$d = e_1 d_1$, where e_1 is an integer. The remaining conditions (6) now hold if and only if $a - e_1 c_1 = q d_1$, $f - b_1 d_1 = -q c_1$, where q is an integer. Next, when $a, \cdots, f$ are any numbers (not necessarily integers) of the field R, the conditions (6) are equivalent to

$$b = b_1 d_1, \quad c = b_1 c_1, \quad e = e_1 c_1, \quad d = e_1 d_1,$$
$$a = e_1 c_1 + q d_1, \quad f = b_1 d_1 - q c_1,$$

where b_1, c_1, d_1, e_1, q are numbers of R. We now have the most general operation (5) under which the numbers of R form a group.

5. We are led to a fraction of the form (5) in which α and β enter linearly if we demand that the inverse operation shall be applicable to every pair of numbers of the field. Suppose that also $\alpha \oplus \beta$ is a similar symmetric function of α and β. If these two operations obey the associative and distributive laws, it seems probable that they must be of type (2) and (3), defined by the linear fractional correspondence (1). This is easily proved for integral functions:

$$\alpha \oplus \beta = A\alpha\beta + B(\alpha + \beta) + C,$$
$$\alpha \odot \beta = a\alpha\beta + b(\alpha + \beta) + c.$$

Of the conditions for $(\alpha \oplus \beta) \odot \gamma = (\alpha \odot \gamma) \oplus (\beta \odot \gamma)$, those which involve γ^2 show that $Aa = Ab = 0$, whence $A = 0$, and the remaining conditions are

$$aC + b = 2Bb, \qquad bC + c = 2Bc + C.$$

By the associative law for $\oplus$, $B^2 = B$, whence $B = 1$. Thus $b = aC$, $c = aC^2 - C$, and we get (4) with $m = -C$, $l = 1/a$.

NOTE ON THE DISTRIBUTION OF QUADRATIC RESIDUES.

BY MR. H. S. VANDIVER.

(Read before the American Mathematical Society, October 30, 1915.)

THE present note relates mainly to the distribution of quadratic residues for a rational prime modulus. A special quadratic form is also considered.

1. Let the prime be $p = 4n + 1$ and assume that k is the number of distinct positive quadratic residues which are less than $\sqrt{p}$. If x is an integer such that

$$x^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}, \tag{1}$$

then by a known theorem* it is possible to write

$$x \equiv \pm \frac{m}{n} \pmod{p},$$

where $0 < m < \sqrt{p}$ and $0 < n < \sqrt{p}$. There are $\frac{1}{2}(p-1)$ distinct positive non-quadratic residues of p which are less than p, and from (1) we have

$$\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = -1.$$

We may then assume

$$\left(\frac{m}{p}\right) = 1, \quad \left(\frac{n}{p}\right) = -1.$$

Let there be l distinct positive quadratic non-residues less than $\sqrt{p}$. If m/n is a quadratic non-residue of p, then $-m/n$ and $\pm n/m$ are also non-residues, and we therefore have

$$kl \geqq \tfrac{1}{8}(p-1). \tag{2}$$

We also have $k + l = [\sqrt{p}]$, where $[\sqrt{p}]$ denotes the largest integer in $\sqrt{p}$. We get, after using (2),

$$l \text{ or } k \geqq \frac{[\sqrt{p}] - \sqrt{[\sqrt{p}]^2 - \frac{1}{2}(p-1)}}{2},$$

which gives

THEOREM I. *If p is a prime of the form $4n + 1$, then in the set $1, 2, \cdots, [\sqrt{p}]$ there are at least*

$$\left[\frac{[\sqrt{p}] - \sqrt{[\sqrt{p}]^2 - \frac{1}{2}(p-1)}}{2}\right]$$

distinct quadratic residues and at least the same number of non-residues.

2. In connection with the distribution of quadratic residues the writer has proved the following:

* This BULLETIN, 1915, p. 61.

THEOREM II. *Let p be a prime of the form $4n+3$ and let pR be the sum of the quadratic residues of p. Consider the $\mu = \frac{1}{2}(p-1)$ integers $h < p$ defined by*

$$h + [ah] < p, \tag{3}$$

where $[ah]$ is the least positive residue of ah modulo p and a is a fixed integer less than $p-1$. Then the number of quadratic residues in such a set is equal to

$$\left\{\left(\frac{a+1}{p}\right) - \left(\frac{a}{p}\right) - 1\right\} R + S + T,$$

where $S = 0$ or μ according as $(a/p) = \mp 1$, and $T = 0$ or μ according as $(a+1)/p = \pm 1$.

The proof of this result will be given in another paper. The theorem evidently shows that if the number of incongruent positive quadratic residues less than $\frac{1}{2}p$ is known then it is possible to write down immediately the number of quadratic residues in any set (3).

3. By a theorem already cited it is possible to express all the $p-1$ incongruent residues of p, which are prime to p, by means of the set

$$\pm \frac{m}{n}, \tag{4}$$

modulo p, where m and n each range over all the distinct positive quadratic residues of p which are $< \sqrt{p}$. We proceed to find another expression for the number of incongruent fractions (4). Reduce each fraction to its lowest terms and let the number of distinct fractions be K, say. If any two are congruent modulo p we must have

$$\frac{m}{n} \equiv -\frac{m'}{n'} \pmod{p},$$

and, since each m and n is $< \sqrt{p}$, we obtain

$$mn' + m'n = p. \tag{5}$$

Corresponding to such a representation of p, we derive the following relations:

$$\begin{aligned} &\frac{m}{n} \equiv -\frac{m'}{n'}, \quad -\frac{m}{n} \equiv \frac{m'}{n'}, \quad \frac{n}{m} \equiv -\frac{n'}{m'}, \quad -\frac{n}{m} \equiv \frac{n'}{m'}, \\ &\frac{m}{m'} \equiv -\frac{n}{n'}, \quad -\frac{m}{m'} \equiv \frac{n}{n'}, \quad \frac{m'}{m} \equiv -\frac{n'}{n}, \quad -\frac{m'}{m} \equiv \frac{n'}{n}, \end{aligned} \tag{6}$$

modulo p. In counting the number of incongruent fractions in the set (4) we must therefore consider the number of representations (5). We shall regard two representations

$$mn' + m'n = p, \quad m_1n_1' + m_1'n_1 = p$$

as the same if and only if $m = m_1$, $n' = n_1'$, $m' = m_1'$, $n = n_1$. If N is the number of representations of this type, then the relations (6) show that

$$N = K - (p - 1).$$

Now K by definition is equal to twice the number of distinct positive irreducible fractions whose numerators and denominators are each not greater than $\sqrt{p}$. Hence*

$$K = 4(\varphi(2) + \varphi(3) + \cdots + \varphi([\sqrt{p}])) + 2,$$

where $\varphi(k)$ denotes the number of integers $< k$ and prime to it. We therefore have

THEOREM III. *If p is a prime, then the number of representations of p in the form*

$$xy + x'y',$$

where x, y, x', y' are all positive integers $< \sqrt{p}$, is equal to

$$-(1 + p) + 4\sum_{k=1}^{[\sqrt{p}]} \varphi(k).$$

PROOF OF A GENERAL THEOREM ON THE LINEAR DEPENDENCE OF p ANALYTIC FUNCTIONS OF A SINGLE VARIABLE.

BY MR. HAROLD MARSTON MORSE.

(Read before the American Mathematical Society, September 5, 1916.)

A PROOF of the following theorem has to my knowledge not been published to date. The theorem contains as a special case the ordinary theorem concerning the wronskian. Its usefulness in a general treatment of single-valued func-

* Lucas, Théorie des Nombres, p. 393.