ABSTRACTS OF PAPERS

SUBMITTED FOR PRESENTATION TO THE SOCIETY

The following papers have been submitted to the Secretary and the Associate Secretaries of the Society for presentation at meetings of the Society. They are numbered serially throughout this volume. Cross references to them in the reports of the meetings will give the number of this volume, the number of this issue, and the serial number of the abstract.

Algebra and Theory of Numbers

299. Leonard Carlitz: *Representation of a polynomial in certain forms.*

Explicit formulas are found for the representation of an irreducible polynomial P in $GF(p^n)$ in certain factorable forms of degree k in k indeterminates. For example, when $k=2$, $p\neq 2$, the form may be taken as $U^2-\alpha V^2$, where α is not a square in $GF(p^n)$. Here U is determined by the formula $2A(x)\equiv(-1)^h[1][3]\cdots[2h-1]$ (mod $P(x)$), where P is of degree $2h$, and $[i]=x^{p^{ni}}-x$ (Duke Mathematical Journal, vol. 9 (1942), pp. 234–243, p. 242). Similar results are obtained for the general case. (Received August 3, 1942.)

300. Leonard Carlitz: *Some formulas for the composition of numerical functions.*

This note is concerned with the sum $h(M)=\sum f(U)g(V)$ extended over polynomials of fixed degree k in $GF(p^n)$ such that $(\alpha+\beta)M=\alpha U+\beta V$, α, β in $GF(p^n)$; it is assumed that $f(U)$ and $g(V)$ are of the form $\sum e(D)$, where D runs through the divisors of U of degree at most $k/2$. It is found that $h(M)$ is of the same general form. In various special cases $h(M)$ can be expressed in quite simple form. In particular the formulas of the present paper include formulas occurring in the problem of representing a polynomial as the sum of an even number of squares. (Received August 3, 1942.)

301. R. P. Dilworth: *On the decomposition theory of modular lattices.*

The Kurosch-Ore decomposition theorem asserts that if an element a of a modular lattice has two reduced decompositions into irreducibles $a=p_1\frown\cdots\frown p_m=q_1\frown\cdots\frown q_n$, then each p_i may be replaced by a suitably chosen q_j. However, this leaves unanswered questions like the following: Does each q_j replace some p_i? Can different p's be replaced by different q's? The following precise result is proved: If $a=p_1\frown\cdots\frown p_m=q_1\frown\cdots\frown q_n$, then the q's can be renumbered in such a way that each p_i may be replaced by q_i. This theorem requires a much deeper analysis of the arithmetical structure of a modular lattice. For this purpose extensive use is made of the concept of an *over-divisor* which is defined as follows: a is said to *over-divide* b, or to be an *over-divisor* of b if $x\frown a=b$ implies $x=b$. (Received August 4, 1942.)