIDUES

D. A. Burgess

1. If p is a prime other than 2, half of the numbers

$$1,\ 2,\ \dots,\ p-1$$

are quadratic residues (mod p) and the other half are quadratic non-residues. Various questions have been proposed concerning the distribution of the quadratic residues and non-residues for large p, but as yet only very incomplete answers to these questions are known. Many of the known results are deductions from the inequality

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

found independently by Pólya* and Vinogradov†, the symbol $\left(\frac{n}{p}\right)$ being Legendre's symbol of quadratic character.

My object in the present paper is to prove an inequality which in some respects goes further than (1), and to make a few deductions from it. The result in question is:

Theorem 1. *Let δ and ϵ be any fixed positive numbers. Then, for all sufficiently large p and any N, we have*

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

provided

$$H > p^{\frac{1}{4}+\delta}. \tag{3}$$

This implies, in particular, that *the maximum number of consecutive quadratic residues or non-residues* (mod p) *is $O(p^{\frac{1}{4}+\delta})$ for large p.* Previously it was known‡ only that the number is $O(p^{1/2})$.

Theorem 1 enables me to improve on Vinogradov's estimate§ for the magnitude of the least (positive) quadratic non-residue (mod p). Using

---

* G. Pólya, " Über die Verteilung der quadratischen Reste und Nichtreste ", *Göttinger Nachrichten* (1918), 21–29.

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

‡ H. Davenport and P. Erdös, " The distribution of quadratic and higher residues ", *Publicationes Mathematicae* (Debrecen), 2 (1952), 252–265.

§ I. M. Vinogradov, " On a general theorem concerning the distribution of the residues and non-residues of powers ", *Trans. American Math. Soc.*, 29 (1927), 209–217.

[Mathematika 4 (1957), 106–112]

(1), he proved that this least quadratic non-residue is $O(p^{\alpha})$ for any fixed $\alpha > \frac{1}{2}e^{-1/2}$. Using Theorem 1 instead, but otherwise following Vinogradov's argument, I prove:

THEOREM 2. *Let d denote the least positive quadratic non-residue* (mod p). *Then $d = O(p^{\alpha})$ as $p \to \infty$, for any fixed $\alpha > \frac{1}{4}e^{-1/2}$.*

The result of Theorem 1 can be made more explicit, in that the right-hand side of (2) can be replaced by a particular function of p, H, δ. The result can also be extended to characters other than the quadratic character. These further results, which will form the subject-matter of a later paper, have enabled me to improve also on Vinogradov's estimate* $O(p^{\frac{1}{2}+\delta})$ for the least primitive root (mod p).

The starting point for all this work is an estimate (Lemma 2 below) which was mentioned by Davenport and Erdös (*loc. cit.*, footnote on p. 262) and which is a consequence of A. Weil's proof of the analogue of the Riemann Hypothesis for algebraic function-fields over a finite field.

I take this opportunity of thanking Prof. Davenport for much valuable advice, and also for preparing the final draft of the paper.

2. LEMMA 1. *Let $f(x)$ be a polynomial of odd degree ν with integral coefficients and highest coefficient* 1. *Suppose that $f(x)$ is square-free* (mod p), *that is, that there is no identity of the form $f(x) \equiv \big(g(x)\big)^2 f_1(x)$* (mod p) *with polynomials $g(x)$, $f_1(x)$, where $g(x)$ is not a constant. Then*

$$\left| \sum_x \left(\frac{f(x)}{p}\right) \right| \leqslant (\nu - 1) p^{1/2}, \tag{4}$$

where the summation is over a complete set of residues (mod p).

Proof. The result is a consequence of A. Weil's theorem† that the congruence zeta-function for the algebraic function-field generated by the equation $y^2 = f(x)$, over the finite field of p elements, has all its roots on the critical line. This congruence zeta-function has the same roots as the congruence L-function‡

$$L(s) = 1 + \sigma_1 p^{-s} + \ldots + \sigma_{\nu-1} p^{-(\nu-1)s},$$

where
$$\sigma_1 = \sum_x \left(\frac{f(x)}{p}\right).$$

---

* See E. Landau, *Vorlesungen über Zahlentheorie* II, 178–180.

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

‡ See H. Hasse, "Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper", *Journal für Math.*, 172 (1935), 37–54.

Thus, if $s_1, \ldots, s_{\nu-1}$ are the roots of the congruence zeta-function (distinct in the obvious sense), we have

$$-\sigma_1 = p^{s_1} + \ldots + p^{s_{\nu-1}}.$$

Weil's theorem is that $\mathscr{R}s_j = \frac{1}{2}$ for each j, and the conclusion follows.

LEMMA 2. *Let r be a positive integer, let p be a prime, and let h be any integer satisfying $0 < h < p$. Let*

$$S_h(x) = \sum_{m=1}^{h} \left(\frac{x+m}{p}\right). \tag{5}$$

Then
$$\sum_x \left(S_h(x)\right)^{2r} < (2r)^r p h^r + r(2p^{1/2}+1)\, h^{2r}. \tag{6}$$

Proof. We follow the argument of Davenport and Erdös (*loc. cit.*, Lemma 3). We have

$$\sum_x \left(S_h(x)\right)^{2r} = \sum_{m_1=1}^{h} \ldots \sum_{m_{2r}=1}^{h} \sum_x \left(\frac{(x+m_1)\ldots(x+m_{2r})}{p}\right).$$

Divide the sets of values of $m_1, \ldots, m_{2r}$ into two classes, putting in the first class those which consist of at most r distinct integers, each occurring an even number of times, and putting into the second class all other sets. The number of sets in the first class is less than $(2r)^r h^r$, and for each set the inner sum over x is at most p. Hence the contribution made by the sets of the first class is less than $(2r)^r p h^r$.

The number of sets in the second class is at most h^{2r} (trivially). For each set of the second class, the inner sum over x is of the form

$$\sum_x \left(\frac{(x+n_1)^{e_1}\ldots(x+n_s)^{e_s}}{p}\right),$$

where $s \leqslant 2r$ and $n_1, \ldots, n_s$ are mutually incongruent $(\bmod\, p)$ and $e_1, \ldots, e_s$ are not all even. We can omit those factors $(x+n_j)^{e_j}$ for which e_j is even, provided we make an allowance of at most r for those values of x for which $x \equiv -n_j \pmod p$ for some j. We can also replace the odd exponents e_j by 1. Thus the above sum differs by at most r from a sum of the form

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

where $1 \leqslant k \leqslant 2r$ and $u_1, \ldots, u_k$ are mutually incongruent $(\bmod\, p)$. The polynomial

$$f(x) = (x+u_1)\ldots(x+u_k)$$

is square-free $(\bmod\, p)$ in the sense of Lemma 1, and if k is odd it follows from that Lemma that

$$|S| \leqslant (k-1)p^{1/2} < 2r\,p^{1/2}.$$

This holds also if k is even, for the transformation from x to y defined by

$$(x+u_1)y \equiv 1 \pmod{p}$$

changes the sum S into a similar sum with $k-1$ factors instead of k factors, together with a term -1 arising from the fact that $y \equiv 0$ does not correspond to any x. Thus, when k is even, we get

$$|S| \leqslant 1+(k-2)p^{1/2} < (k-1)p^{1/2} < 2rp^{1/2},$$

as before.

Putting together the results proved, we obtain (6).

3. For any integers $H>0$, $q>0$, t, N we define the interval $I(q, t)$ to consist of all real z satisfying

$$\frac{N+tp}{q} < z \leqslant \frac{N+H+tp}{q}. \tag{7}$$

LEMMA 3. *Let q run through a set of distinct positive integers, Q in number, all satisfying*

$$q_1 < q < q_2, \tag{8}$$

and all relatively prime in pairs. Suppose that

$$2Hq_2 < p. \tag{9}$$

Then (for given p, N, H) it is possible to associate with each q a set $T(q)$ of integers t, with $0 \leqslant t < q$, their number being $q-Q$, in such a way that the intervals $I(q, t)$, for all q and all t in $T(q)$, are disjoint.

Proof. We observe first that two of the intervals (7) with the same q but different t are always disjoint, since $0 < H < p$.

Now suppose that the intervals $I(q, t)$ and $I(q', t')$ have a point in common, where $q > q'$. Then

$$\frac{N+tp}{q} < \frac{N+H+t'p}{q'} \quad \text{and} \quad \frac{N+t'p}{q'} < \frac{N+H+tp}{q},$$

whence
$$p(tq'-t'q)+N(q'-q) < Hq,$$
$$p(tq'-t'q)+N(q'-q) > -Hq'.$$

Hence
$$|p(tq'-t'q)+N(q'-q)| < Hq < \tfrac{1}{2}p,$$

by (9). This inequality shows that, for any particular pair q, q', there is at most one value for $tq'-t'q$. Since $0 \leqslant t < q$ and $0 \leqslant t' < q'$, and since q, q' are relatively prime, it follows that there is at most one pair t, t'.

We construct the set $T(q)$ for each q by removing from the set $0 \leqslant t < q$ all those values of t which occur in any pair t, t', corresponding to any $q' \neq q$. The number of values of t removed in this way is at most $Q-1$, hence we can construct the sets $T(q)$ so that each of them contains $q-Q$ numbers t.

4. *Proof of Theorem* 1. It suffices to prove the inequality (2), for any N, on the assumption that

$$p^{\frac{1}{4}+\delta} < H < p^{\frac{1}{2}+\delta}; \tag{10}$$

for if $H > p^{\frac{1}{2}+\delta}$ the conclusion follows from (1).

We suppose that

$$\left| \sum_{n=N+1}^{N+H} \left(\frac{n}{p}\right) \right| \geqslant \epsilon H \tag{11}$$

for some N and some H satisfying (10), and deduce a contradiction if p is sufficiently large.

For any positive integer $q < p$, we have

$$\sum_{n=N+1}^{N+H} \left(\frac{n}{p}\right) = \sum_{t=0}^{q-1} \sum_{\substack{n=N+1 \\ n \equiv -tp \ (\mathrm{mod}\ q)}}^{N+H} \left(\frac{n}{p}\right).$$

Putting $n = -tp+qz$ in the inner sum, the conditions on z are

$$\frac{N+1+tp}{q} \leqslant z \leqslant \frac{N+H+tp}{q}.$$

Thus z runs through the integers of the interval $I(q, t)$ defined in (7). Since

$$\left(\frac{n}{p}\right) = \left(\frac{qz}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{z}{p}\right),$$

it follows from (11) that

$$\epsilon H \leqslant \sum_{t=0}^{q-1} \left| \sum_{z \in I(q,t)} \left(\frac{z}{p}\right) \right|. \tag{12}$$

We now apply Lemma 3, taking the set of integers q in that Lemma to consist of all the primes in the interval

$$\tfrac{1}{2}p^{1/4} < q < p^{1/4}. \tag{13}$$

The condition (9) is amply satisfied, by (10). The number of integers q is Q, given by

$$Q = \pi(p^{1/4}) - \pi(\tfrac{1}{2}p^{1/4}). \tag{14}$$

Summing (12) over the primes q in question, we obtain

$$\epsilon HQ \leqslant \sum_q \sum_{t=0}^{q-1} \left| \sum_{z \in I(q,t)} \left(\frac{z}{p}\right) \right| \leqslant \sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \left(\frac{z}{p}\right) \right| + \sum_q Q \,.\, 2Hq^{-1},$$

since the number of integers z in $I(q, t)$ is less than $2Hq^{-1}$ and since all but Q of the values of t belong to $T(q)$. Since $\Sigma q^{-1} < 2p^{-1/4}Q$ by (13), we have

$$\sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \left(\frac{z}{p}\right) \right| > HQ(\epsilon - 4p^{-1/4}Q) > \tfrac{1}{2}\epsilon HQ$$

for large p, since $Q = o(p^{1/4})$ by (14).

Let I denote the general interval $I(q, t)$. All these intervals are disjoint by Lemma 3, and their number is

$$\sum_q (q-Q) < p^{1/4} Q. \tag{15}$$

We can rewrite the last result as

$$\sum_I \left| \sum_{z \varepsilon I} \left(\frac{z}{p}\right) \right| > \tfrac{1}{2}\epsilon H Q. \tag{16}$$

For any positive integer h, we have

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

where $|\phi_m| \leqslant 2m$. Hence

$$\sum_{n \varepsilon I} \sum_{m=1}^{h} \left(\frac{n+m}{p}\right) = h \sum_{z \varepsilon I} \left(\frac{z}{p}\right) - \sum_{m=1}^{h} \phi_m.$$

Thus, with the notation of (5), we have

$$\sum_{n \varepsilon I} |S_h(n)| \geqslant h \left| \sum_{z \varepsilon I} \left(\frac{z}{p}\right) \right| - 2h^2.$$

Summing over I and using the estimate (15) for the number of intervals I, we deduce from (16) that

$$\sum_I \sum_{n \varepsilon I} |S_h(n)| > \tfrac{1}{2}\epsilon H Q h - 2p^{1/4} Q h^2.$$

Take
$$h = [\tfrac{1}{8}\epsilon H p^{-1/4}]; \tag{17}$$
then
$$\sum_I \sum_{n \varepsilon I} |S_h(n)| > \tfrac{1}{4}\epsilon H Q h.$$

By Hölder's inequality,

$$\sum_I \sum_{n \varepsilon I} |S_h(n)| \leqslant \left\{ \sum_I \sum_{n \varepsilon I} 1 \right\}^{1-1/2r} \left\{ \sum_I \sum_{n \varepsilon I} |S_h(n)|^{2r} \right\}^{1/2r},$$

whence

$$\sum_I \sum_{n \varepsilon I} |S_h(n)|^{2r} > (\tfrac{1}{4}\epsilon H Q h)^{2r} (p^{1/4} Q \,.\, 3p^{-1/4} H)^{1-2r},$$

on recalling that the number of integers in any interval I is at most $3p^{-1/4} H$. Since the intervals I are disjoint, it follows that

$$\sum_x |S_h(x)|^{2r} > (\tfrac{1}{12}\epsilon)^{2r} H Q h^{2r}.$$

Comparing this with the result of Lemma 2, we obtain

$$(\tfrac{1}{12}\epsilon)^{2r} H Q h^{2r} < (2r)^r p h^r + 3r p^{1/2} h^{2r}.$$

Now $Q > C p^{1/4} (\log p)^{-1}$ with some positive absolute constant C, by (14). Since $H > p^{\frac{1}{4}+\delta}$, the left-hand side is large compared with the second term on the right, for any fixed r, if p is sufficiently large. Further, if we choose $r > \delta^{-1}$, then, since

$$h > \tfrac{1}{9}\epsilon p^{\delta}$$

by (17), we have

$$h^r > (\tfrac{1}{9}\epsilon)^r p,$$

and this makes the left-hand side large compared with the first term on the right. Thus we have a contradiction, and this establishes the result.

5. *Proof of Theorem* 2. Since $\frac{1}{4}e^{-1/2} = 0.15\ldots > \frac{1}{8}$, we can suppose, on taking $H = [p^{\frac{1}{4}+\delta}]$, that $H < d^2$. Then every quadratic non-residue (mod p) up to H has a prime factor q which is a quadratic non-residue, and this prime is at least d. Since the number of multiples of q not exceeding H is $[Hq^{-1}]$, we have

$$\sum_{n=1}^{H} \left(\frac{n}{p}\right) \geqslant H - 2 \sum_{d \leqslant q \leqslant H} [Hq^{-1}] > H\left\{1 - 2 \sum_{d \leqslant q \leqslant H} q^{-1}\right\},$$

the summation being over primes q.

It follows from Theorem 1, with $N = 0$, that

$$1 - 2 \sum_{d \leqslant q \leqslant H} q^{-1} < \epsilon,$$

that is,

$$\sum_{d \leqslant q \leqslant H} q^{-1} > \tfrac{1}{2}(1-\epsilon).$$

By a well-known result, the sum on the left is

$$\log\log H - \log\log d + o(1)$$

as $p \to \infty$. Putting $d = H^{1/\beta}$, we obtain

$$\log \beta > \tfrac{1}{2} - \epsilon$$

for all sufficiently large p, and since $H = [p^{\frac{1}{4}+\delta}]$ the result follows.

Department of Mathematics,
University College,
London.

(*Received* 18*th September*, 1957.)