ON SETS OF THREE CONSECUTIVE INTEGERS WHICH ARE QUADRATIC RESIDUES OF PRIMES*
BY A. A. BENNETT

In this paper we shall prove the following theorems.

Theorem I. For each prime, p, for which there are as many as three incongruent squares, there is a set of three consecutive residues (admitting zero and negative numbers as residues) which are squares, modulo p.

Theorem II. For p = 11, and for each prime p greater than 17, (and for no other primes), there is a set of three consecutive least positive (non-zero) residues which are squares, modulo p.

The problem† of finding three consecutive integers which are quadratic residues of a prime, p, is equivalent to the formally more general problem of finding two quantities, x, y, (y ≠ 0), such that x, y, x + y, x − y, are proportional to squares in the domain,‡ since we then have \(\frac{x}{y} - 1, \frac{x}{y}, \frac{x}{y} + 1\) as consecutive squares in the domain. We may show that for residues with respect to a modulus the condition is equivalent to the existence of a square of the form§ \(uv(u + v)(u - v)\). By taking \(u = x, v = y\), we see that the condition is necessary.

* Presented to the Society, April 10, 1925.
† For references, compare article of similar title by H. S. Vandiver, this BULLETIN, vol. 31 (1925), p. 33.
‡ That, in the system of natural numbers, it is impossible to have distinct quantities, x, y, such that x, y, x + y, x − y are all proportional to squares was proved by Fermat by his celebrated method of "infinite descent". See Carmichael, Theory of Numbers, p. 86.
§ It is of interest to note that in the case of natural numbers we may take \(u = x\) and \(v = y\) for this relation. Indeed, if \(x, y, x + y, x - y\) were proportional to squares, certainly their product would be a square. Conversely, suppose that their product were a square. Then either \(x, y, x + y, x - y\) would all be relatively prime, or if
That it is also sufficient may be shown as follows. Take \( x = (u^2 + v^2)^2 \) and \( y = 4uv(u^2 - v^2) \). Now \( x \) may also be written in the form \( 4u^2v^2 - (u^2 - v^2)^2 \). Hence \( x + y = [2uv + (u^2 - v^2)]^2 \), and \( x - y = [2uv - (u^2 - v^2)]^2 \). Thus if \( uv(u^2 - v^2) \) is a perfect square, so also are \( x, y, x + y, \) and \( x - y \), when these are related in this manner.

The expression \( uv(u + v)(u - v) \) takes on the values \( 6^2 \cdot 5, 2^2 \cdot 6, 2^2 \cdot 30 \), for the choices of \((u, v)\) as \((5, 4), (3, 1), (5, 1)\), respectively. But at least one of the three numbers \( 5, 6, 30 \) is a quadratic residue of the prime \( p \) no matter how \( p \) is chosen. Hence there is always a choice of \( uv(u + v)(u - v) \) which is a non-zero quadratic residue for each prime \( p \) greater than 5. The corresponding solutions of the original problem are \((1/4, 5/4, 9/4), (1/24, 25/24, 49/24), (49/120, 169/120, 289/120)\). These numbers in turn are all different from zero for \( p = 11 \), or for \( p > 17 \), but not otherwise. Now every three consecutive residues no one of which is congruent to zero are congruent to a set of three consecutive least positive (non-zero) residues. Thus we establish the theorems announced.

There is no difficulty in obtaining linear forms, the primes within which are such that for each of these choices of \( p \), a preassigned number of consecutive residues shall be squares. Indeed, we have merely to select assigned numbers to be quadratic residues. Thus for \( p \) of the form \( 24k + 1 \) or \( 24k + 23 \), each of the numbers \( 1, 2, 3, 4 \) is a square. By choosing a form for which \( 2, 3, 5, 7, -1 \) are all quadratic residues, and dropping the condition of positivity, we have always the following twenty-one consecutive residues as squares, \(-10, -9, -8, \ldots, 9, 10\).

The University of Texas