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* $|a_{ik}| \equiv A \pmod{M}$, 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.

the Euler ϕ-function being involved in (4). We now prove these results.

1. **Two lemmas.** The first is due to C. Jordan.[3] Let $N_n(d, m)$ represent the number of different sets $a_1, a_2, \cdots, a_n$ of n positive integers not greater than m such that $(a_1, a_2, \cdots, a_n, m) = d$, d being any divisor of m. This, with $d = 1$, is Jordan's generalization of the Euler ϕ-function.

LEMMA 1.

$$N_n(d, m) = N_n(1, m/d);$$
$$N_n(1, ab) = N_n(1, a)N_n(1, b) \quad \textit{if} \quad (a, b) = 1;$$
$$N_n(1, p^k) = (p^k)^n - (p^{k-1})^n \quad \textit{for} \quad k \geqq 1, \quad p \textit{ any prime.}$$

The first equation reduces our function to that of Jordan, and the other equations are his.

LEMMA 2. *Let $a_1, a_2, \cdots, a_n$ be any integers such that $(a_1, a_2, \cdots, a_n, m) = 1$. Then integral solutions λ_i can be found for the congruence*

$$\sum_{i=1}^{n} a_i\lambda_i \equiv 1 \pmod{m}, \tag{6}$$

such that λ_1 is prime to m.

Let $x_1, x_2, \cdots, x_n$ be any solution of the congruence (6). Let c be defined by $c = (a_2, a_3, \cdots, a_n, m)$, so that we have $(x_1, c, m) = 1$. Also there exist integers $k_2, k_3, \cdots, k_n$ such that

$$\sum_{i=2}^{n} k_i a_i \equiv c \pmod{m}.$$

Let b be the product of those primes which divide m but not x_1. Then we set

$$\lambda_1 = x_1 + \sum_{i=2}^{n} bk_i a_i, \qquad \lambda_j = x_j - bk_j a_1 \qquad (j = 2, 3, \cdots, n),$$

noting that these give a solution of (6). We have $\lambda_1 \equiv x_1 + bc \pmod{m}$. Let p be any prime factor of m. If $p \mid x_1$, then $p \nmid b$ and $p \nmid c$. If $p \nmid x_1$, then $p \mid b$. Hence λ_1 is prime to m.

2. **A recursion formula.** Consider now the determinant of order n

[3] *Traité des substitutions*, Paris, 1870, pp. 95–97, or L. E. Dickson, *History of the theory of numbers*, vol. 1, p. 147.

with arbitrary integral elements modulo m. Let $a_1, a_2, \cdots, a_n$ and $b_1, b_2, \cdots, b_n$ designate the elements of the first two rows, respectively. We shall assume that the g.c.d. of the elements of the first row and m has been factored and placed in front of the determinant, so that $(a_1, a_2, \cdots, a_n, m) = 1$. Using Lemma 2 we choose $\lambda_1, \lambda_2, \cdots, \lambda_n$ so that (6) holds with $(\lambda_1, m) = 1$. We now apply the following transformation to the determinant. Multiply the first column by λ_1. This of course multiplies the value of the determinant by λ_1, which is immaterial since in this section we are concerned with divisibility by m, that is, with $P_n(0, m)$. Next we add to the elements of the first column the elements of the succeeding columns multiplied by $\lambda_2, \lambda_3, \cdots, \lambda_n$, respectively. Having obtained 1 in the first place, we use it to eliminate all succeeding elements of the first row (by subtracting from the ith column the elements of the first column multiplied by a_i, for $i = 2, 3, \cdots, n$), so that the first row is now $1, 0, 0, \cdots, 0$. Suppose the second row has become $c_1, c_2, \cdots, c_n$.

We propose to show that the transformation thus effected on the second row (and hence on all succeeding rows) is unique in the following sense: for any fixed set of a's in the first row and any set of c's, there is a unique set of b's which is transformed into the set of c's. The b's and c's are connected by the equations

$$c_1 = \sum_{j=1}^{n} \lambda_j b_j, \qquad c_i = b_i - a_i c_1 \qquad (i = 2, 3, \cdots, n).$$

The determinant of the transformation has the value λ_1 (prime to m), and the result follows.

Now the value modulo m of the transformed determinant is deduced from the minor of the leading element, and since some divisor (say d) of m was removed from the elements of the first row, we are interested in the probability $P_{n-1}(0, m/d)$ that m/d divide this principal minor. There are $N_n(d, m)$ arrangements of the first row having d for the g.c.d. of the elements and m, and for each of these arrangements there are m^{n^2-n} possible arrangements for all the other rows (m possibilities for each element). Among these the number of favorable cases, that is, determinants divisible by m, is

$$m^{n^2-n} N_n(d, m) P_{n-1}(0, m/d).$$

By considering all possible divisors d of m we get the total number of favorable cases. But this total number can also be obtained by multiplying the number m^{n^2} of possible determinants by $P_n(0, m)$. Hence we have

$$m^{n^2}P_n(0, m) = \sum_{d|m} m^{n^2-n}N_n(d, m)P_{n-1}(0, m/d).$$

Using the first equation in Lemma 1 and the fact that m/d ranges over the divisors of m as d does, and dividing by m^{n^2-n}, we obtain

$$m^nP_n(0, m) = \sum_{d|m} N_n(1, d)P_{n-1}(0, d) \qquad (n > 1, m \geqq 1). \tag{7}$$

If m is a power of a prime, say p^k, we have

$$p^{kn}P_n(0, p^k) = \sum_{\alpha=0}^{k} N_n(1, p^\alpha)P_{n-1}(0, p^\alpha). \tag{8}$$

3. **The formula for** $P_n(0, p^k)$. Subtracting equation (8) from the corresponding equation with k replaced by $k+1$, and using the last formula in Lemma 1, we obtain the recursion formula

$$p^{(k+1)n}P_n(0, p^{k+1}) = p^{kn}P_n(0, p^k) + (p^{(k+1)n} - p^{kn})P_{n-1}(0, p^{k+1}).$$

It is convenient here to set $Q_n^k = 1 - P_n(0, p^k)$ and $q = p^{-1}$. Making these substitutions we have

$$Q_n^{k+1} = q^nQ_n^k + (1 - q^n)Q_{n-1}^{k+1}. \tag{9}$$

We shall now prove

$$Q_n^k = \prod_{r=k}^{k+n-1} (1 - q^r) \qquad (k = 0, 1, 2, \cdots; n = 1, 2, 3, \cdots). \tag{10}$$

This result is trivial for $k = 0$ and all n, and for $n = 1$ and all k. Assume it true for $k \leqq K$ and all n, and for $k = K+1$ and $n < N$. To complete the induction we must prove it for $k = K+1$ and $n = N$. By (9) and the induction hypotheses we have

$$\begin{aligned} Q_N^{K+1} &= q^N \prod_{r=K}^{K+N-1} (1 - q^r) + (1 - q^N) \prod_{r=K+1}^{K+N-1} (1 - q^r) \\ &= \prod_{r=K+1}^{K+N} (1 - q^r). \end{aligned}$$

This proves (10) and equation (5) follows.

4. **Proofs of** (3) **and** (4). In the light of (2), we need demonstrate (3) for $m = p^k$ only. We wish to prove, then, that the number of determinants congruent to p^α (mod p^k) equals the number congruent to cp^α, where $(c, p) = 1$ and $\alpha < k$. Now any one of the former type gives one of the latter if the first row (say) is multiplied by c, and con-

versely if the first row is multiplied by the inverse of c (mod p^k). This inverse exists, and the correspondence is one-to-one, because c is prime to p. This proves (3).

The sum of the probabilities $P_n(ap^\alpha, p^k)$, where a runs through the values $1, 2, \cdots, p^{k-\alpha}$, is clearly the probability that a determinant be divisible by p^α. The terms of this sum can be simplified and collected by use of (3), and we have

$$P_n(0, p^\alpha) = \sum_{r=0}^{k-\alpha} \phi(p^{k-\alpha-r}) P_n(p^{\alpha+r}, p^k). \tag{11}$$

Replacing α by $\alpha+1$, and subtracting the resulting equation from (11), we arrive at (4).

PURDUE UNIVERSITY

ON THE NOTION OF THE RING OF QUOTIENTS OF A PRIME IDEAL

CLAUDE CHEVALLEY

Let $\mathfrak{o}$ be a domain of integrity (that is, a ring with unit element and with no zero divisor not equal to 0), and let $\mathfrak{u}$ be a prime ideal in $\mathfrak{o}$. We can construct two auxiliary rings associated with $\mathfrak{u}$: the factor ring $\mathfrak{o}/\mathfrak{u}$, composed of the residue classes of elements of $\mathfrak{o}$ modulo $\mathfrak{u}$, and the ring of quotients $\mathfrak{o}_\mathfrak{u}$, composed of the fractions whose numerator and denominator belong to $\mathfrak{o}$, but whose denominators do not belong to $\mathfrak{u}$. These constructions are of paramount importance in algebraic geometry; if $\mathfrak{o}$ is the ring of a variety $\boldsymbol{V}$, there corresponds to $\mathfrak{u}$ a subvariety $\boldsymbol{U}$ of $\boldsymbol{V}$; $\mathfrak{o}/\mathfrak{u}$ is the ring of $\boldsymbol{U}$, whereas the ring $\mathfrak{o}_\mathfrak{u}$ is the proper algebraic tool to investigate the neighborhood of $\boldsymbol{U}$ with respect to $\boldsymbol{V}$.

Now, the local theory of algebraic varieties involves the consideration of rings which are not domains of integrity (this, because the completion of a local ring may introduce zero divisors). Let then $\mathfrak{o}$ be any commutative ring with unit element, and let again $\mathfrak{u}$ be a prime ideal in $\mathfrak{o}$. We may define the factor ring $\mathfrak{o}/\mathfrak{u}$ exactly in the same way as above, but we cannot so easily generalize the notion of the ring of quotients $\mathfrak{o}_\mathfrak{u}$. If there exist zero divisors outside $\mathfrak{u}$, these zero divisors cannot be used as denominators of fractions, which shows that the definition of $\mathfrak{o}_\mathfrak{u}$ cannot be extended verbatim. If we

Received by the editors September 4, 1943.