ARKIV FÖR MATEMATIK Band 3 nr 24

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

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