THE PROBABILITY THAT A DETERMINANT BE CONGRUENT TO a (MOD m)

N. J. FINE AND IVAN NIVEN

The problem treated is the evaluation of $P_n(a, m)$, the probability that a determinant of order n having integral elements be congruent to a modulo m. By "probability" is meant the fraction obtained by dividing the number of favorable cases by the number of possible cases: let each element of the determinant range over the values $1, 2, \cdots, m$; among the m^{n^2} possible determinants let g be the number which are congruent to a modulo m; then $P_n(a, m) = g/m^{n^2}$.

This problem has been investigated by Jordan,[1] whose solution involves the function

$$S_n(p, \lambda) = \sum p^{-(\lambda_1+\lambda_2+\cdots+\lambda_{n-1})} \qquad (n \geqq 2), \tag{1}$$

where the sum ranges over all values satisfying the inequality

$$0 \leqq \lambda_1 \leqq \lambda_2 \leqq \cdots \leqq \lambda_{n-1} \leqq \lambda.$$

We use here a different method and obtain results more explicit than (1). Our results can be obtained from Jordan's, but it is as convenient to derive them independently.

It will be convenient to use a result stated by Hull,[2] which in our notation can be written

$$P_n(a, m_1)P_n(a, m_2) = P_n(a, m_1m_2) \quad \text{if} \quad (m_1, m_2) = 1. \tag{2}$$

We shall prove

$$P_n(a, m) = P_n(q, m) \quad \text{where} \quad q = (a, m), \tag{3}$$

so that our problem has been reduced to the determination of $P_n(p^\alpha, p^k)$, p being a prime. This can be evaluated by means of

$$P_n(p^\alpha, p^k) = \{\phi(p^{k-\alpha})\}^{-1}\{P_n(0, p^\alpha) - P_n(0, p^{\alpha+1})\} \qquad (0 \leqq \alpha < k), \tag{4}$$

and

$$P_n(0, p^k) = 1 - \prod_{r=k}^{k+n-1} (1 - p^{-r}) \qquad (k \geqq 1), \tag{5}$$

Presented to the Society, November 27, 1943; received by the editors July 30, 1943.

[1] C. Jordan, *Sur le nombre des solutions de la congruence* $|a_{ik}| \equiv A$ (mod M), J. Math. Pures Appl. (6) vol. 7 (1911) pp. 409–416.

[2] Ralph Hull, *Congruences involving kth powers*, Trans. Amer. Math. Soc. vol. 34 (1932) p. 910.