A SIMPLE PRINCIPLE OF UNIFICATION IN THE ELEMENTARY THEORY OF NUMBERS[1]

By R. D CARMICHAEL, University of Illinois

1. *Introduction.* The elementary theory of positive integers lacks the unity which is essential to a structure of the most pleasing esthetic quality. This fact is apparent from, and indeed is emphasized by, the record given in the first volume of Dickson's *History of the Theory of Numbers*—a volume devoted largely to elementary aspects of the theory of positive integers. As long as these numbers are dealt with only by the methods hitherto invented, this proposition concerning esthetic quality is likely to remain true; for there is apparent no ground of hope that these methods, by their development and extension, will grow into each other and so lead to the desired unity. You will therefore not expect me to suggest a means of bringing order into all this confusion. At the best only a part of these scattered results can now be given a place in any structure of thought possessing esthetic unity. But I hope to indicate how a significant part of them may be united by a method which is both elementary and rather comprehensive as regards the material brought into unity through its use.

A convenient point of departure is afforded by certain theorems due to Fermat. If the integer a is prime to the prime p then $a^{p-1}-1$ is divisible by p; more generally, if a and m are relatively prime integers and if $\phi(m)$ denotes the totient of m then $a^{\phi(m)}-1$ is divisible by m. One inevitably raises the question as to what is the least positive integer ν such that $a^{\nu}-1$ is divisible by p or by m. The question also arises concerning the existence of numbers a such that the least value of ν for which $a^{\nu}-1$ is divisible by p or m is $p-1$ or $\phi(m)$ respectively. The customary propositions arising here you recognize as part of the classic theory of integers. You observe also that they are all intimately associated with the infinite sequence of integers

$$a-1, \quad a^2-1, \quad a^3-1, \quad a^4-1, \cdots .$$

This will afford the point of departure for the method to be presented. If we write

$$u_n = a^n - 1, \quad n = 0,1,2, \cdots ,$$

then it is easy to verify that

$$u_{n+2} - (a+1)u_{n+1} + au_n = 0, \quad u_0 = 0, \quad u_1 = a - 1.$$

Conversely, the solution of this difference system leads to the given sequence. The indicated propositions may therefore be presented in the form of equivalent theorems pertaining to the named sequence. As soon as they are seen in this light, several possible generalizations come at once to mind. It is these which afford the simple principle of unification to be treated.

[1] This paper was read by invitation before the Mathematical Association of America at New York City on Dec. 28, 1928.

2. *Recurrent Sequences of Integers.*[1] The sequence of integers

$$u_0,\ u_1,\ u_2,\ \cdots \tag{1}$$

is uniquely defined in terms of the initial numbers $u_0, u_1, \cdots, u_{k-1}$ by the recurrence relation

$$u_{x+k} + \alpha_1 u_{x+k-1} + \alpha_2 u_{x+k-2} + \cdots + \alpha_k u_x = \alpha, \tag{2}$$

in which $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_k$ are given integers. We assume that $\alpha_k \neq 0$. We use m to denote a given positive integer and p to denote a given prime; and often (as occasion arises) we think of p as a possible value of m.

Let

$$r_0,\ r_1,\ r_2,\ \cdots \tag{3}$$

be in order the least non-negative residues of the integers $u_0, u_1, u_2, \cdots$ with respect to the modulus m. It is easy to show that the sequence (3) always contains a set of k consecutive residues which is repeated (as an ordered set) infinitely often in the sequence. The infinite sequence beginning with this set in any position in the sequence is the same as that beginning with the same set in any other position. We may therefore say that the residues (3), with the possible exception of a finite number at the beginning, repeat themselves periodically in cycles. If μ is the number of residues in the smallest cycle which is thus repeated we shall call μ the characteristic number of (1) modulo m, and we shall write

$$\mu = \mu(m\ ;\ k\ ;\ \alpha\ ;\ \alpha_1,\alpha_2,\ \cdots,\ \alpha_k\ ;\ u_0,u_1,\ \cdots,\ u_{k-1}).$$

When a and m are relatively prime integers the relations

$$\mu(m; 1; a-1; -a; 0) = \mu(m; 2; 0; -a-1, a; 0, a-1) = \text{the exponent of } a \text{ (modulo } m)$$

are easily verified in view of the sequence treated in § 1. Thus μ is in two ways a generalization of an important function in the classic theory. Furthermore, from the classic theory it follows that this particular μ is always a factor of $\phi(m)$. These special results are instances of propositions concerning the general function μ, propositions which may be attained without too great difficulty (see the memoir cited) when m and α_k are relatively prime.

The more important applications of the theory belong to the case in which equation (2) is homogeneous ($\alpha=0$) and indeed to a case in which further conditions are also satisfied. The resulting sequences are then said to be restricted. By a restricted sequence (1) modulo m, where m and α_k are relatively prime, we shall mean a sequence

$$U_0,\ U_1,\ U_2,\ \cdots \tag{4}$$

such that U_n is a solution of the homogeneous equation

[1] For this section generally, see the Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372.

$$u_{x+k} + \alpha_1 u_{x+k-1} + \cdots + \alpha_k u_x = 0, \tag{5}$$

while the corresponding sequence of residues (3) modulo m,

$$R_0,\ R_1,\ R_2,\ \cdots, \tag{6}$$

has a subset σ of k consecutive elements (which we call a chief subset) containing at least one element prime to m and being such that another and later subset σ_1 of k consecutive elements are in order congruent to the elements of the former set, each multiplied by one and the same integer τ prime to m. Then we call τ a multiplier modulo m of the sequence. If ρ is the exponent modulo m to which the multiplier τ belongs, then μ/ρ is an integer μ_τ which is called the restricted characteristic number modulo m of the restricted sequence (4) as to the chief subset σ and the multiplier τ. Some of the most useful applications of the theory are associated with the number μ_τ.

These ideas furnish the basis for a general theory of these recurrent sequences of integers. Since we are now to treat mainly certain special cases it is not necessary to outline the general theory. We may however give an idea of the latter by stating a few results for the very simple case when m is the prime power p^t and the polynomial $f(\rho)$,

$$f(\rho) = \rho^k + \alpha_1\rho^{k-1} + \cdots + \alpha_k,$$

is irreducible modulo p. When $k=1$ and $\alpha=0$ we suppose further that $f(\rho)$ is not identically equal to $\rho-1$. We suppose also that $p>k$. Then the characteristic number μ of the sequence modulo p^t is a factor of p^k-1 when $t=1$ and is a factor of $p^t(p^k-1)$ when $t>1$, α_k in each case being prime to p. As a special case we have the classic result that the exponent of a modulo p is a factor of $p-1$, a being prime to p. There are numbers a belonging modulo p to the exponent $p-1$. As a generalization of this classic result we have the theorem that for every value of k there are sequences (1) whose characteristic number modulo p is p^k-1. In a similar way it is possible to generalize other classic results concerning primitive roots modulo m.

There are also general theorems (see the Quarterly Journal of Mathematics, l. c.) asserting that a given number m is a prime when the characteristic number μ of a sequence modulo m has certain defined properties. For special cases of these results see the next section.

3. *The Functions*[1] D_n, S_n *and* F_n. The instances of the foregoing general theory which have been most fully treated are those which are associated with the functions

$$D_n \equiv D_n(\alpha,\beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad S_n \equiv S_n(\alpha,\beta) = \alpha^n + \beta^n,$$

both of which satisfy the equation

$$u_{n+2} - (\alpha+\beta)u_{n+1} + \alpha\beta u_n = 0,$$

[1] For this section generally, see the *Annals of Mathematics*, (2), vol. 15 (1913), pp. 30–70.

where $\alpha+\beta$ and $\alpha\beta$ are relatively prime integers. [The case when α and β are both roots of unity is excluded from consideration.] Associated with D_n and S_n is the function $F_n(\alpha, \beta)$, where

$$F_n(\alpha,\beta) = \beta^{\phi(n)}Q_n(\alpha/\beta)$$

and $Q_n(x)$ is the polynomial of degree $\phi(n)$ with leading coefficient unity whose roots are the primitive n^{th} roots of unity without repetition. When $n>1$ the value of $F_n(\alpha, \beta)$ is an integer; the value of F_1^2 is also an integer.

Then we have the obvious relation $D_{2n}=D_nS_n$ and the fundamental partial numerical factorization of D_n afforded by the formula

$$D_n(\alpha,\beta) = \prod_d{}' F_d(\alpha,\beta) ,$$

where d ranges over all the divisors of n except unity.

The properties of D_n, S_n and F_n have been developed in some detail. Perhaps the most fundamental properties of F_n are those represented in the following theorem:

I. Let ν be any positive integer and let p be any prime not dividing ν; then

(1) If $F_{\nu p^a}\equiv 0 \bmod p$, then $F_\nu^2\equiv 0 \bmod p$.

(2) If $F_\nu^2\equiv 0 \bmod p$, then each of the numbers $F_{\nu p}$, $F_{\nu p^2}$, $F_{\nu p^3}$, $\cdots$ is divisible by p, and none of them is divisible by p^2 except when $\nu=1$ in which case F_p may be divisible by p^2 and when $\nu=3$, $p=2$ in which case F_6 may be divisible by 2^2. Moreover, $F_k^2\not\equiv 0 \bmod p$ unless k is of the form νp^a.

(3) If $F_{\nu p^a}\not\equiv 0 \bmod p$, $a>0$, then $F_{\nu p^a}\equiv 1 \bmod p$ when $\nu>1$ or when $\nu=1$ and $p=2$; if $\nu=1$ and p is odd we have

$$F_{p^a} \equiv (\alpha - \beta)^{p-1} \equiv \pm 1 \bmod p.$$

Consider the sequence of integers F_1^2, F_2, F_3, $\cdots$. By a characteristic factor of F_n we mean a prime divisor of F_n which is not a factor of any number of the set F_1^2, F_2, F_3, $\cdots$, F_{n-1}. Similarly, a characteristic factor of $D_n[S_n]$ is a prime divisor of $D_n\,[S_n]$ which is not a factor of any $D_\nu\,[S_\nu]$ for which ν is a positive integer less than n. In this connection the principal theorems are the following:

II. A necessary and sufficient condition that a prime p which divides F_n shall be a characteristic factor of F_n is that p shall be prime to n.

III. A characteristic factor of $F_n\,[F_{2n}]$ is also a characteristic factor of $D_n[S_n]$.

IV. If α and β are real and if $n\neq 1, 2, 6$, then $F_n(\alpha, \beta)$ contains at least one characteristic factor in all cases except when

(1) α and β are suitably chosen irrational numbers and n is equal to an odd prime divisor of $(\alpha-\beta)^2$;

(2) $\qquad n = 3, \quad \alpha+\beta = \pm 1, \quad \alpha\beta = -2;$

(3) $\qquad n = 5, \quad \alpha+\beta = \pm 1, \quad \alpha\beta = -1;$

(4) $\qquad n = 12, \quad \alpha+\beta = \pm 1, \quad \alpha\beta = -1.$

V. If α and β are real and $n \neq 1, 2, 6$, then D_n contains at least one characteristic factor except when

$$n = 12, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -1.$$

VI. If α and β are real and $n \neq 1, 3$, then S_n contains at least one characteristic factor except when

$$n = 6, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -1.$$

VII. A characteristic factor of $F_n(\alpha, \beta)$ is of the form $kn \pm 1$. When a and b are relatively prime integers a characteristic factor of $F_n(a, b)$ is of the form $kn+1$.

From another point of view we have the following theorem:

VIII. If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where the p's are distinct primes, and if m is prime to $\alpha\beta$ then $D_\lambda \equiv 0$ and $D_\phi \equiv 0 \bmod m$, where λ is the least common multiple of the integers

$$p_i^{\alpha i-1}[p_i - (\alpha,\beta)_{p_i}], \quad i = 1,2, \cdots, k,$$

and where ϕ is their product, the symbol $(\alpha, \beta)_p$ for odd prime p having the value 0, 1, or -1 according as $(\alpha-\beta)^2$ is divisible by p, is a quadratic residue of p, or a quadratic non-residue of p, while $(\alpha, \beta)_2$ is 1, 0 or -1 according as (a) $\alpha\beta$ is even, (b) $\alpha\beta$ is odd and $\alpha+\beta$ is even, or (c) $\alpha\beta$ and $\alpha+\beta$ are both odd.

The function ϕ here introduced is a generalization of the Euler ϕ-function. Many of the generalizations of this function which have been employed may be associated similarly with the general theory indicated in § 2; and the latter general theory may be so developed as to bring a certain measure of unity into the known results concerning Euler's ϕ-function and its generalizations. In a similar way some unity may likewise be introduced into the generalizations of the theory of primitive roots modulo m.

By means of the functions treated in this section it may be shown that each of the sequences

$$p^k x - 1, \; 3 \cdot 2^k x - 1, \; 4x + 1, \; 4x - 1, \; 6x + 1, \; 6x - 1, \; x = 1,2,3, \cdots,$$

where p is any given odd prime and k is any given positive integer, contains an infinite number of primes.

In another range of ideas we have the following theorems:

IX. A necessary and sufficient condition that a given odd number p shall be a prime is that there shall exist relatively prime integers $\alpha+\beta$ and $\alpha\beta$ such that $F_{p-1}(\alpha, \beta)$ shall be divisible by p.

X. A necessary and sufficient condition that a given odd number p shall be a prime is that an integer a shall exist such that $F_{p-1}(a, 1)$ shall be divisible by p.

XI. A necessary and sufficient condition that an odd number p shall be a prime is that there shall exist relatively prime integers $\alpha+\beta$ and $\alpha\beta$ such that $F_{p+1}(\alpha,\beta)$ shall be divisible by p.

XII. If $p=2^2+1$, $n>1$, and if r is any odd prime of which p is a quadratic non-residue, then a necessary and sufficient condition that p shall be a prime is that

$$r^{(p-1)/2}+1\equiv 0 \bmod p.$$

[For each p one may use 3 for r.]

XIII. A necessary and sufficient condition that $2^{k+1}\cdot q+1$, where q is an odd prime, shall be a prime is that an integer a shall exist such that

$$\frac{(a^{2^kq}+1)}{(a^{2^k}+1)}\equiv 0 \bmod 2^{k+1}\cdot q+1.$$

It is by means of theorems of this sort that the discovery of large primes has been effected. Perhaps the whole of the known related theory may be unified by means of such theorems and their generalizations arising in connection with the general theory of recurrent sequences of integers.

We may suggest as worthy of attention two generalizations of the important function $D_n(\alpha,\beta)$, namely, the following:

$$G_n=\frac{\begin{vmatrix}1 & 1 & \cdots 1\\ \alpha_1 & \alpha_2 & \cdots \alpha_k\\ \cdot & \cdot & \cdot\cdot\cdot\cdot\\ \cdot & \cdot & \cdot\cdot\cdot\cdot\\ \alpha_1^{k-2} & \alpha_2^{k-2} & \cdots \alpha_k^{k-2}\\ \alpha_1^n & \alpha_2^n & \cdots \alpha_k^n\end{vmatrix}}{\begin{vmatrix}1 & 1 & \cdots 1\\ \alpha_1 & \alpha_2 & \cdots \alpha_k\\ \alpha_1^2 & \alpha_2^2 & \cdots \alpha_k^2\\ \cdot & \cdot & \cdot\cdot\cdot\cdot\\ \cdot & \cdot & \cdot\cdot\cdot\cdot\\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots \alpha_k^{k-1}\end{vmatrix}},\quad H_n=\frac{\begin{vmatrix}1 & 1 & \cdots 1\\ \alpha_1^n & \alpha_2^n & \cdots \alpha_k^n\\ \alpha_1^{2n} & \alpha_2^{2n} & \cdots \alpha_k^{2n}\\ \cdot & \cdot & \cdot\cdot\cdot\cdot\\ \cdot & \cdot & \cdot\cdot\cdot\cdot\\ \alpha_1^{(k-1)n} & \alpha_2^{(k-1)n} & \cdots \alpha_k^{(k-1)n}\end{vmatrix}}{\begin{vmatrix}1 & 1 & \cdots 1\\ \alpha_1 & \alpha_2 & \cdots \alpha_k\\ \alpha_1^2 & \alpha_2^2 & \cdots \alpha_k^2\\ \cdot & \cdot & \cdot\cdot\cdot\cdot\\ \cdot & \cdot & \cdot\cdot\cdot\cdot\\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots \alpha_k^{k-1}\end{vmatrix}},$$

where $\alpha_1, \alpha_2, \cdots, \alpha_k$ are distinct roots of the equation

$$x^k+c_1x^{k-1}+\cdots+c_k=0,$$

in which $c_1, c_2, \cdots c_k$ are given integers. The investigation of the properties of these functions will lead to two generalizations of the theory associated with the function $D_n(\alpha,\beta)$, which is the special case for $k=2$ of both G_n and H_n. It seems likely that this investigation will lead to something of interest.

In G_n the numerator is formed by replacing the last row in the denominator by $\alpha_1^n, \alpha_2^n, \cdots, \alpha_k^n$. Other useful functions may also be formed similarly by putting these elements for other rows in the denominator.

The theory of recurrent sequences of integers, together with certain closely related matters, and particularly the special case treated in this section, may be shown to pervade, or at least to be implicit in important ways in, ten of the twenty chapters of volume I of Dickson's *History of the Theory of Numbers*. Around this theory may obviously be developed practically the whole of the theory of chapters XV, XVI, XVII, and VI; and it has important connections with chapters I, III, V, VII, and XIV, as one may readily see; that one may also bring into relation with it certain parts of chapter VIII is apparent from our §5 below.

It thus appears that the general theory of recurrent sequences of integers may be used as a unifying element for a significant portion of that part of the theory of numbers which has been treated in the volume mentioned. So far as I am aware, no systematic analysis of this theory has been made with reference to the problem of generalization and extension in such a way as to lead to further unification. What unification is brought about by the theory in its present state seems to have been accidental rather than purposed or foreseen; and yet what is present is significant. It appears that there is some ground to hope that further progress toward coordinating what are now diverse elements might be made here both by particular investigations undertaken with this in mind and by a systematic exposition from this point of view. One must not expect too much from such an investigation; but even the probable partial successes which are to be anticipated will justify the effort required.

4. *Propositions Discovered by Fermat.* On a previous occasion[1] I have insisted on the fact that many of the results announced by Fermat (See list in his *Oeuvres*, Vol. IV, pp. 231–237) may be associated closely with the properties of recurrent sequences of integers. In fact, a systematic examination of this matter brings out the following facts:—

(1) The results which may be derived readily from this theory by further methods known to have been employed by Fermat comprise about one-third of his principal discoveries in the theory of numbers as listed on pp. 231–237 of the fourth volume of his *Oeuvres*.

(2) In interest and value these results are fully up to the high level of Fermat's work in general.

(3) Approximately another third in the list in Fermat's *Oeuvres* may be selected of such sort that one can see from Fermat's writings a natural way by which he was led to each result in such portion of the total list and to its proof.

(4) Of the remaining third it can be determined from Fermat's work itself that some of the most remarkable of them were by him associated with the

[1] Quarterly Journal of Mathematics, vol. 48 (1920), pp. 363–372.

results which may readily be derived from the theory of recurrent sequences of integers; as, for instance, the fact that the theorem about polygonal numbers is a consequence of the fact that every prime of the form $4x+1$ is a sum of two squares.

Moreover, an analysis of the proofs of the general theorems about these recurrent sequences, with reference to the simplifications which would result for just the cases actually to be used in deriving Fermat's theorems, reveals the fact that the proofs in these cases are of extremely simple character and involve only those conceptions into which Fermat may naturally have been led from certain other matters to which he is known to have given much attention.

Furthermore, the theory of these recurrent sequences has many elements analogous to the theory of singly periodic functions; and this suggests inevitably the question whether there is a corresponding situation in the theory of numbers (not yet brought to explicit notice, to be sure) in which we should have elements corresponding to the theory of doubly periodic functions.

These considerations tend to suggest the conjecture that we may have in the theory of recurrent sequences of integers a reconstruction (and extension) of certain of the methods employed by Fermat in some of his most remarkable discoveries in the theory of numbers. While the evidence is of too uncertain a character to justify insistence upon the conjecture it is yet true that there is too much plausibility in the suggestion for it to be ignored in presence of the fact that Fermat's work is so important both in the history of the theory of numbers and with respect to its actual content in its present state.

In order to make clear the nature of the relations insisted upon, we present a few instances of theorems of Fermat which belong to the range of ideas now in consideration.

One of Fermat's important results is the following: If p is an odd prime number and a^t is the lowest power of a, such that a^t-1 is divisible by p, then t is a factor of $p-1$; if t is odd no number of the form a^t+1 is divisible by p; if t is the even number 2τ, then $a^\tau+1$ is divisible by p. All these propositions follow readily from the theory of recurrent sequences of integers.

If q is a prime divisor of 2^p-1, when p is a prime, then the restricted characteristic number modulo q of the sequence 2^n-1, $n=0, 1, \cdots$, as to the chief subset $(0, 1)$ is a divisor of p, and hence equal to p. Therefore p is a factor of $q-1$, as asserted by Fermat.

It is obvious that the Fermat numbers $2^{2^\tau}+1$ are intimately associated with the theory of recurrent sequences.

As a final example, let us consider the properties of an odd prime factor p of the sum a^2+b^2 of two relatively prime squares. For D_n we now take $D_n=(a^n-b^n)/(a-b)$. Then we have

$$D_0 = 0,\ D_1 = 1,\ D_2 = a + b,\ D_3 = a^2 + ab + b^2,\ D_4 = (a + b)(a^2 + b^2).$$

Then we see that the restricted characteristic number modulo p of the sequence $D_0, D_1, D_2, \cdots$ as to the chief subset $(0, 1)$ is 4; whence it follows from the general theory that $p-1$ is divisible by 4, or that p is of the form $4x+1$. That is, every odd prime factor of the sum of two relatively prime squares is of the form $4x+1$. Thence we have readily other results stated by Fermat: No divisor of a sum of two relatively prime squares can be of the form $4x-1$; no number of the form $4x-1$ can be the sum of two squares, either integral or fractional; no number of the form $9x\pm 3$ can be the sum of two squares, either integral or fractional.

If we turn to the converse of the theorem that every odd prime factor p of the sum of two relatively prime squares is of the form $4x+1$ we may derive readily (by means of recurrent sequences) the conclusion that every prime of the form $4x+1$ is a factor of the sum of two relatively prime squares. Having reached this stage one observes that certain of these primes $4x+1$ may actually be represented as the sum of two squares, and naturally raises the question whether this is a common property of all of them. That this question is to be answered in the affirmative is then readily shown by the method of infinite descent, a method known to have been employed by Fermat in proving this theorem.

Such considerations as these lead to a realization of the fact that many of the apparently unrelated theorems stated by Fermat constitute so many fragments of a general theory of certain particular classes of recurrent sequences of integers.

5. *Galois Fields. Higher Congruences.* In order to associate the Galois field theory with the theory of recurrent sequences of integers, let us consider a primitive mark ω of the Galois field $GF[p^k]$ where p is a prime and k is a positive integer. Then integers $c_1, c_2, \cdots, c_k$ exist in the field such that

$$\omega^k = c_1\omega^{k-1} + c_2\omega^{k-2} + \cdots + c_{k-1}\omega + c_k. \tag{7}$$

Thence it follows that integers $u_n^{(1)}, u_n^{(2)}, \cdots, u_n^{(k)}$ exist such that

$$\omega^n = u_n^{(1)}\omega^{k-1} + u_n^{(2)}\omega^{k-2} + \cdots + u_n^{(k-1)}\omega + u_n^{(k)}. \tag{8}$$

Moreover, when $0 \leqq n < k$ we have $u_n^{(i)}$ equal to zero except when $n = k-i$ in which case the value is 1. Multiplying (8) by ω and employing (7) we have

$$\omega^{n+1} = u_n^{(1)}(c_1\omega^{k-1} + c_2\omega^{k-2} + \cdots + c_k) + u_n^{(2)}\omega^{k-1} + u_n^{(3)}\omega^{k-2} + \cdots + u_n^{(k)}\omega.$$

Comparing this equation with what is obtained from (8) on replacing n by $n+1$ we see that

$$\begin{aligned} u_{n+1}^{(1)} &= c_1u_n^{(1)} + u_n^{(2)}, \\ u_{n+1}^{(2)} &= c_2u_n^{(1)} + u_n^{(3)}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ u_{(n+1)}^{(k-1)} &= c_{k-1}u_n^{(1)} + u_n^{(k)}, \\ u_{n+1}^{(k)} &= c_ku_n^{(1)}. \end{aligned} \tag{9}$$

Eliminating from this system all the functions u except $u_n^{(1)}$ we find that $u_n^{(1)}$ is a solution of the following recurrence equation:

$$u_{n+k} = c_1 u_{n+k-1} + c_2 u_{n+k-2} + \cdots + c_n u_n . \tag{10}$$

Thence it is obvious that each of the functions $u_n^{(1)}, u_n^{(2)}, \cdots, u_n^{(k)}$ satisfies this recurrence relation. They are then uniquely determined by the help of their initial values as already given. (It is to be observed that the function-values may be reduced modulo p to numbers of the set $0, 1, 2, \cdots, p-1$.) It may be seen from (8) that $u_n = \omega^n$ is a solution of (10) in the $GF[p^k]$, whence it follows that the successive powers of a primitive mark in a $GF[p^k]$ satisfy a recurrence relation of order k with integral coefficients.

That p^k-1 is the characteristic number modulo p of the sequence $u_n^{(1)}$, $n=0, 1, 2, \cdots$, follows readily from the fact that the order of ω is p^k-1, proof being made by means of (9) and (8). Hence for every prime p and given k there exists a recurrence relation (10) with integral coefficients such that p^k-1 is the characteristic number modulo p of that solution of equation (10) for which $0, 0, \cdots, 0, 1$ are the initial constants. It may be shown that this is a property of prime numbers which belongs to no composite number.

Consider now the k solutions $u_n^{(1)}, u_n^{(2)}, \cdots, u_n^{(k)}$ of equation (10) where n ranges over the set $0, 1, 2, \cdots$. The corresponding sequences may be indicated as in the following array:

$$\begin{array}{lllll}
000\cdots 001 & u_k^{(1)}, & u_{k+1}^{(1)}, & u_{k+2}^{(1)}, & \cdots, \\
000\cdots 010 & u_k^{(2)}, & u_{k+1}^{(2)}, & u_{k+2}^{(2)}, & \cdots, \\
\cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots \\
010\cdots 000 & u_k^{(k-1)}, & u_{k+1}^{(k-1)}, & u_{k+1}^{(k-1)}, & \cdots, \\
100\cdots 000 & u_k^{(k)}, & u_{k+1}^{(k)}, & u_{k+2}^{(k)}, & \cdots,
\end{array}$$

Now consider the p^k-1 ordered sets of k elements each, one set being formed from each of the first p^k-1 columns of the foregoing array by taking the elements in order in such a column beginning at the top and reducing each modulo p to a number of the set $0, 1, \cdots, p-1$. Then no two of these p^k-1 columns give rise to the same symbol, and no one of the symbols consists entirely of zeros. Hence the p^k-1 symbols may be denoted by $(\lambda_1, \lambda_2, \cdots, \lambda_k)$ where each of the λ's is a number of the set $0, 1, \cdots, p-1$ and in no symbol are all the λ's zero. Adjoin the symbol $(0, 0, \cdots, 0)$. The p^k symbols may then be used to represent the marks of the Galois field $GF[p^k]$ with the rules of addition and multiplication defined as follows: the element $(0, 0, \cdots, 0)$ enjoys both the additive and the multiplicative properties of 0; the sum of any two symbols is defined as the symbol obtained from the given symbols by adding corresponding elements and reducing modulo p to numbers of the set $0, 1, 2, \cdots, p-1$; the product of the elements formed from the mth column and the nth column is the element formed from the $(m+n-1)$th column. It is not difficult to show that the elements so defined, together with the defined operations of addition and multiplication, constitute the $GF[p^k]$. Thus the Galois field theory is exhibited as belonging to the general theory of recurrent sequences of integers reduced modulo p where p is a prime number.

From this conclusion it may be seen that a significant part of the general theory of higher congruences may be intimately associated with the recurrent sequences here in consideration.

If the theory of the finite geometries is considered as a geometric phrasing of certain matters in the theory of numbers, then this division of number theory is intimately connected with recurrent sequences of integers. Thence one is led to a large part of the theory of Abelian groups, as is shown by the connection of that theory with the finite geometries.

We have now said enough to make it apparent that a considerable and a highly significant portion of that part of the theory of numbers analyzed in the first volume of Dickson's history of number theory is capable of a marked unification through a treatment of it in intimate connection with the theory of recurrent sequences. We have not had time to go into details. But the results presented indicate that here is an important work of exposition (and, to a smaller extent, of discovery) which should be carried out systematically. It would certainly bear fruit of interest.

6. *Connections with Finite Groups.* Perhaps I may be allowed a digression from the main theme of the paper for the purpose of presenting an empirical connection between some of the numbers here treated and certain properties of groups of finite order.

In 1905 (Göttingen Nachrichten) Dickson presented the following conjectured theorem, which he verified numerically in a wide range without however obtaining a proof of its validity:

I. If G is any group of order p^n-1, where p is a prime and n is an odd integer greater than two, then G contains a self-conjugate subgroup of order a power of a prime q, where q is a factor of p^n-1 but not of any p^m-1 where $0<m<n$.

Dickson found a need for this theorem in investigating the existence of certain finite algebras which generalize Galois fields. The problem of the existence of these algebras is intimately connected with that of the existence of doubly transitive groups of degree p^n and order $p^n(p^n-1)$. In connection with a study of the latter problem I have lately encountered a need for just such a theorem; and in analyzing the matter have come to raise several questions concerning theorems analogous to that conjectured by Dickson.

Dickson verified the foregoing theorem for the cases of 144 values of p^n-1. These I have checked and have continued the verification through 15 additional cases. Neither of us found any exception to the theorem.

The foregoing theorem is intimately connected with the following:

II. When α and β are real and the exceptional cases of theorem V of §3 are excluded (as far as may be necessary) and when n is odd and greater than 2, then a group G of order $D_n(\alpha,\beta)$ has a self-conjugate subgroup whose order is of the form $q^t(t>0)$ where q is a characteristic prime factor of $D_n(\alpha,\beta)$.

No method has been discovered which so much as promises to yield a proof of this theorem. A verification has been carried out for each of 230 cases for orders $D_n(\alpha, \beta)$; and no failure of the theorem has been discovered. For the purposes of this verification I have employed the known tables of factors of the numbers $D_n(\alpha, \beta)$ for particular values of α and β and indeed have constructed some additional tables for the problem in hand. Owing to the rapid increase of $D_n(\alpha, \beta)$ for increasing n (α and β being fixed) it is very laborious to obtain tables with a large number of entries.

The examination of these propositions has led to the consideration of others, the principal ones of which will be mentioned.

III. This is theorem I with the removal from the hypothesis of the condition that n shall be odd and with the further restriction that $n \neq 4, 6$.

This has been verified for 183 values of $p;-1$, twenty-four of them being cases for which n is even. The presence of the named exceptional cases indicates the possible presence of others.

IV. This is theorem II with the removal from the hypothesis of the condition that n shall be odd.

This theorem has been verified for 285 cases of values of $D_n(\alpha, \beta)$, fifty-five of the verifications being for even values of n.

A theorem implied by, but (apparently) not implying, theorem IV is the following:

V. When α and β are real and the exceptional cases of theorem IV of §3 are excluded, then a group G of order $F_n(\alpha, \beta)$, $n > 2$, contains a self-conjugate subgroup whose order is of the form $q^t (t > 0)$ where q is a prime factor of $F_n(\alpha, \beta)$ but is not a factor of n.

This theorem has been verified for each of 639 cases for the order $F_n(\alpha, \beta)$. It was found indeed that for each of these cases a Sylow subgroup serves for the invariant subgroup whose existence is asserted by the theorem.

In the case of propositions III and IV the conclusion may be weakened without destroying the value of the resulting theorems, if in their weaker form it should be possible to prove them. Writing $n = 2\nu$, we may thus weaken the conclusion by allowing q to be a characteristic factor of either $p^{2\nu} - 1$ or of $p^\nu - 1$ in the case of theorem III and of either $D_{2\nu}$ or D_ν in the case of theorem IV.

No one of the foregoing five theorems has been proved, and indeed no possible method of proof is apparent. No exception has been found to any one of them. So far as I have been able to find out, some characteristics of these propositions do not appear in any of the demonstrated theorems in group theory. If this opinion is well founded, then these propositions deserve especial attention; and that is my reason for calling them to your notice. If the propositions are true a demonstration of them would establish an interesting connection between group theory and the additive theory of numbers; for here the orders of the groups are determined by additive means while the conjectured properties of the groups have to do with fundamental matters pertaining to the structure of these groups.