GALOIS FIELD TABLES FOR $p^n \leqq 169$.

BY DR. W. H. BUSSEY.

(Read before the American Mathematical Society, September 7, 1905).

EVERY field of a finite number of marks may be represented as a Galois field of order $s = p^n$, where p^n is a power of a prime. The $GF[p^n]$ is defined uniquely by its order, and is therefore independent of the particular irreducible congruence used in its construction. In each of the following tables the $GF[p^n]$ is constructed by means of a primitive irreducible congruence which appears at the top of the table. The marks of each field are arranged in two tables. In each table each mark appears as a power of a primitive root i, and also as a polynomial in i of degree $k \leqq n - 1$. The coefficients in this polynomial are integers reduced modulo p. The mark $Ai^k + Bi^{k-1} + \cdots + Di + E$, $A \neq 0$ is denoted by $AB \cdots DE$, a symbol consisting of its detached coefficients in order. Zero coefficients must not be omitted. This is the usual symbol for a positive integer in the notation of the number system whose base is p. In the first table the marks are arranged according to ascending powers of i. In the second table the marks are arranged so that the symbols $AB \cdots DE$ represent the positive integers in natural order. By means of these two tables it is possible to perform with ease the operations of addition, subtraction, multiplication and division, within the field.

For an exposition of the Galois field theory, see Dickson's Linear Groups, pages 1–54; Jordan's Traité des Substitutions, pages 14–18, pages 156–161; Serret's Algèbre supérieure. For other references on Galois fields and higher irreducible congruences, see the preface to Dickson's Linear Groups.

Example 1. Simplify $(i^7 + i^{13})(i^2 + 3i + 4)$, i being a primitive root of the $GF[7^2]$.

From the first table for $GF[7^2]$, $i^7 = 6i + 1$, $i^{13} = 3i + 3$, $i^2 = i + 4$.

Therefore $i^7 + i^{13} = 9i + 4 = 2i + 4 \pmod 7 = i^6$ (by second table).

Also $i^2 + 3i + 4 = 4i + 8 = 4i + 1 \pmod 7 = i^{22}$ (by second table).

Therefore $(i^7 + i^{13})(i^2 + 3i + 4) = i^6 \cdot i^{22} = i^{28} = 5i + 1$ (by first table).