Communicated 26 October 1955 by T. Nagell

A theorem concerning the least quadratic residue and non-residue

By Lars Fjellstedt

The purpose of this paper is to prove the following

Theorem: *Denote by* $\psi^*(p;2)$ *the least odd prime number which is quadratic non-residue modulo the prime* p. *Then for* $p > p_0$

$$\psi^*(p;2) < 6 \cdot \log p.$$

Denote by $\pi^*(p;2)$ *the least odd prime number which is quadratic residue modulo the prime* p. *Then for* $p > p_0$

$$\pi^*(p;2) < 6 \cdot \log p.$$

We shall require the following result which we do not prove:

Lemma. *If the system*

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \ldots, \quad x \equiv b_k \pmod{m_k}, \quad b_i \geqq 0,$$

is solvable, its positive solutions are given by

$$x = b_1 + m_1 t_1 + \frac{m_1 m_2}{d_1} t_2 + \cdots + \frac{m_1 m_2 \cdots m_{k-1}}{d_1 d_2 \cdots d_{k-2}} t_{k-1} + \frac{m_1 m_2 \cdots m_k}{d_1 d_2 \cdots d_{k-1}} t,$$

where

$$d_1 = (m_1, m_2), \quad d_i = \left(\frac{m_1 m_2 \cdots m_i}{d_1 \cdots d_{i-1}}, m_{i+1}\right), \quad i = 2, 3, \ldots, k-1,$$

$$0 \leqq t_i < \frac{m_{i+1}}{d_i}$$

and $t \geqq 0$ *an integer.*

Proof of the theorem. If we assume $\psi^*(p;2) = p_n$, p_m denoting the mth prime in the sequence $2, 3, 5, 7, \ldots, p$ satisfies

$$\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \cdots = \left(\frac{p_{n-1}}{p}\right) = +1, \quad \left(\frac{p_n}{p}\right) = -1. \tag{1}$$

Thus

$$p \equiv 1, 11 \pmod{12}, \quad p \equiv 1, 4 \pmod 5, \text{ etc.} \ldots$$

Putting $N = 3 \cdot 5 \cdot 7 \cdots p_n$, there exist $\nu = \varphi(N)/2^{n-1}$ integers a_i with

$$0 < a_i < 4N, \quad (a_i, 4N) = 1, \quad i = 1, 2, \ldots, \nu$$

and with the property that every prime p satisfying (1) belongs to one of the arithmetical progressions

$$4Nt + a_1, \quad 4Nt + a_2, \ldots, 4Nt + a_\nu.$$

If we choose for each of the primes $p_i, i = 2, 3, \ldots, n$, one of the possible congruence conditions modulo p_i or $4p_i$, we get exactly one residue class modulo $4N$ which is therefore one of the numbers a_k. Let us assume that we have chosen x_0, $0 < x_0 < 4N$, such that

$$x_0 \equiv b_2 \pmod{p_2^*}, \quad x_0 \equiv b_3 \pmod{p_3^*}, \ldots, \quad x_0 \equiv b_n \pmod{p_n^*}, \quad b_i > 0,$$

where

$$p_i^* = \begin{cases} p_i \text{ for } p_i \equiv 1 \pmod 4, \\ 4p_i \text{ for } p_i \equiv 3 \pmod 4. \end{cases}$$

We may of course assume that this system is solvable. Putting $b = \text{Min}(b_2, b_3, \ldots, b_n)$ and assuming that $b_{i_1}, b_{i_2}, \ldots, b_{i_k}$ are all the integers b_i for which

$$b_{i_1} = b_{i_2} = \cdots = b_{i_k} = b,$$

and putting also

$$P = p_{i_1} \cdot p_{i_2} \cdots p_{i_k}$$

and

$$P^* = \begin{cases} P \text{ if } p_{i_m} \equiv 1 \pmod 4, \quad m = 1, 2, \ldots, k, \\ 4P \text{ otherwise,} \end{cases}$$

we have

$$x_0 \equiv b \pmod{P^*}.$$

If we put $P \cdot Q = N$ when $Q > 1$, and define

$$Q^* = \begin{cases} Q \text{ if } p_j \equiv 1 \pmod 4 \text{ when } p_j/Q, \\ 4Q \text{ otherwise,} \end{cases}$$

we also have, according to the lemma,

$$x_0 \equiv a \pmod{Q^*},$$

where a is an integer such that $b < a < Q^*$. Using the lemma once more we get

$$\begin{cases} x_0 = b + P^* t_0, \quad 0 < t_0 < \dfrac{Q^*}{(P^*, Q^*)} \\ x_0 = a + Q^* t_1, \quad 0 \leq t_1 < \dfrac{P^*}{(P^*, Q^*)}. \end{cases}$$

If $t_1 > 0$ it follows from

$$PQ = 4N \cdot (P^*, Q^*)$$

that

$$x_0 > \sqrt{4N}. \tag{2}$$

If $t_1 = 0$ we proceed in the following way. The number k of different prime factors in P is either $\geqq n/3$ or it is $< n/3$. If $k \geqq n/3$, we have for $s = [n/3]$

$$x_0 > P^* \geqq p_1 p_2 \cdots p_s. \tag{3}$$

Assuming next that $k < n/3$ we define for all possible combinations of r different prime factors $p_{i_{\mu_q}}$, $q = 1, 2, \ldots, r$, of Q

$$Q(i_{\mu_1}, i_{\mu_2}, \ldots, i_{\mu_r}) = \frac{Q}{p_{i_{\mu_1}} \cdot p_{i_{\mu_2}} \cdots p_{i_{\mu_r}}}$$

and

$$Q^*(i_{\mu_1}, \ldots, i_{\mu_r}) = \begin{cases} Q(i_{\mu_1}, \ldots, i_{\mu_r}) \text{ if this integer has only prime divisors } \equiv 1 \pmod 4, \\ 4Q(i_{\mu_1}, \ldots, i_{\mu_r}) \text{ otherwise.} \end{cases}$$

For these integers $Q^*(i_{\mu_1}, \ldots, i_{\mu_r})$ we have the congruences

$$x_0 \equiv c(i_{\mu_1}, \ldots, i_{\mu_r}) \pmod{Q^*(i_{\mu_1}, \ldots, i_{\mu_r})}, \qquad 0 < c(i_{\mu_1}, \ldots, i_{\mu_r}(< Q^*(i_{\mu_1}, \ldots, i_{\mu_r})$$

and ask for the least integer r with the property that for one $c(i_{\mu_1}, \ldots, i_{\mu_r})$ at least

$$x_0 > c(i_{\mu_1}, \ldots, i_{\mu_r}). \tag{4}$$

It is easy to see that $r \leqq [(n-k)/2]$. In fact, suppose we have two congruences

$$\begin{cases} x \equiv a \pmod A, & 0 < a < A \\ x \equiv b \pmod B, & 0 < b < B \end{cases} \quad a \neq b \tag{5}$$

where A and B are products of different primes and $(A, B) = 1$, and suppose that

$$x \equiv c \pmod{AB}, \qquad \max(a, b) < c < AB. \tag{6}$$

If the total number of prime factors in AB is m, one of the integers A and B contains $\leqq [m/2]$ prime factors. If we cancel, in all possible ways, $[m/2]$ prime factors of AB, thus obtaining new integers A^*, B^*, $(A, B^*) = (A^*, B) = 1$, then for at least one such pair we cannot have

$$x \equiv c \pmod{A^* B^*}, \quad 0 < c < A^* B^*,$$

with the same integer c as in (6). Since we may assume $x_0 > p_n$ (otherwise we should have $p > x_0 + 4N$), this argument obviously applies in our case.

Thus it follows that for a modulus $Q^*(i_{\mu_1}, \ldots, i_{\mu_r}) = Q^{**}$ with the property (4) we have

$$x_1 = c^* + T \cdot Q^{**}, \qquad T > 0.$$

Since the number of different prime factors in Q^{**} is at least

$$n - k - r > \frac{n}{3} - 1$$

we have, for $s = [n/3]$,

$$x_0 \geqq p_1 \cdot p_2 \cdots p_s \tag{7}$$

It results from (2), (3) and (7) that in all cases

$$x_0 > R = p_1 \cdot p_2 \cdots p_s.$$

If we had $Q = 1$, p would be $> 4N$.
From

$$\log R = \vartheta(p_s) > \frac{2}{3} p_s > \frac{2}{3} s \log s > \frac{1}{5} n \log n > \frac{1}{6} p_n, \qquad n > n_0,$$

we get

$$6 \cdot \log p > 6 \cdot \log x_0 > p_n.$$

Hence the first part of our theorem is proved.
Starting from

$$\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \cdots = \left(\frac{p_{n-1}}{p}\right) = -1, \quad \left(\frac{p_n}{p}\right) = +1$$

instead of starting from (1) the second part is obtained in exactly the same way.

The best results previously obtained concerning this question are the following:

$$\psi^*(p; 2) < p^{\lambda} (\log p)^2, \quad \lambda = \frac{1}{2\sqrt{e}}, \quad p \equiv \pm 1 \pmod 8 \quad \text{and } p > p_0.$$

This was proved by Vinogradov [1] in 1927. A. Brauer [2] and T. Skolem [6] proved using elementary methods

$$\psi^*(p; 2) < C \cdot p^{2/5}, \quad p \equiv \pm 3, -1 \pmod 8, \quad C \text{ a constant}.$$

In 1954 Ankeny [3] proved

$$\psi^*(p; 2) < p^{\varepsilon}, \quad \varepsilon > 0, \quad p \equiv 3 \pmod 4 \text{ and } p > p_0.$$

Using the extended Riemann hypothesis several authors, Linnik, Erdös, Ankeny etc., have obtained bounds for $\psi^*(p; 2)$. The best one of these results is, as far as I know, the following (Ankeny [4]):

$$\psi^*(p; 2) = 0((\log p)^2).$$

On the other hand it has been proved by Salié [5] and others that

$$\psi^*(p;2) > c \cdot \log p$$

$$\pi^*(p;2) > c \cdot \log p$$

for infinitely many primes p. Hence our result is in a sense the best possible.

Actually Salié proves only the first inequality. It is however easy to see that the second one can be proved by the same method.

REFERENCES

1. VINOGRADOV, On the bound of the least non-residue of nth powers. Trans. Amer. Math. Soc. *29*, 218–226 (1927).
2. BRAUER, A., Über den kleinsten quadratischen Nichrest. Math. Zeitschrift *33*, 161–176 (1931).
3. ANKENY, N. C., Quadratic residues. Duke Math. J. *21*, 107–112 (1954).
4. —— The least quadratic non-residue. Ann. of Math. (2) *55*, 65–72 (1952).
5. SALIÉ, H., Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl. Math. Nachr. *3*, 7–8 (1949).
6. SKOLEM, T., On the least odd positive quadratic non-residue modulo p. Det Kongel. Norske Vid. Selsk. Forh. *27*: 20 (1954).

Tryckt den 30 januari 1956

Uppsala 1956. Almqvist & Wiksells Boktryckeri AB