Since by hypothesis $H(t,t) \neq 0$, we conclude that the derivative of $f_{p+1}(t)$ exists and is continuous and that $f_{p+1}(1) = f_{p+1}(0) = 0$. Hence it is necessary that the linear functional of continuity order p reduce, by an integration by parts, to a linear functional of continuity order $p-1$. The lemma applied again to this new functional reduces it to a linear functional of continuity order $p-2$. Applying the lemma successively in such a manner, we finally get, as a necessary condition for invariance, the result that the original linear functional of continuity order p has to reduce at least to a linear functional of continuity order one. This result coupled with the existence theorems cited in the beginning of § 5, establishes our theorem.

THE RICE INSTITUTE

ON THE DISTRIBUTION OF QUADRATIC AND HIGHER RESIDUES*

BY H. S. VANDIVER

1. *Introduction.* In the present paper theorems will be obtained regarding the distribution of quadratic and higher residues. Special cases of the theorems yield results concerning the class number of quadratic forms of determinant $(-d)$ where $d \equiv 3 \pmod 4$.

2. *Conjugate Sets of Residues.* In a previous article† the writer considered the notion of *conjugate set* in a *finite algebra.* Applied to the finite algebra represented by the residue classes of a rational integer as modulus, we may define a *conjugate set of residues* of the modulus m to be a set

$$a_1, a_2, \cdots, a_i \tag{1}$$

* Presented to the Society, October 28, 1916.

† ANNALS OF MATHEMATICS, (2), vol. 18 (1917), p. 106.

which has the property that

$$na_1,\ na_2,\ \cdots,\ na_i$$

may be expressed, modulo m, as a permutation of the original set, n being some rational integer $\not\equiv 1 \pmod{m}$. In this case n is called a *multiplier* of the set. Let r, s, and $(r+s)$ all be multipliers of the set (1), modulo $m = p$, a prime, and $0 < a_c < p$, $(c = 1, 2, \cdots, i)$. Consider the expression

$$\sum_h \frac{|rh|+|sh|-|(r+s)h|}{p} h^{kp},$$

where h ranges over the elements of (1), and $|x|$ is the least positive residue of x, modulo p. Then

$$rh = |rh| + pt,$$

where t is an integer, and

$$(2)\qquad \begin{cases} (rh)^{pk} \equiv |rh|^{pk} & \pmod{p^2}, \\ h^{pk} \equiv r^{p(p-1)-pk}\,|rh|^{pk} & \pmod{p^2}. \end{cases}$$

Similarly

$$(3)\qquad h^{pk} \equiv s^{p(p-1)-pk}\,|sh|^{pk} \pmod{p^2},$$

$$(4)\qquad h^{pk} = (r+s)^{p(p-1)-pk}\,|(r+s)h|^{pk} \pmod{p^2}.$$

Since r is a multiplier of (1), we have $\sum_h |rh| = \sum_{c=1}^{i} a_c$; and similarly, for $\sum_h |sh|$ and $\sum_h |(r+s)h|$. Hence

$$\sum_h \left(|rh|\,h^{pk} + |sh|\,h^{pk} - |(r+s)h|^{pk}\right) \equiv (r^e + s^e - (r+s)^e) \sum_{c=1}^{i} a_c^{pk+1} \pmod{p^2},$$

or

$$\sum_h \frac{(|rh|+|sh|-|(r+s)h|)h^{pk}}{p} \equiv \frac{(r^e + s^e - (r+s)^e) \sum_{c=1}^{i} a_c^{pk+1}}{p} \pmod{p},$$

where $e = p(p-1) - pk$. The coefficient of h^{pk} on the left is 0 or 1 according as $|rh|+|sh|$ is less than or

greater than p. Hence we have proved the following theorem.

THEOREM I. *If $a_1, a_2, \cdots, a_i$ is a conjugate set modulo p, and $|x|$ is the least positive residue of x modulo p, then*

$$\sum_{h_1} h_1^k \equiv \frac{(r^e + s^e - (r+s)^e) \sum_{c=1}^{i} a_c^{pk+1}}{p} \pmod{p}, \tag{5}$$

where h_1 ranges over the a's which satisfy $|rh_1| + |sh_1| > p$ and $e = p(p-1) - pk$.

3. *The. Number of j-ic Residues.* In Theorem I, let $a_1, a_2, \cdots, a_i$ be the i roots of $x^i \equiv 1 \pmod{p}$, $p = ij+1$; and suppose that r, s, and $(r+s)$ are each congruent, mod p, to an integer included among the a's. Set $k = i$. Then (2) gives

$$H \equiv \frac{\sum_{c=1}^{i} a^c}{p} \pmod{p},$$

where H is the number of j-*ic* residues included in the integers $h < p$ such that $|rh| + |sh| > p$. Each side of this congruence is a positive integer less than p; consequently

$$H = \frac{\sum_{c=1}^{i} a_c}{p};$$

hence we have the following theorem.

THEOREM II. *If $p = ij+1$ and $a_1, a_2, \cdots, a_i$, $(0 < a_c < p$, $c = 1, 2, \cdots, i)$, are the incongruent roots of $x^i \equiv 1 \pmod{p}$, r, s, and $(r+s)$ being j-ic residues of p, then*

$$H = \frac{\sum_{c=1}^{i} a_c}{p},$$

where H is the number of j-ic residues included in the integers $h < p$ whi h satisfy $|rh| + |sh| > p$.

This result was previously known for the case $r = 1$, $s = 1$, $j = 2$.

4. *Generalization for Quadratic Residues.* For quadratic residues we shall obtain a more general theorem. Let the set (1) range over the distinct positive quadratic residues of p which are less than p, and suppose now that r and s are not necessarily quadratic residues of p. Then if $(r/p)=1$,

$$\sum_h |rh| = \sum a.$$

If however $(r/p) = -1$, then

$$\sum_h |rh| = \sum b = p(p-1)/2 - \sum a,$$

where b ranges over the distinct quadratic non-residues $0<b<p$. Each of these relations is included in the statement

$$\sum_h |rh| = \left(1 - \left(\frac{r}{p}\right)\right)p\mu + \left(\frac{r}{p}\right)\sum a,$$

where $\mu = (p-1)/4$, (not necessarily an integer), and r is any integer prime to p. If we take s and $(s+r)$ in lieu of this relation we get two other equations, which, with the original, give

$$\sum_h \frac{|rh|+|sh|-|(r+s)h|}{p} = (1-R)\mu + \frac{R\sum a}{p},$$

$$R = \left(\frac{r}{p}\right) + \left(\frac{s}{p}\right) - \left(\frac{r+s}{p}\right).$$

A term in the expression on the left of (6) is one or zero according as $|rh|+|sh|$ greater than or less than zero. We may then state the following theorem.

THEOREM III. *If p is an odd prime and K is the number of quadratic residues h included in the set $1, 2, \cdots, p-1$, and satisfying $|rh|+|sh| > p$, then*

$$K = (1-R)\mu + R\frac{\sum a}{p}$$

where $\mu = (p-1)/4$, and

$$R = \left(\frac{r}{p}\right) + \left(\frac{s}{p}\right) - \left(\frac{r+s}{p}\right),$$

r, s, and $(r+s)$ being prime to p, with the a's ranging over the positive quadratic residues of p which are less than p.

For the case $s=1$, this theorem was previously stated in another form and without proof by the writer*. For $s=r=1$, the relation reduces to an equality which is well known.

We shall now show that the number of distinct integers h in the set $1, 2, \cdots, p-1$, which satisfy $|rh|+|sh|>p$ are $(p-1)/2$ in number. If $|rh|+|sh|<p$ then

$$rh = i_1 p + \varepsilon_1, \quad |sh| = i_2 p + \varepsilon_2,$$

ε_1 and ε_2 being each less than p. Also

$$(p-h)r = pr - rh = p(r-i_1) - \varepsilon_1,$$

and

$$|(p-h)r| = p - \varepsilon_1.$$

Similarly,

$$|(p-h)s| = p - \varepsilon_2;$$

hence

$$|(p-h)r| + |(p-h)s| = 2p - \varepsilon_1 - \varepsilon_2.$$

Also, by definition, $|rh| = \varepsilon_1$, $|sh| = \varepsilon_2$ and $\varepsilon_1 + \varepsilon_2 < p$, therefore $2p - \varepsilon_1 - \varepsilon_2 > p$. Hence if h satisfies $|rh|+|sh|>p$, then $p-h$ will not. This shows that there are $(p-1)/2$ distinct values h.

5. *Conclusion.* From Theorem III we see that K is immediately determined if $\sum a/p$ is known, since, for $p = 4n+3$,

$$2\left(1-\left(\frac{2}{p}\right)\frac{1}{2}\right)\frac{\sum b - \sum a}{p} = h(-p)$$

is the expression for the number of classes of properly primitive quadratic forms of determinant $(-p)$. Since also $\sum b + \sum a = (p^2-p)/2$, it is possible to give a relation between h and K. In particular we obtain a variety of expressions for h.

THE UNIVERSITY OF TEXAS

* This BULLETIN, vol. 23 (1916), p. 113.