enter linearly and homogeneously, found their finite equations, and introduced variables such that each group becomes its own parameter group. The resulting groups (l. c., page 648, bottom, and page 649) are our h and g. From these he derived the above two algebras.

6. Scheffers' determination (pages 654–6) of the algebra of quaternions is based upon the existence of the group of transformations t'_Y of § 4. In a rather arbitrary manner he selected four infinitesimal transformations out of an aggregate of the ∞^6 infinitesimal automorphs of the quadric surface, and verified that the four generate a four-parameter group. The guide to this seemingly fortunate selection may well have been the previous knowledge of the group defined by the algebra of quaternions. The above discussion in § 4 not only gives a natural derivation of quaternions from the theory of groups but leads to the total group of automorphs of a quadric surface and not merely to its continuous subgroup.

THE UNIVERSITY OF CHICAGO.

AN ASPECT OF THE LINEAR CONGRUENCE WITH APPLICATIONS TO THE THEORY OF FERMAT'S QUOTIENT.

BY MR. H. S. VANDIVER.

(Read before the American Mathematical Society, August 4, 1915.)

IN 1903, Professor G. D. Birkhoff communicated to me the following theorem:

If p is a prime integer and a is a positive integer prime to p, then there is at least one and not more than two sets (x, y) such that

$$a \equiv \pm x/y \pmod{p}$$

where x and y are integers prime to each other and $0 < x < \sqrt{p}$, $0 < y < \sqrt{p}$.

Professor Birkhoff has kindly allowed me to use this result, and in the present paper I shall give a proof of the theorem which involves a continued fraction algorithm for a direct determination of each set. Some extensions and applications are also given.

1. *Proof and Algorithm.*—We have

$$p = am_1 + r_1 \quad (0 < r_1 < a),$$
$$a = m_2 r_1 + r_2 \quad (0 < r_2 < r_1),$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$r_{k-2} = m_k r_{k-1} + r_k \quad (0 < r_k < r_{k-1}),$$
$$r_k < \sqrt{p} \leqq r_{k-1}.$$

These relations give

$$(m_k m_{k-1} + 1) r_{k-2} = r_k + m_k r_{k-3}$$

and similarly

$$r_{k-3}(m_k m_{k-1} m_{k-2} + m_k + m_{k-2}) = -r_k + r_{k-4}(m_k m_{k-1} + 1).$$

Hence we ultimately have

$$al \equiv \pm r_k \pmod{p},$$

where l is the continuant

$$\begin{vmatrix} m_k & 1 & 0 & \cdots & & 0 \\ -1 & m_{k-1} & 1 & \cdots & & 0 \\ 0 & -1 & m_{k-2} & \cdots & & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & -1 & m_1 \end{vmatrix}.$$

Note that l is prime to p since r_k is so.

We now prove that $l < \sqrt{p}$. We have

$$r_{k-3} = (m_{k-1} m_k + 1) r_{k-1} + m_{k-1} r_k,$$
$$r_{k-4} = (m_k m_{k-1} m_{k-2} + m_k + m_{k-2}) r_{k-1} + r_k (m_{k-1} m_{k-2} + 1),$$

and finally

(1) $$p = l r_{k-1} + r_k j,$$

where j equals

$$\begin{vmatrix} m_{k-1} & 1 & 0 & \cdots & & 0 \\ -1 & m_{k-2} & 1 & \cdots & & 0 \\ 0 & -1 & m_{k-3} & \cdots & & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & -1 & m_1 \end{vmatrix}.$$

Hence, since $r_{k-1} \geqq \sqrt{p}$ then $l < \sqrt{p}$ because $r_k j > 0$. Also r_k is prime to l since l is prime to p. Therefore one of the sets (x, y) is (r_k, l). Set $x_0 = r_k$, $y_0 = l$. Then if there were a second set (x_1, y_1) where x_1 is prime to y_1, we should have

$$x_0 y_1 + x_1 y_0 = p,$$

since x_0 and y_0 are prime to each other. This being the case, we see from (1), after noting that $r_{k-1} \geqq \sqrt{p}$, that there must exist a positive integer μ such that

$$y_0(r_{k-1} - \mu x_0) + x_0(j + \mu y_0) = p,$$

where

$$r_{k-1} - \mu x_0 < \sqrt{p},\ j + \mu y_0 < \sqrt{p}.$$

These two conditions may be written

$$(1a) \qquad \frac{r_{k-1} - \sqrt{p}}{x_0} < \mu < \frac{\sqrt{p} - j}{y_0}.$$

Now μ cannot have more than one integral value, since the above relation would then give

$$(2) \qquad -p + (x_0 + y_0)\sqrt{p} > 2x_0 y_0,$$

which shows that one of the integers x_0, y_0, is $> \frac{1}{2}\sqrt{p}$. If $y_0 > \frac{1}{2}\sqrt{p}$ and $x_0 = 1$, then (2) evidently does not hold. Also, if $x_0 > 1$, the right-hand member of (2) increases faster than the left-hand member when x_0 is increased. Since, then, μ has no more than one positive integral value, there are not more than two sets (x, y) satisfying the conditions of the theorem. Further, μ, when it exists, is uniquely determined by (1a). This completes the proof and algorithm.

The existence of one set (x, y) may also be shown by means of a theorem due to Minkowski.*

If

$$\begin{aligned} f_1 &= a_{11}\ u_1 + \cdots + a_{1m} u_m, \\ &\cdots\cdots\cdots\cdots\cdots \\ f_m &= a_{m1} u_1 + \cdots + a_{mm} u_m \end{aligned}$$

are m linear homogeneous forms in $u_1, u_2, \cdots, u_m$ with arbitrary real coefficients $a_{11}, \cdots, a_{mm}$ of determinant Δ, then it is

* Geometrie der Zahlen, page 104.

always possible to select integers for $u_1, u_2, \cdots, u_m$ so that

$$|f_i| \leqq \sqrt[m]{\Delta} \qquad (i = 1, 2, \cdots, m).$$

In this relation set all the $a_{ij} = 0$ for $i > 1$, except when $i = j$ in which case $a_{ii} = 1$, $i = 2, 3, \cdots, m$. Then

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1m} \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = a_{11}.$$

Assume further that $a_{11}, a_{12}, \cdots, a_{1m}$ are integers, then the result may be expressed as follows:

It is always possible to choose integers $u_2, u_3, \cdots, u_m$ such that

$$f_1 = a_{12}u_2 + \cdots + a_{1m}u_m \pmod{M},$$

where $a_{12}, \cdots, a_{1m}$ and M are given integers and $|f_1| \leqq \sqrt[m]{M}$, $|u_i| \leqq \sqrt[m]{M}$ $(i = 2, 3, \cdots, m)$. If we further put $m = 2$, we obtain

$$a_{12}u_2 \equiv f_1 \pmod{M},$$

where $|f_1| < \sqrt{p}$ and $|a_{12}| < \sqrt{p}$. We note that μ is not necessarily prime. The existence of at least one set (a_{12}, f_1) for a composite modulus M may also be shown by the algorism which has just been explained for the derivation of the first set (x_0, y_0) in

$$ay \equiv \pm x \pmod{p}.$$

Evidently the reasoning used also holds for the case where p is composite.

2. *Applications to Fermat's Quotient.*—The congruence

$$x^{p-1} \equiv 1 \pmod{p^2}, \tag{3}$$

where p is an odd prime, has $p - 1$ incongruent roots modulo p^2. By the theorem just proved, each can be represented by an expression of the type $\pm m/n$, where m and n are positive integers each $< p$. If

$$\left(\pm \frac{m}{n}\right)^{p-1} \equiv 1 \pmod{p^2},$$

then

$$m^{p-1} \equiv n^{p-1} \pmod{p^2}.$$

The relation (3) has the roots ± 1. If it has another root, say $\pm m_{10}/m_{20}$, when numerator and denominator are each positive and $< p$, then assume that there are k positive integers $m_{k0} < p$ such that

$$m_{10}{}^{p-1} \equiv m_{20}{}^{p-1} \equiv \cdots m_{k0}{}^{p-1}$$

modulo p^2, when $m_{a0} \neq m_{b0}$. Then we may form the $2k(k-1)$ expressions

$$\pm \frac{m_{10}}{m_{20}}, \pm \frac{m_{10}}{m_{30}}, \cdots \pm \frac{m_{30}}{m_{20}}, \cdots,$$

$$\pm \frac{m_{20}}{m_{10}}, \pm \frac{m_{30}}{m_{10}}, \cdots \pm \frac{m_{20}}{m_{30}}, \cdots,$$

each of which satisfies (3). If the $p-1$ roots of (3) exclusive of ± 1, are not exhausted by this set, then in like manner, there must exist m's such that

$$m_{11}{}^{p-1} \equiv m_{21}{}^{p-1} \equiv \cdots \equiv m_{k_1 1}{}^{p-1},$$

where

$$m_{a1} \neq m_{b1} \text{ and } m_{c1} \neq m_{d0} \text{ and } k_1 \geqq 2.$$

As before, we may form a set of solutions of (3) by means of these m's in the same way the former solutions were set up. If this second set does not exhaust the remaining roots of (3), the process may be repeated. Ultimately we obtain a set

$$\pm \frac{m_{1i}}{m_{2i}}, \pm \frac{m_{1i}}{m_{3i}}, \cdots, \pm \frac{m_{3i}}{m_{2i}}, \cdots,$$

$$\pm \frac{m_{2i}}{m_{1i}}, \pm \frac{m_{3i}}{m_{1i}}, \cdots, \pm \frac{m_{2i}}{m_{3i}}, \cdots,$$

where

$$m_{1i}{}^{p-1} \equiv m_{2i}{}^{p-1} \equiv \cdots \equiv m_{k_i i}{}^{p-1},$$

such that it includes, when taken together with the preceding i sets and the special roots ± 1, all the incongruent roots of (3). We have evidently

$$\sum_{j=0}^{i} 2k_j(k_j - 1) \geqq p - 3.$$

Assume $i = 0$, then

$$2k_0^2 - 2k_0 \geqq p - 3,$$

whence

$$k_0 \geqq \frac{1 + \sqrt{2p - 5}}{2}.$$

Consider the set

$$1^{p-1}, \quad 2^{p-1}, \quad 3^{p-1}, \cdots, \quad (p-1)^{p-1},$$

and call the least positive residues of these integers modulo p^2, *proper residues* modulo p^2. If $i = 0$, then from

$$m_{10}{}^{p-1} \equiv m_{20}{}^{p-1} \equiv \cdots \equiv m_{k0}{}^{p-1}$$

we are enabled to conclude that there are not more than

$$p - \frac{1 + \sqrt{2p - 5}}{2}$$

incongruent proper residues modulo p^2. Assume now that $i = 1$. We have

$$2k_1^2 + 2k_0^2 - 2k_1 - 2k_0 \geqq p - 3,$$

whence

$$k_1 + k_0 - 2 \geqq \frac{1 + \sqrt{2p - 5}}{2} - 1.$$

Hence we conclude as before that there are not more than

$$p - \frac{1 + \sqrt{2p - 5}}{2}$$

incongruent proper residues modulo p^2. In general we have

$$\sum_{j=0}^{i} k_j - (i + 1) \geqq \frac{1 + \sqrt{2p - 5}}{2} - 1.$$

Now consider a lower limit for the number of incongruent proper residues modulo p^2. There cannot be less than $[\sqrt{p}]$ residues of this type, for if there were only $[\sqrt{p}] - 1$ residues then there must exist at least one set of distinct positive integers $m_i < p$ such that

$$m_1{}^{p-1} \equiv m_2{}^{p-1} \equiv \cdots \equiv m_s{}^{p-1} \pmod{p^2},$$

where $s > [\sqrt{p}]$. This being the case, consider

$$(p - m_i)^{p-1}, \qquad (i = 1, 2, \cdots, s).$$

Each of these gives a proper residue and they are all incongruent modulo p^2. Evidently, also, there are at least $[\sqrt{p}]$ of them, contrary to hypothesis. Hence the theorem:

There are not more than

$$p - \frac{1 + \sqrt{2p - 5}}{2}$$

and not less than $[\sqrt{p}]$ *incongruent proper residues modulo* p^2, *where* p *is prime* > 2.

3. We now consider the relation of the foregoing to Fermat's last theorem. If

$$x^p + y^p + z^p = 0$$

is satisfied in integers prime to each other and to the odd prime p, then $2^{p-1} \equiv 1 \pmod{p^2}$, a result due to Wieferich. This being the case, then the set

$$1^{p-1}, \ 3^{p-1}, \ \cdots, \ (p - 2)^{p-1}$$

evidently includes all the incongruent proper residues modulo p^2. Hence they are not more than $\frac{1}{2}(p - 1)$ in number. Similarly, using the criterion of Mirimanoff, $3^{p-1} \equiv 1 \pmod{p^2}$, we note that the forms

$$(1 + 6k)^{p-1}, \quad (5 + 6k_1)^{p-1}$$

include all the incongruent proper residues and there are not more than $2[p/6]$. We may further reduce the number by using the criteria $5^{p-1} \equiv 11^{p-1} \equiv 17^{p-1} \equiv 1 \pmod{p^2}$.*

* Vandiver, *Journal für Mathematik*, vol. 144, p. 314. Frobenius, *Sitzungsberichte der K. Akademie der Wissenschaften*, Berlin, 1914, p. 653.