ON SETS OF THREE CONSECUTIVE INTEGERS WHICH ARE QUADRATIC OR CUBIC RESIDUES OF PRIMES*

BY H. S. VANDIVER

1. *Introduction.* The problem of finding sets of two consecutive integers which are quadratic residues of a prime has been considered by a number of writers† from the point of view of finding integers x and y such that

$$x^2 \equiv y^2+1 \pmod{p}$$

p being a prime. I know of no references however, on the problem of finding three consecutive integers which are squares.

As to consecutive integers which are cubic residues, the congruence

$$x^3 \equiv y^3+1 \pmod{p}$$

has been studied,‡ but the problem of determining sets of three consecutive integers or sets in arithmetic progression which are cubic residues has apparently not been considered.

In the present note special results on such distribution of quadratic and cubic residues will be obtained.

2. *Three Consecutive Quadratic Residues.* It is known that

$$\frac{x^5-1}{x-1} \equiv 0 \pmod{p}$$

has solutions prime to 5 only when the prime $p \equiv 1 \pmod{5}$.

* Presented to the Society, December 29, 1923. The author was enabled to carry out this investigation through a grant from the Heckscher Foundation for the Advancement of Research, established by August Heckscher at Cornell University.

† See the references in Dickson, *History of the Theory of Numbers*, vol. 2, pp. 282–303 (These are included incidentally in the literature on representation of a number as the sum of four squares.)

‡ See Libri[24], Pellet[128–244], Dickson[199], Cornacchia[217], Mantel[277], Hurwitz[213], Schur[283], of Chapter 26 of vol. 2 of Dickson's *History*.

Under this assumption put $v=x+1/x$; then $(x^5-1)/(x-1)=0$ may be written $v^2+v-1=0$ and $v\equiv(-1\pm a)/2 \pmod{p}$ where $a^2\equiv 5 \pmod{p}$. From $v=x+1/x$ it follows that the congruence*

$$\frac{-1\pm a}{2}\equiv x+\frac{1}{x} \pmod{p}$$

has solutions in x. Hence the discriminant is a square modulo p, or there exists an integer u such that

$$\begin{aligned} 2u^2 &\equiv -5\pm a && \pmod{p},\\ 2u^2 &\equiv -a^2\pm a && \pmod{p},\\ -2au^2 &\equiv a^2(a\pm 1) && \pmod{p} \end{aligned} \tag{1}$$

and, using Legendre's quadratic residue symbol we have

$$\left(\frac{a\pm 1}{p}\right)=\left(\frac{-2a}{p}\right). \tag{2}$$

If p is of the form $5n-1$, then the congruence $x^2\equiv 5 \pmod{p}$ has a solution, but $(x^5-1)/(x-1)\equiv 0 \pmod{p}$ has no solution. Hence

$$\left(\frac{a\pm 1}{p}\right)=-\left(\frac{-2a}{p}\right); \tag{3}$$

(2) and (3) prove a proposition proposed as a problem in the AMERICAN MATHEMATICAL MONTHLY.†

From (1) we have $4u^2\equiv -10\pm 2a \pmod{p}$ for $p=5n+1$, but no such congruence holds for $p=5n-1$. Hence we have the following theorem.

THEOREM I. *If* $a^2\equiv 5 \pmod{p}$, *then*

$$\left(\frac{10+2a}{p}\right)=\left(\frac{10-2a}{p}\right)=\pm 1$$

according as p *is a prime of the form* $5n\pm 1$.

In (2), let p be a prime of the form $40k+11$. Then $(-2/p)=1$, and therefore

* The fraction m/n in a congruence stands for the integer z, where $zn\equiv m \pmod{p}$.

† Problem 152, vol. 15, 1908, p. 235.

$$\left(\frac{a+1}{p}\right)=\left(\frac{a}{p}\right)=\left(\frac{a-1}{p}\right)$$

and $a+1$, a and $a-1$ are successive integers which are all quadratic residues of p, or all quadratic non-residues. There are two roots of $x^2\equiv 5 \pmod{p}$, so if $(a/p)=-1$, then $(p-a)/p=1$, and we have therefore determined three successive integers which are all quadratic residues of p. If $p=40k+39$, we have by (3)

$$\left(\frac{a+1}{p}\right)=\left(\frac{a-1}{p}\right)=-\left(\frac{-2}{p}\right)\left(\frac{a}{p}\right)=\left(\frac{a}{p}\right)$$

and as before we may select a to be a quadratic residue of p. If $p=40n+1$, then

$$\left(\frac{a+1}{p}\right)=\left(\frac{a-1}{p}\right)=\left(\frac{a}{p}\right)$$

and these are not quadratic residues of p unless a is a quadratic residue of p, or in other words 5 is a biquadratic residue of p. Since p is of the form $40n+1$, it is not always possible to select a so that it is a quadratic residue. Similar remarks apply to the case $p=40n+29$. Hence we have the following theorem.

THEOREM II. *If p is of one of the forms $40k+1$, $40k+11$, $40k+29$, $40k+39$, then $a+1$, a, $a-1$ are all quadratic residues of p, where $a^2\equiv 5 \pmod{p}$ and 5 is a biquadratic residue of p. If p is of one of the two forms $40k+11$, $40k+39$, it is always possible to select a so that $(a/p)=1$. If p is one of the two forms $40k+1$, $40k+29$, then if one set $a+1$, a, $a-1$, exists then at least one other exists, namely $(p-a)+1$, $p-a$, $(p-a)-1$, having the desired property.*

In case we are testing the existence of sets in the case $p=40k+1$ or $40k+29$, and p is large, we may avoid the determination of a by the use of the law of biquadratic reciprocity,* which enables us to find the value of $(5/p)_4$.

* Smith, *Report on the theory of numbers*, COLLECTED WORKS, vol. 2, p. 77.

EXAMPLES: The three consecutive integers 3, 4, and 5 are quadratic residues of 11; also 19, 20, and 21 are quadratic residues of 79.

It is evident that we can also set up, by similar methods, theorems regarding integers a, $a+1$, $a+2$, modulo p, where each of these integers have prescribed quadratic characters.

3. *Cubic Residues.* We shall now discuss cubic residues. We shall first prove the following lemma.

LEMMA. *If p is an odd prime >3, and*

$$y^3+ay+b\equiv 0 \pmod{p} \tag{4}$$

where a, b, and y are integers, and also k is an integer not congruent to 0 (mod p) *such that*

$$R=\frac{b^2}{4}+\frac{a^3}{27}\equiv k^2 \pmod{p}$$

then

$$\left(-\frac{b}{2}+k\right) \text{ and } \left(-\frac{b}{2}-k\right)$$

are cubic residues modulo p.

To show this we follow a procedure analogous to that employed in Cardan's solution of the cubic. Let $y=u+v$; then (4) gives $3uv=-a$, $u^3+v^3=-b$. Assuming that y is an integer, then $u^2+2uv+v^2$ is an integer. Assuming $p>3$, then $3uv=-a$ shows that uv is congruent to an integer modulo p, hence u^2+v^2 has the same property, as well as u^2+uv+v^2. Also since $(u^3-v^3)^2=4R$ the same is true of u^3-v^3. Now $(u-v)(u^2+uv+v^2)=u^3-v^3$ and $k\not\equiv 0 \pmod{p}$, whence $u-v$ is congruent to an integer modulo p. Since $u+v$ is also, we have both u and v congruent to integers modulo p. Since $u^3=(-b/2+k)$ and $v^3=(-b/2-k)$ the lemma is proved.

We now apply the above result to the function

$$f(x)=x^3-3\lambda x-m\lambda \tag{5}$$

where λ is a prime,

$$4\lambda = m^2 + 27n^2, \quad m \equiv 1 \qquad (\mathrm{mod}\ 3).$$

We also have

$$f(x) = (x-\eta_1)(x-\eta_2)(x-\eta_3)$$

where

$$\eta_1 = \alpha \ + \alpha^{r^3} + \alpha^{r^6} + \cdots + \alpha^{r^{\lambda-4}},$$
$$\eta_2 = \alpha^{r} + \alpha^{r^4} + \alpha^{r^7} + \cdots + \alpha^{r^{\lambda-3}},$$
$$\eta_3 = \alpha^{r^2} + \alpha^{r^5} + \alpha^{r^8} + \cdots + \alpha^{r^{\lambda-2}},$$

$\alpha^{\lambda} = 1$, $\alpha \neq 1$, r a primitive root of λ. By a theorem of Kummer* we know that the congruence $f(x) \equiv 0\ (\mathrm{mod}\, p)$ always has solutions if $p^{(\lambda-1)/3} \equiv 1\ (\mathrm{mod}\ \lambda)$. Identifying (5) with (4) we have, since $a = -3\lambda$, $b = -m\lambda$,

$$R = \frac{-27n^2\lambda^2}{4}.$$

Now if p is a prime congruent to 1 or 7, modulo 12, then $(-3/p) = 1$, so that an integer k exists so that $k^2 \equiv R\ (\mathrm{mod}\, p)$. Put $j^2 \equiv -3\ (\mathrm{mod}\, p)$; then we may write

$$k \equiv \frac{j^3 n}{2} \qquad (\mathrm{mod}\, p),$$

so that, from the lemma,

$$\frac{\lambda m}{2} + \frac{n\lambda}{2} j^3, \qquad \frac{\lambda m}{2} - \frac{n\lambda}{2} j^3$$

are cubic residues of p.

Hence, if both $4\lambda m$ and $4\lambda n$ are cubic residues, so that $4\lambda m \equiv g^3$ and $4\lambda n j^3 \equiv h^3\ (\mathrm{mod}\, p)$, then

$$\left(\frac{g}{2}\right)^3 + \left(\frac{h}{2}\right)^3, \quad \left(\frac{g}{2}\right)^3, \quad \left(\frac{g}{2}\right)^3 - \left(\frac{h}{2}\right)^3$$

are all cubic residues and if $(h/2)f \equiv 1\ (\mathrm{mod}\ p)$ then, modulo p,

* Crelle, vol. 30 (1846), pp. 107–116.

$$\left(\frac{fg}{2}\right)^3+1, \quad \left(\frac{fg}{2}\right)^3, \quad \left(\frac{fg}{2}\right)^3-1$$

give a set of consecutive integers which are cubic residues. If either $4\lambda m$ or $4\lambda n$ is a cubic residue then we may find three cubic residues in arithmetic progression. Noting that if s is a cubic residue of p then $(-s)$ is also, and

$$\frac{n\lambda}{2}j^3-\frac{\lambda m}{2}$$

is a cubic residue, the result follows easily. We may then state the following theorem.

THEOREM. *If λ is a prime,*

$$\lambda=\frac{m^2+27n^2}{4}, \quad m\equiv 1 \pmod 3, \quad p\equiv 1 \text{ or } 7 \pmod{12},$$

$p^{(\lambda-1)/3}\equiv 1 \pmod \lambda$ *and if* $4\lambda m$ *or* $4\lambda n$ *is a cubic residue of* p *then it is possible to find three cubic residues of* p *in arithmetic progression. If both* $4\lambda m$ *and* $4\lambda n$ *are cubic residues, it is possible to find three consecutive integers which are cubic residues of* p.

EXAMPLE. Let $p=37$, $\lambda=19$, whence $m=7$, $n=1$, $j=16$. Here we find $4\lambda m=14$ is a cubic residue of 37 and 36, 11, 23 are cubic residues of 37 in arithmetic progression, with common difference 12.

The methods employed above apply to other similar problems, but I have not been able to obtain any theorems which are very general. In particular owing to the use of the equations $\varphi(z)=(z-\eta_1)(z-\eta_2)\cdots(z-\eta_e)$, where $\eta_1, \eta_2, \ldots, \eta_e$ are the cyclotomic periods, $ef=n-1$, of the equation $x^n=1$, in the algebraic solution of this equation, and the results of Kummer already cited on the integral divisors of $\varphi(z)$, it is possible to obtain a variety of results, but they all seem to be rather special in character, as are the theorems of this paper.

CORNELL UNIVERSITY