A TWO-FOLD GENERALIZATION OF FERMAT'S THEOREM.

Presented to the American Mathematical Society, February 29, 1896.

BY PROFESSOR ELIAKIM HASTINGS MOORE.

Formulation of the generalized Fermat theorem $\mathrm{III}[k+1, n; p]$. §§ 1–4.

1. In *Gauss's* congruence notation *Fermat's theorem* is:

I_1 $$a^p - a \equiv 0 \pmod{p}$$

where p is any prime and a is any integer:
or, otherwise expressed,

I_2 *The two rational integral functions of the indeterminate X with integral coefficients*

$$X^p - X, \quad \prod_{a=0}^{a=p-1} (X+a)$$

are identically congruent ($\equiv$) (mod p):

$$X^p - X \equiv \prod_{a=0}^{a=p-1} (X+a) \pmod{p}.$$

We write I_2 thus:

I_3 *The two forms in the two indeterminates X_0, X_1,*

$$D[2,1;p](X_0, X_1) \equiv X_0 X_1^p - X_0^p X_1,$$

$$P[2,1;p](X_0, X_1) \equiv X_0 \cdot \prod_{a_0=0}^{a_0=p-1} (a_0 X_0 + X_1),$$

are identically congruent (mod p):

$$D[2,1;p](X_0, X_1) \equiv P[2,1;p](X_0, X_1) \pmod{p}.$$

2. We proceed in two steps to a two-fold generalization of Fermat's theorem I_3.

II. *The two forms in the $k+1$ indeterminates $X_0, X_1, \cdots, X_k$,*

(1) $D[k+1, 1; p](X_0, X_1, \cdots, X_k) \equiv |X_j^{p^i}|$ $(i, j = 0, 1, \cdots, k)$,

(2) $P[k+1, 1; p](X_0, X_1, \cdots, X_k) \equiv \Pi^* \sum_g a_g X_g$ $(g = 0, 1, \cdots, k)$,

—where the product Π^* embraces the $(p^{k+1}-1)/(p-1)$ linear forms $\sum_{g=0}^{g=k} a_g X_g$ whose coefficients a_g $(g=0, 1, \cdots, k)$ are integers selected from the series $0, 1, \cdots, p-1$, in all possible ways, only