the motion of an infinite linear system of discrete masses, connected by springs. The solution is obtained indirectly by a limiting process from the solution for a finite number of masses, and is then verified directly. The main features of the oscillations of a given mass are interpreted in terms of familiar properties of the Bessel functions of the time which occur as coefficients.

H. E. SLAUGHT,
Secretary of the Section.

THE DECOMPOSITION OF MODULAR SYSTEMS CONNECTED WITH THE DOUBLY GENERALIZED FERMAT THEOREM.

BY PROFESSOR ELIAKIM HASTINGS MOORE.

(Read before the Chicago Section of the American Mathematical Society, December 29, 1898.)

Introduction. The Generalized Fermat Theorem (A) in Purely Arithmetic Phrasing (A', A'') with Extension (A'''). §§ 1–5.

1. The theorem * in question is the following:

(*A*) In the Galois field $GF[p^n]$ of prime modulus p and of rank n the two forms each of degree $(p^{n(k+1)}-1)/(p^n-1)$ in the $k+1$ indeterminates $X_0, X_1, \cdots, X_k$

$$D_{k+1,n,p}[X_0, X_1, \cdots, X_k] = |X_j^{p^{ni}}| \qquad (i, j = 0, 1, \cdots, k)$$

$$P_{k+1,n,p}[X_0, X_1, \cdots, X_k] = \prod_{g=0,k} \prod_{\alpha_{fg}|p^n} (X_g + \sum_{f=0,g-1} \alpha_{fg} X_f)$$

are identical:

$$D_{k+1,n,p}[X_0, \cdots, X_k] = P_{k+1,n,p}[X_0, \cdots, X_k].$$

Here the subscript remark $\alpha_{fg}|p^n$ indicates that the mark α_{fg} is to run over the p^n marks of the Galois field $GF[p^n]$, and for the case $g=0$ the final $\sum_{f=0,g-1}$ does not enter.

For this theorem, which for $(k, n) = (1, 1)$ is one form of Fermat's theorem, I have given three proofs, couched as is the statement of the theorem in the abstract Galois field phrasing introduced by me in the paper "A doubly-infinite system of simple groups" presented to the Chicago Congress of 1893.

* Moore, "A two-fold generalization of Fermat's theorem," BULLETIN, vol. 2 (1896), pp. 189–199.

In the development of the Galois field theory and in its applications to algebra and groups this abstract phrasing is very convenient.

2. Here however we are interested in converses of the theorem stated above; after replacing the marks α_{fg} by functions of the realm $[1, y]$ we decompose, in the sense of equivalence, into prime modular systems the modular system $\mathfrak{M}$ whose elements are the coefficients of various powers of the indeterminates in the form

$$M_{k+1,\,n,\,p} \equiv D_{k+1,\,n,\,p} - P_{k+1,\,n,\,p}.$$

We need first to use the concrete purely arithmetic phrasings of Serret and Kronecker. The $GF[p^n]$ is then the totality of p^n classes (abstractly, marks) of rational integral functions of an indeterminate y with integral coefficients (forming the realm of integrity $[1, y]$) considered with respect to a (prime) modular system $[p, F_n[y]]$, where $F_n[y]$ is a function of the realm $[1, y]$ of degree n (a polynomial in y with integral coefficients) irreducible modulo p. We operate with these classes by operating with representative functions with respect to the modular system $[p, F_n[y]]$. For the marks α we may take the p^n reduced functions

$$a_0 + a_1 y + a_2 y^2 + \cdots + a_{n-1} y^{n-1},$$

where the n coefficients $a_0, \cdots, a_{n-1}$ take independently the values $0, 1, 2, \cdots, p-1$. There are in this sense as many concretely distinct Galois fields as there are functions $F_n[y]$ congruentially distinct modulo p. These Galois fields are however abstractly identical.

We restate theorem

(A') In the realm of integrity $[1, y]$ the two forms each of degree $(p^{n(k+1)} - 1)/(p^n - 1)$ in the $k+1$ indeterminates $X_0, \cdots, X_k$

$$D_{k+1,\,n,\,p}[X_0, \cdots, X_k] = |X_j^{p^{ni}}| \quad (i, j = 0, 1, \cdots, k)$$

$$P_{k+1,\,n,\,p}[X_0, \cdots, X_k] = \prod_{g=0,\,k} \prod_{a_{fgl}=0,\,p-1} \left(X_g + \sum_{f=0,\,g-1} X_f \sum_{l=0,\,n-1} a_{fgl} y^l\right)$$

are identically * congruent ($\equiv$):

* In pure arithmetic all identities and identical congruences are *formal* in certain specified indeterminates.

$$D_{k+1,n,p}[X_0, \cdots, X_k] \equiv P_{k+1,n,p}[X_0, \cdots, X_k] \quad [p, F_n[y]],$$

with respect to every prime modular system $[p, F_n[y]]$, where p is a prime and $F_n[y]$ is any function of $[1, y]$ of degree n and irreducible modulo p.

3. I take as known the fundamental definitions and elementary theorems of Kronecker's theory of modular systems, in particular with respect to the composition and equivalence of modular systems. It is however desirable to fix the notations * to be used here.

A realm $\mathfrak{R}$ of integrity-rationality

$$\mathfrak{R} = [R_1 \cdots, R_\mu](R_{\mu+1}, \cdots, R_{\mu+\nu})$$

consists of all functions

$$F[R_1, \cdots, R_\mu](R_{\mu+1}, \cdots, R_{\mu+\nu})$$

rational integral in $R_1, \cdots, R_\mu$ and rational in $R_{\mu+1}, \cdots, R_{\mu+\nu}$, the coefficients being integers. These functions are called the *quantities* of the realm. The realm is closed under addition, subtraction, and multiplication, and likewise under division by any function not 0 of $\mathfrak{R}' = (R_{\mu+1}, \cdots, R_{\mu+\nu})$.

Any set of quantities $F_1, \cdots, F_m$ of a realm $\mathfrak{R}$ constitutes a modular system $\mathfrak{F} = [F_1, \cdots, F_m]$ of that realm. The whole theory of such modular systems relates to the underlying realm.

Any set of modular systems

$$\mathfrak{F}_i = [F_{i1}, \cdots, F_{im_i}] \qquad (i = 1, 2, \cdots, m)$$

determines a modular system $[\cdots F_{ij_i} \cdots {}^{i=1,\cdots,m}_{j_i=1,\cdots,m_i}]$ for which we use the notation $[\mathfrak{F}_1, \cdots, \mathfrak{F}_m]$.

(1) The theorem:

If

$$[\mathfrak{F}_1, \mathfrak{F}_2, \mathfrak{F}] \sim [1],$$

then

$$[\mathfrak{F}_1, \mathfrak{F}][\mathfrak{F}_2, \mathfrak{F}] \sim [\mathfrak{F}_1\mathfrak{F}_2, \mathfrak{F}],$$

and its useful generalization:

If

$$[\mathfrak{F}_i, \mathfrak{F}_j, \mathfrak{F}] \sim [1] \qquad (i \neq j;\ i, j = 1, \cdots, m),$$

* The notations are those of my paper "The decomposition of modular systems of rank n in n variables," BULLETIN, vol. 3 (1897), pp. 372-380.

then

$$\prod_{i=1,\,m} [\mathfrak{F}_i, \mathfrak{F}] \sim [\prod_{i=1,\,m} \mathfrak{F}_i, \mathfrak{F}]:$$

may readily be proved.

(2) A system $\mathfrak{F}$ of the realm $\mathfrak{R}$ I call *prime* * in case (α) $\mathfrak{F}$ and [1] are not equivalent and (β) for any quantity G of the realm we have one of the alternative equivalences

$$[\mathfrak{F}, G] \sim \mathfrak{F} \quad \text{or} \quad [\mathfrak{F}, G] \sim [1],$$

that is, one of the alternative congruences

$$G \equiv 0 [\mathfrak{F}] \quad \text{or} \quad GG' \equiv 1 [\mathfrak{F}],$$

where in the latter case G' is a properly determined quantity of the realm.

For a prime system $\mathfrak{F}$ in connection with any system $\mathfrak{G}$ we have one of the alternatives

$$[\mathfrak{F}, \mathfrak{G}] \sim \mathfrak{F} \quad \text{and} \quad \mathfrak{G} \equiv 0 [\mathfrak{F}] \quad \text{or} \quad [\mathfrak{F}, \mathfrak{G}] \sim [1],$$

that is, any system $\mathfrak{G}$ contains or is relatively prime to a prime system $\mathfrak{F}$.

We have the fundamental theorem:

If $\mathfrak{F}$ is prime and the product $\mathfrak{G}_1\mathfrak{G}_2$ of two systems $\mathfrak{G}_1, \mathfrak{G}_2$ contains $\mathfrak{F}$, while $\mathfrak{G}_1$ does not contain $\mathfrak{F}$, then $\mathfrak{G}_2$ does contain $\mathfrak{F}$.

For $\mathfrak{G}_1\mathfrak{G}_2 \equiv 0 [\mathfrak{F}]$ and $\mathfrak{G}_1 \not\equiv 0 [\mathfrak{F}]$ and hence, since $\mathfrak{F}$ is prime, $[\mathfrak{F}, \mathfrak{G}_1] \sim [1]$. Now $\mathfrak{F}\mathfrak{G}_2 \equiv 0 [\mathfrak{F}]$. Hence we have $[\mathfrak{F}, \mathfrak{G}_1]\mathfrak{G}_2 \equiv 0 [\mathfrak{F}]$, and so indeed $\mathfrak{G}_2 \equiv 0 [\mathfrak{F}]$.

(3) If $[\mathfrak{F}, \mathfrak{G}_i] \sim [1]$ ($i = 1, 2, \cdots, m$), then

$$[\mathfrak{F}, \prod_{i=1,\,m} \mathfrak{G}_i] \sim \prod_{i=1,\,m} [\mathfrak{F}, \mathfrak{G}_i] \sim [1].$$

(4) If $[\mathfrak{F}_i, \mathfrak{F}_j] \sim [1]$ ($i \neq j$; $i, j = 1, 2, \cdots, m$) and $\mathfrak{M} \equiv 0$ $[\mathfrak{F}_i]$ ($i = 1, 2, \cdots, m$), then $\mathfrak{M} \equiv 0 [\mathfrak{F}]$ where $\mathfrak{F} = \prod_i \mathfrak{F}_i$.

4. We are now to work in the realm of integrity $\mathfrak{R}_1 = [1, y]$, where y is an indeterminate. There are in all say m functions $F_n[y]$ of $\mathfrak{R}_1$ congruentially distinct (mod. p) and each of degree n and irreducible mod. p; we write them $F_{nj}[y] (j = 1, \cdots, m)$. The modular systems $\mathfrak{F}_{nj} = [p, F_{nj}[y]] (j = 1, \cdots, m)$ are

* Kronecker's prime modular system of a given rank (*Jour. für Mathematik*, vol. 99, p. 337) is differently defined.

all prime and by pairs relatively prime. We write their product

$$\mathfrak{F}_n = \prod_{j=1,m} \mathfrak{F}_{nj} = \prod_{j=1,m} [p, F_{nj}[y]] \sim [p, \prod_{j=1,m} F_{nj}[y]].$$

5. We set (using the notations of § 2)

$$M_{k+1,n,p}[X_0, \cdots, X_k] = D_{k+1,n,p}[X_0, \cdots, X_k] - P_{k+1,n,p}[X_0, \cdots, X_k]$$

and denote by $\mathfrak{M}_{k+1,n,p}$ the modular system of coefficients of $M_{k+1,n,p}[X_0, \cdots, X_k]$; this system $\mathfrak{M}$ belongs to the realm $\mathfrak{R}_1 = [1, y]$.

Our theorem A'(§ 2) is then

$$(A'') \qquad \mathfrak{R}_{k+1,n,p} \equiv 0 \ [\mathfrak{F}_{nj}] \qquad (j = 1, \cdots, m),$$

whence follows in accordance with § 4 and § 3 (4),

$$(A''') \qquad \mathfrak{M}_{k+1,n,p} \equiv 0 \ [\mathfrak{F}_n].$$

The Equivalence Theorem (*B*) *and the Decomposition Theorem* (*C*) §§ 6–14.

6. We are to prove the equivalence

$$(B) \qquad \mathfrak{M}_{k+1,n,p} \sim \mathfrak{F}_n,$$

whence in view of § 4 follows the decomposition, in the sense of equivalence, of the system $\mathfrak{M}_{k+1,n,p}$, viz.,

$$(C) \qquad \mathfrak{M}_{k+1,n,p} \sim \prod_{j=1,m} \mathfrak{F}_{nj},$$

that is, its exhibition as a product of systems no further decomposable and indeed in this case prime.

7. To prove (*B*) we need to prove, (A''') being admitted, merely the converse of (A'''), viz.,

$$(\bar{A}''') \qquad \mathfrak{F}_n \equiv 0 \quad [\mathfrak{M}_{k+1,n,p}].$$

Here $\mathfrak{F}_n$ depends upon n and p and not on k. The congruence ($\bar{A}'''$) follows from the following two congruences:

$$(\bar{A}'''_{k=1}) \qquad \mathfrak{F}_n \equiv 0 \quad [\mathfrak{M}_{2,n,p}],$$

$$(D) \qquad \mathfrak{M}_{2,n,p} \equiv 0 \quad [\mathfrak{M}_{k+1,n,p}],$$

of which the former is the particular case of $(\bar{A}''')$ for $k = 1$. We shall, however, prove (D) and then (B, C) without the mediation of $(\bar{A}'''_{k=1})$.

8. Proof of (D). The obviously true congruence

$$\mathfrak{M}_{k+1,\,n,\,p} \equiv 0 \quad [\mathfrak{M}_{k+1,\,n,\,p}]$$

implies the identical congruence

$$M_{k+1,\,n,\,p}[X_1, X_1, \cdots, X_0] \equiv 0 \quad [\mathfrak{M}_{k+1,\,n,\,p}]$$

in the $k+1$ indeterminates $X_0, \cdots, X_k$. Considering in particular the terms of M with the literal part containing the factor $X_2^{p^{2n}} \cdots X_i^{p^{in}} \cdots X_k^{p^{kn}}$, we have the identical congruence in X_0, X_1

$$(X_0X_1^{p^n} - X_1X_0^{p^n}) - \prod_{\substack{a_0 \ldots a_{n-1} \\ =0,\,p-1}} (X_1 + X_0\overline{a_0 + a_1y + \cdots + ay^l + \cdots + a_{n-1}y^{n-1}}) \equiv 0 \quad [\mathfrak{M}_{k+1,\,n,\,p}],$$

that is,

$$M_{2,\,n,\,p}[X_0, X_1] \equiv 0 \quad [\mathfrak{M}_{k+1,\,n,\,p}],$$

and so in fact we have

$$(D) \qquad \mathfrak{M}_{2,\,n,\,p} \equiv 0 \quad [\mathfrak{M}_{k+1,\,n,\,p}].$$

9. We consider in preparation for the proof of (B, C) (§ 11) various properties of the system $\mathfrak{M} = \mathfrak{M}_{k+1,\,n,\,p}$, consequences of the identical congruence

$$M[X_0, X_1] = D[X_0, X_1] - P[X_0, X_1] = (X_0X_1^{p^n} - X_1X_0^{p^n}) - \prod_{\substack{a_0 \ldots a_{n-1} \\ =0,\,p-1}} (X_1 + X_0\overline{a_0 + a_1y + \cdots + a_ly^l + \cdots + a_{n-1}y^{n-1}}) \equiv 0\,[\mathfrak{M}];$$

this congruence obviously true for $\mathfrak{M} = \mathfrak{M}_{2,\,n,\,p}$ is by (D) true for $\mathfrak{M} = \mathfrak{M}_{k+1,\,n,\,p}$.

(1) G being any quantity $G = a_0 + a_1y + \cdots + a_{n-1}y^{n-1}$ of our realm $\mathfrak{R}_1 = [1, y]$ of degree in y at most $n-1$ with coefficients a_l each 0 or positive integers less than p but not all 0, we have

$$[\mathfrak{M}, G] \sim [1],$$

and so there is a quantity G' of $\mathfrak{R}_1$ such that

$$GG' \equiv 1 \quad [\mathfrak{M}].$$

Proof. Since $\mathfrak{M} \equiv 0 \quad [\mathfrak{M}, G]$ we have

$$D[X_0, X_1] \equiv P[X_0, X_1] \quad [\mathfrak{M}, G].$$

Now $P[X_0, X_1]$ has the distinct factors X_1 and $X_1 + GX_0$ and other factors with product say $Q[X_0, X_1]$; hence

$$P[X_0, X_1] \equiv X_1^2 Q[X_0, X_1] \quad [G]$$

and so, since $G \equiv 0 [\mathfrak{M}, G]$,

$$P[X_0, X_1] \equiv X_1^2 Q[X_0, X_1] \quad [\mathfrak{M}, G].$$

Hence

$$D[X_0, X_1] \equiv X_1^2 Q[X_0, X_1] \quad [\mathfrak{M}, G].$$

The term $X_1 X_0^{p^n}$ gives the congruence

$$-1 \equiv 0 \quad [\mathfrak{M}, G],$$

that is, $[1] \equiv 0 [\mathfrak{M}, G]$, and, since $[\mathfrak{M}, G] \equiv 0 \; [1]$, we have proved that $(\mathfrak{M}, G] \sim [1]$.

(2°) There is an integer g for which

$$pg \equiv 0 \quad [\mathfrak{M}] \quad \text{and} \quad [p, g] \sim [1].$$

Proof. From the identical congruence by the substitution $(X_0, X_1) = (1, -\overline{p-1})$ we have a congruence identical in y, and the term y° gives the congruence

$$(-\overline{p-1})^{p^n} + \overline{p-1} \equiv 0 \quad [\mathfrak{M}],$$

whence follows the statement (2) in case $p = 2$ for $g = 1$ at once, and in case $p > 2$ for $g = (\overline{p-1}^{p^n} - \overline{p-1})/p$ by the remark that $pg \equiv -p \; [p^2]$ and so $g \equiv -1 \; [p]$.

$$p^{p^{n-1}} \equiv 0 \quad [\mathfrak{M}]. \tag{3}$$

Proof. In case $p = 2$ (3) follows at once from (2), $2 \equiv 0 \; [\mathfrak{M}]$, as proved for $p = 2$. In case $p > 2$ the coefficient of $X_0^2 X_1^{p^n - 1}$ gives

$$[\tfrac{1}{2}p(p-1)]^{p^{n-1}} \cdot (1 + y + \cdots + y^{n-1}) \equiv 0 \quad [\mathfrak{M}].$$

Setting $G_1 = \frac{1}{2}(p-1)$ and $G_2 = 1 + \cdots + y^{n-1}$ we have (1) quantities G_1', G_2' of $\mathfrak{R}_1$ for which $G_1 G_1' \equiv 1$, $G_2 G_2' \equiv 1$ $[\mathfrak{M}]$, and obtain (3) in multiplying the congruence just written by $G_1'^{p^{n-1}} G_2'$.

(4) $$p \equiv 0 \quad [\mathfrak{M}].$$

Proof. From (2), $[p, g] \sim [1]$, it follows by § 3 (3) that $[p^{p^{n-1}}, g] \sim [1]$, that is, for properly determined g', $gg' \equiv 1$ $[p^{p^{n-1}}]$, so that by (3) $gg' \equiv 1$ $[\mathfrak{M}]$, whence from (2), $pg \equiv 0$ $[\mathfrak{M}]$ we have the desired congruence (4).

(5) $$y^{p^n} - y \equiv 0 \quad [\mathfrak{M}].$$

Proof. (5) follows from the identical congruence by the substitution $(X_0, X_1) = (1, y)$ with the remark that, since $P[X_0, X_1]$ has the factor $X_1 + \overline{p-1} y X_0$, $P[1, y] \equiv 0$ $[p]$ and so by (4) $P[1, y] \equiv 0$ $[\mathfrak{M}]$.

10. We need further the known decomposition

$$[p, y^{p^n} - y] \sim \prod_d \prod_{j=1, m_d} [p, F_{dj}[y]],$$

where for every divisor d of n the $F_{dj}[y] (j = 1, \cdots, m_d)$ are the say m_d quantities of $\mathfrak{R}_1$ congruentially distinct and each of degree d and irreducible modulo p. We may and do suppose that the coefficients of the $F_{dj}[y]$ are taken from the integers $0, 1, \cdots, p-1$. Here the $F_{nj}[y]$ are the $F_{nj}[y]$ of § 4; $m_n = m$. The systems $[p, F_{dj}[y]]$ are by pairs relatively prime.

11. Proof of (B, C): $\mathfrak{M} \sim \mathfrak{F}_n \sim \prod_{j=1, m} \mathfrak{F}_{nj}$. We have from § 9 (4, 5)

$$\mathfrak{M} \sim [\mathfrak{M}, p, y^{p^n} - y],$$

whence by § 10 and § 3 (1) we have the decomposition

$$\mathfrak{M} \sim \prod_d \prod_{j=1, m_d} [\mathfrak{M}, p, F_{dj}[y]],$$

and so, since $[\mathfrak{M}, F_{dj}[y]] \sim [1]$ for $d < n$ (§ 9, 1),

$$\mathfrak{M} \sim \prod_{j=1, m} \{\mathfrak{M}, p, F_{nj}[y]\},$$

that is, in the notation of § 4,

$$\mathfrak{M} \sim \prod_{j=1,\,m} [\mathfrak{M}, \mathfrak{F}_{nj}].$$

Now by (A'') $\mathfrak{M} \equiv 0\ [\mathfrak{F}_{nj}]$ and so $[\mathfrak{M}, \mathfrak{F}_{nj}] \sim \mathfrak{F}_{nj}$, and thus we have finally

$$(B,C) \quad \mathfrak{F} \sim \prod_{j=1,\,m} \mathfrak{F}_{nj} \sim \mathfrak{F}_n.$$

12. It is noteworthy that the modular system $\mathfrak{M} = \mathfrak{M}_{k+1,\,n,\,p}$ is in the sense of equivalence in fact independent of k and dependent only on n and p,

$$\mathfrak{M}_{k+1,\,n,\,p} \sim \mathfrak{F}_n \sim \mathfrak{M}_{2,\,n,\,p}.$$

13. My exhibition of the system $\mathfrak{F}_n$ by its equivalent $\mathfrak{M}_{k+1,\,n,\,p}$ for k any positive integer, the elements of $\mathfrak{M}_{k-1,\,n,\,p}$ being the coefficients of the integral function $M_{k+1,\,n,\,p}$, is to be compared with that of Serret (Algèbre supérieure, fifth edition, volume 2, §349). In our notation we have (using §3, 1°)

$$\mathfrak{F}_n \sim \prod_{j=1,\,m} \mathfrak{F}_{nj} \sim \prod_{j=1,\,m} [p,\ F_{nj}[y]] \sim [p,\ F_n[y]],$$

where

$$F_n[y] = \prod_{j=1,\,m} F_{nj}[y].$$

Serret gives a fraction $F[y]$

$$\prod_{n_e} (y^{p^{n_e}} - y) \Big/ \prod_{n_o} (y^{p^{n_o}} - y),$$

where n_e, n_o run through those divisors of n whose complementary divisors n/n_e, n/n_o have respectively an even (or 0), an odd number of unrepeated prime factors, and shows that modulo p the division indicated by the notation of $F(y)$ can be performed and that for the resulting integral function $F[y]$ we have $F[y] \equiv F_n[y]\ [p]$ and so $\mathfrak{F}_n \sim [p,\ F[y]]$. — Apparently my exhibition lends itself more easily to investigations in the domain of pure arithmetic.

THE UNIVERSITY OF CHICAGO.