ON THE ASYMPTOTIC DISTRIBUTION OF THE ELEMENTARY SYMMETRIC FUNCTIONS (MOD p)

BY

N. J. FINE

1. **Introduction.** Much work has been done on the problem of evaluating or estimating the number of solutions of certain congruences in many variables. For example, it is of interest in Waring's Problem to find the number of solutions of

$$x_1^k + x_2^k + \cdots + x_n^k \equiv a \pmod{p}. \tag{1}$$

Equation (1) has been discussed by Hardy and Littlewood [1](1), and by Hull [2]. More recently, Weil [3] has treated the equation

$$x_1^{k_1} + x_2^{k_2} + \cdots + x_n^{k_n} = a \tag{2}$$

in finite fields. Niven and the author [4] solved the problem for the equation $\Delta_n \equiv a \pmod{m}$, where Δ_n is a determinant of order n in the independent variables x_{ij} $(i, j = 1, \cdots, n)$.

In the cases mentioned above, the number of variables is fixed, but it makes sense to ask what happens for large n. For this purpose it is convenient to speak of the *probability* that $f_n(x_1, \cdots, x_n) \equiv a \pmod{p}$, for example. This is defined as the ratio of the number of successes to the total number of possibilities, p^n. If this ratio tends to a limit as n increases, for fixed p and a, we may speak of the asymptotic distribution of the function under consideration. Thus, for equation (2), which includes (1) as a special case, it is seen that all the values a have the same weight asymptotically. For the determinant Δ_n this is not true; the exact values can be determined from the explicit formulas given in [4]. For example, with a prime modulus p, the asymptotic probability that $\Delta_n \equiv 0 \pmod{p}$ is given by

$$P(0) = 1 - \prod_{r=1}^{\infty} (1 - p^{-r}),$$

while $P(a) = (1 - P(0))/(p-1) < P(0)$ for $a \not\equiv 0 \pmod{p}$.

This paper deals with the asymptotic distribution of the elementary symmetric functions mod p. To state the problem precisely, let

$$U_k^{(n)}(x_1, \cdots, x_n) = \sum_{i_1 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}$$

Presented to the Society, November 25, 1944; received by the editors September 12, 1949.

(1) Numbers in brackets refer to the bibliography at the end of the paper.

be the elementary symmetric function of order k in the n independent variables $x_1, \cdots, x_n$, each ranging over a complete residue system modulo p, a prime. Of the p^n values of $U_k^{(n)}$ thus obtained, let g be the number which are congruent to a (mod p). We propose to study the ratio $P_n(p, k, a) = g/p^n$, or rather the limit of this ratio as n increases. This limit is shown to exist in §3, Theorem 1, and will be denoted by $P(p, k, a)$, or more briefly by $P_k(a)$. In addition, the proof of Theorem 1 yields an algorithm for determining the value of $P(p, k, a)$ in any specific case. As models for further study, the cases $p=2$ and $p=3$ are treated in §§4 and 5. In §6 we prove a theorem concerning the distribution of the nonzero residues which has as a corollary the result that for k relatively prime to $p-1$, these residues are equidistributed. In the next section we introduce the useful notion of a *correlated pair*, leading to Theorem 6, which exhibits a class of integers k for which complete equidistribution holds. We conjecture that for all k not belonging to this class, the residue 0 has the greatest weight. This would imply the weaker statement, which we are also unable to prove, that $P_k(0) \geqq 1/p$ for all $k>0$. However, we can exhibit (Theorem 12) a large class of integers k for which $P_k(0) > 1/p$. This, too, leaves open the question, is lim sup $P_k(0) = 1$ as $k \to \infty$? The remainder of the paper is concerned with establishing certain relationships among the probabilities $P(p, k, 0)$.

§2 contains five lemmas, one of which (Lemma 4) is actually not needed in the body of the paper, but is included for its intrinsic interest. In addition, it serves to explain why certain methods used in the paper cannot be extended.

2. **Lemmas.**

In this section we shall give several important lemmas which may be of some interest in themselves. The first was proved by Lucas [5] and more recently by us [6]:

LEMMA 1. *Let p be a prime, and let*

$$M = M_0 + M_1 p + \cdots + M_t p^t \qquad (0 \leqq M_i < p),$$
$$N = N_0 + N_1 p + \cdots + N_t p^t \qquad (0 \leqq N_i < p).$$

Then

$$\binom{M}{N} \equiv \binom{M_0}{N_0}\binom{M_1}{N_1} \cdots \binom{M_t}{N_t} \pmod{p}.$$

LEMMA 2. *Let $\alpha = (\alpha_1, \cdots, \alpha_q)$ be a fixed q-dimensional vector with integral coordinates and let $\mathfrak{M}_\alpha$ be the set of vectors $\sigma = (\sigma_1, \cdots, \sigma_q)$ satisfying*

(i) $\sigma_r \geqq 0 \qquad (r = 1, \cdots, q),$

(ii) $\sigma_r \equiv \alpha_r \pmod{m} \qquad (r = 1, \cdots, q),$

(iii) $\sigma_1 + \cdots + \sigma_q \leqq n,$

where m and n are positive integers. Then, setting $\omega = \exp(2\pi i/m)$, we have

$$
\begin{aligned}
(3)\qquad & m^q \sum_{\sigma\in\mathfrak{M}_\alpha} \frac{n!}{\sigma_1!\cdots\sigma_q!(n-\sigma_1-\cdots-\sigma_q)!} \\
&\qquad = \sum_{t_1=0}^{m-1}\cdots\sum_{t_q=0}^{m-1}(1+\omega^{t_1}+\cdots+\omega^{t_q})^n\omega^{-(t_1\alpha_1+\cdots+t_q\alpha_q)}.
\end{aligned}
$$

This is easily proved by expanding $(1+\omega^{t_1}+\cdots+\omega^{t_q})^n$ by the multinomial theorem to give

$$
\sum \frac{n!}{\sigma_1!\cdots\sigma_q!(n-\sigma_1-\cdots-\sigma_q)!}\,\omega^{t_1\sigma_1+\cdots+t_q\sigma_q},
$$

the sum running over all σ satisfying conditions (i) and (iii) above. Now any vector σ which violates (ii) will contribute nothing to the sum on the right side of (3); for then $\sigma_r\not\equiv\alpha_r \pmod m$ for some r, and if we sum over that t_r first we get

$$
\sum_{t_r=0}^{m-1}\omega^{(\sigma_r-\alpha_r)t_r}=0.
$$

Hence the only contribution is made by those $\sigma\in\mathfrak{M}_\alpha$, each σ yielding the corresponding multinomial coefficient taken m times for each summation, m^q times in all.

LEMMA 3. *Let m be a positive integer. Then we can find integers (not necessarily positive) $\alpha_1,\cdots,\alpha_m$ such that the formal expansion*

$$
(4)\qquad \prod_{r=1}^{m}(1+rx)^{\alpha_r}=1+C_1x+C_2x^2+\cdots+C_mx^m+\cdots
$$

satisfies

$$
(5)\qquad C_1=C_2=\cdots=C_{m-1}=0,\qquad C_m\neq 0.
$$

By logarithmic differentiation of (4) we find that the condition (5) implies

$$
\begin{aligned}
mC_mx^{m-1}+\cdots &= \sum_{r=1}^{m} r\alpha_r(1+rx)^{-1} \\
&= \sum_{r=1}^{m} r\alpha_r\sum_{t=0}^{\infty}(-rx)^t \\
&= \sum_{t=0}^{\infty}(-1)^tx^t\sum_{r=1}^{m}\alpha_rr^{t+1}.
\end{aligned}
$$

Comparing coefficients, we must have

$$
(6)\qquad \sum_{r=1}^{m}\alpha_rr^t=0\qquad (t=1,2,\cdots,m-1),
$$

$$(7) \qquad \sum_{r=1}^{m} \alpha_r r^m = (-1)^{m-1} m C_m.$$

It is easy to see that the existence of a set of integers $C_m \neq 0$; $\alpha_1, \cdots, \alpha_m$ satisfying (6) and (7) implies (4) and (5). Now to solve (6) and (7) we observe that the determinant of the system is the familiar Vandermonde, and its value is

$$\Delta = m! \prod_{i>j} (i-j) \qquad (i, j = 1, 2, \cdots, m).$$

Hence $\alpha_r \Delta$ is equal to the determinant Δ_r formed by striking out the rth column and last row from Δ, multiplied by $(-1)^{m-1} m C_m (-1)^{m+r} = (-1)^{r-1} m C_m$. But Δ_r is again a Vandermonde,

$$\Delta_r = \frac{m!}{r} \prod_{i>j} (i-j) \qquad (i, j = 1, 2, \cdots, r-1, r+1, \cdots, m).$$

Therefore

$$\frac{\Delta_r}{\Delta} = \left\{ r(r-1) \cdots (r-(r-1))((r+1)-r) \cdots (m-r) \right\}^{-1} = \frac{1}{r!(m-r)!}.$$

Finally,

$$(8) \qquad \alpha_r = \frac{(-1)^{r-1} m C_m}{r!(m-r)!} = (-1)^{r-1} \binom{m}{r} \frac{C_m}{(m-1)!}.$$

Consequently, if we choose $C_m = (m-1)!$ we are sure that all the α_r will be integers. We have proved, then, that

$$(9) \qquad \prod_{r=1}^{m} (1+rx)^{(-1)^{r-1}\binom{m}{r}} = 1 + (m-1)! x^m + \cdots.$$

We observe from (8) that C_m must be divisible by $(m-1)!$ if α_m is to be an integer and if (4) and (5) are to be satisfied. But even more is true, as we shall now prove.

LEMMA 4. *Let $\alpha_1, \cdots, \alpha_N$ be a set of integers (not necessarily positive) for which the product*

$$(10) \qquad \prod_{r=1}^{N} (1+rx)^{\alpha_r} = 1 + C_1 x + \cdots + C_m x^m + \cdots$$

satisfies

$$(11) \qquad C_1 \equiv C_2 \equiv \cdots \equiv C_{m-1} \equiv 0 \pmod{m!}.$$

Then $C_m \equiv 0 \pmod{(m-1)!}$.

As in the proof of Lemma 3, (10) and (11) imply the system

$$\begin{aligned}&\sum_{r=1}^{N} r^t\alpha_r \equiv 0 \pmod{m!} \qquad (t = 1, \cdots, m-1),\\ (12)\qquad &\sum_{r=1}^{N} r^m\alpha_r \equiv (-1)^{m-1}mC_m \pmod{m!}.\end{aligned}$$

Consider the functions

$$H(x) = \sum_{r=1}^{N} \alpha_r(x^r - 1),$$

$$H_t(x) = \sum_{r=1}^{N} r^t\alpha_r x^r \qquad (t = 1, 2, \cdots, m).$$

From (12),

$$\left.\begin{aligned}H(1) \equiv H_1(1) \equiv \cdots \equiv H_{m-1}(1) \equiv 0,\\ H_m(1) \equiv (-1)^{m-1}mC_m\end{aligned}\right\} \pmod{m!}.$$

But $H_1(x) = xH'(x)$, $H_2(x) = xH'(x) + x^2H''(x)$, and in general

$$H_n(x) = \sum_{s=1}^{n} A(n, s)x^sH^{(s)}(x),$$

where the $A(n, s)$ are certain integers (Stirling numbers) given by the recursion

$$A(n+1, s) = sA(n, s) + A(n, s-1).$$

For our present purpose it is sufficient to observe that $A(n, n) = 1$. This implies that $H(1) \equiv H'(1) \equiv \cdots \equiv H^{(m-1)}(1) \equiv 0 \pmod{m!}$ and that $H^{(m)}(1) \equiv H_m(1) \pmod{m!}$. But for any polynomial $H(x)$ with integral coefficients, $H^{(m)}(x) \equiv 0 \pmod{m!}$ identically. Hence

$$(-1)^{m-1}mC_m \equiv H_m(1) \equiv H^{(m)}(1) \equiv 0 \pmod{m!},$$

$$C_m \equiv 0 \pmod{(m-1)!}.$$

It is easy to see that the conclusion is still valid if we replace the product (10) by $\prod_{r=1}^{n}(1+B_rx)^{\alpha_r}$, where the B_r are arbitrary integers.

LEMMA 5. *For any prime p and any set of residues $C_1, \cdots, C_p$ (mod p) we can find integers $\alpha_1, \cdots, \alpha_{p-1}$ such that*

$$\prod_{r=1}^{p-1}(1 + rx)^{\alpha_r} \equiv 1 + C_1x + C_2x^2 + \cdots + C_px^p + \cdots \pmod{p}.$$

We can surely find a product

$$P(x) = \prod_{r=1}^{p-1} (1 + rx)^{\beta_r} \equiv 1 + C_1x + \cdots + C_{m-1}x^{m-1} + A_mx^m + \cdots \pmod{p},$$

for $m=2$. Suppose that one has been found for $m<p$. By Lemma 3, equation (9), there is a product

$$G_m(x) = 1 + (m-1)!x^m + \cdots .$$

Determine s so that $(m-1)!s+A_m \equiv C_m \pmod{p}$. Then $P(x)G_m(x)$ is the desired product for $m+1$. Thus we can find

$$Q(x) = \prod_{r=1}^{p-1} (1 + rx)^{\gamma_r} \equiv 1 + C_1x + \cdots + C_{p-1}x^{p-1} + A_px^p + \cdots \pmod{p}.$$

Now determine t so that $t+A_p \equiv C_p \pmod{p}$. Then

$$(1 + x)^{tp} \equiv (1 + x^p)^t \equiv 1 + tx^p + \cdots \pmod{p},$$

and $(1+x)^{tp}Q(x)$ is the desired product.

3. **The limit theorem.** In this section we prove that the elementary symmetric functions (mod p) have an asymptotic distribution.

THEOREM 1. *For all primes p, non-negative integers k, and residues a (mod p),*

$$P(p, k, a) = \lim_{n\to\infty} P_n(p, k, a)$$

exists.

Proof. Every ordered set of n residues $x_1, x_2, \cdots, x_n$ (mod p) determines a vector $\sigma=(\sigma_1, \sigma_2, \cdots, \sigma_{p-1})$, in which σ_r is the number of x_i congruent to r (mod p), $r=1, 2, \cdots, p-1$. Clearly, $\sigma_r \geqq 0$ and $0 \leqq \sigma_1+\sigma_2+ \cdots +\sigma_{p-1} \leqq n$. Every such vector σ is derived from a number of sets $(x_1, \cdots, x_n)$, this number being

$$A_n(\sigma) = \frac{n!}{\sigma_1! \cdots \sigma_{p-1}!(n - \sigma_1 - \cdots - \sigma_{p-1})!} .$$

The elementary symmetric function $U_k^{(n)}(x_1, \cdots, x_n)$ is congruent (mod p) to the coefficient of x^k in the expansion of

$$\Phi(\sigma, x) = \prod_{r=1}^{p-1} (1 + rx)^{\sigma_r} = F_0(\sigma) + F_1(\sigma)x + \cdots + F_k(\sigma)x^k + \cdots .$$

Thus $F_0(\sigma)=1$, and $F_m(\sigma)=0$ for $m<0$. For all $k>0$,

$$U_k^{(n)} (x_1, \cdots, x_n) \equiv F_k(\sigma) \pmod{p}.$$

Now suppose that s is any integer such that $p^s>k$, and that $\sigma_r' =\sigma_r+\tau_rp^s$

$(r=1, 2, \cdots, p-1)$. We assert that $F_k(\sigma')\equiv F_k(\sigma)$ (mod p). For

$$\begin{aligned} &1+F_1(\sigma')x+\cdots+F_k(\sigma')x^k+\cdots \\ &\quad = \Phi(\sigma', x) = \Phi(\sigma, x)\Phi(p^s\tau, x) \equiv \Phi(\sigma, x)\Phi(\tau, x^{p^s}) \\ &\quad \equiv \{1+F_1(\sigma)x+\cdots+F_k(\sigma)x^k+\cdots\}\{1+F_1(\tau)x^{p^s}+\cdots\} \pmod{p}. \end{aligned}$$

Our assertion follows by equating coefficients of x^k and using the fact that $k<p^s$. Thus $F_k(\sigma)$, mod p, is a periodic function of each component σ_r, the period being p^s. Accordingly, we shall define the vector space V_s consisting of vectors α satisfying

$$0 \leqq \alpha_r < p^s \qquad (r = 1, 2, \cdots, p-1),$$

the number of elements in V_s being $N(s)=p^{s(p-1)}$. Each σ has a unique $\alpha\in V_s$ such that $\sigma\equiv\alpha$ (mod p^s), and $F_k(\sigma)\equiv F_k(\alpha)$ (mod p). Now let $\mathfrak{N}_s(p, k, a)$ be the set of $\alpha\in V_s$ for which $F_k(\alpha)\equiv a$ (mod p), and let $N_s(p, k, a)$ be the number of elements in this set. Then

$$P_n(p, k, a) = p^{-n}\sum_{\alpha\in\mathfrak{N}}\ \sum_{\sigma\equiv\alpha(\mathrm{mod}\ p^s)} A_n(\sigma). \tag{13}$$

Applying Lemma 2 to the inner sum in (13), with $q=p-1$ and $m=p^s$, we obtain

$$\begin{aligned} &P_n(p, k, a) \\ &\quad = \frac{1}{N(s)}\sum_{\alpha\in\mathfrak{N}}\ \sum_{t_1=0}^{p^s-1}\cdots\sum_{t_{p-1}=0}^{p^s-1}\left(\frac{1+\omega^{t_1}+\cdots+\omega^{t_{p-1}}}{p}\right)^n \omega^{-(t_1\alpha_1+\cdots+t_{p-1}\alpha_{p-1})}. \end{aligned}$$

Now observe that

$$\left|\frac{1+\omega^{t_1}+\cdots+\omega^{t_{p-1}}}{p}\right| \leqq b < 1,$$

unless $t_1=\cdots=t_{p-1}=0$. Hence, removing this one set,

$$P_n(p, k, a) = \frac{N_s(p, k, a)}{N(s)} + R_n,$$

where

$$|R_n| \leqq \frac{1}{N(s)}\sum_{\alpha\in\mathfrak{N}} p^{s(p-1)}b^n = N_s(p, k, a)b^n,$$

which tends to zero as $n\to\infty$. Hence

$$\lim_{n\to\infty} P_n(p, k, a) = \frac{N_s(p, k, a)}{N(s)} = P(p, k, a),$$

and the theorem is proved.

It should be remarked that the proof of Theorem 1 yields a finite algorithm for determining $P(p, k, a)$. We need only count the number of $\alpha \in V_s$ $(p^s > k)$ for which $F_k(\alpha) \equiv a \pmod{p}$, and divide this number by $N(s)$, the number of elements in V_s. We have therefore indentified the asymptotic distribution with a finite distribution in a certain $(p-1)$-dimensional cube. Furthermore, by choosing s sufficiently large, we may discuss the joint distribution of any finite number of random variables $F_{k_1}(\alpha), \cdots, F_{k_N}(\alpha)$. This will prove to be useful later on.

4. **The case $p=2$.** In this section we shall apply the results of §3 to obtain a complete solution of our problem for the case $p=2$. We shall put our observations on this result in the form of corollaries, which we shall compare with a similar set for $p=3$, in the next section, in the hope that the evidence of these two cases may lead to fruitful conjectures and lines of attack in the general case.

THEOREM 2. *Let h be the number of nonzero digits in the dyadic expansion of k. Then*

$$P(2, k, 1) = 2^{-h}, \qquad P(2, k, 0) = 1 - 2^{-h}.$$

Proof. Let $k > 0$ be written in the scale of 2:

$$k = k^{(0)} + 2k^{(1)} + \cdots + 2^{s-1}k^{(s-1)} \qquad (k^{(i)} = 0, 1).$$

The set $\mathfrak{N}_s(2, k, 1)$ consists of those vectors (in this case, ordinary integers) α satisfying $0 \leqq \alpha < 2^s$ and

$$F_k(\alpha) = \binom{\alpha}{k} \equiv 1 \pmod{2}.$$

Now if we write α as

$$\alpha = \alpha^{(0)} + 2\alpha^{(1)} + \cdots + 2^{s-1}\alpha^{(s-1)} \qquad (\alpha^{(i)} = 0, 1),$$

an application of Lemma 1 yields

$$F_k(\alpha) \equiv \binom{\alpha^{(0)}}{k^{(0)}} \cdots \binom{\alpha^{(s-1)}}{k^{(s-1)}} \pmod{2}.$$

For each of the h $k^{(i)}$ which is different from zero, it is necessary that the corresponding $\alpha^{(i)}$ be 1 also, in order that

$$\binom{\alpha^{(i)}}{k^{(i)}}, \text{ hence } \binom{\alpha}{k}, \text{ be odd.}$$

But this condition is also sufficient, so the remaining $\alpha^{(i)}$ may be chosen at will. Hence

$$N_s(2, k, 1) = 2^{s-h},$$

$$P(2,\, k,\, 1) = \frac{1}{N(s)} N_s(2,\, k,\, 1) = 2^{-s}\cdot 2^{s-h} = 2^{-h},$$

$$P(2,\, k,\, 0) = 1 - 2^{-h}.$$

Corollary 1. $P(2,\, 2k,\, a) = P(2,\, k,\, a)$.

Corollary 2. $P(2,\, k,\, 0) \geqq 1/2$ *for* $k>0$, *and the equality holds if and only if* $k=2^s$.

Corollary 3. Lim sup $P(2,\, k,\, 0)=1$. (*This follows directly from the fact that* $P(2,\, 2^s-1,\, 0)=1-2^{-s}$.)

Corollary 4. *The generating function for* $Q_k=1-P(2,\, k,\, 0)$ *is*

$$\sum_{k=0}^{\infty} Q_k z^k = \prod_{n=0}^{\infty}\left(1+\frac{1}{2} z^{2^n}\right).$$

5. **The case** $p=3$. Here the solution is not explicit, but is given in the form of a set of recurrence formulas. Throughout this section we shall write $P(3,\, k,\, a)=P_k(a)$.

Theorem 3.

(i) $$P_{3k}(a) = P_k(a) \qquad (a = 0,\, 1,\, 2).$$

(ii) $$P_{3k+1}(0) = (2 + 6P_k(0) + P_{k-1}(0))/9,$$
$$P_{3k+1}(a) = (3 - 3P_k(0) + P_{k-1}(a))/9 \qquad (a = 1,\, 2).$$

(iii) $$P_{3k+2}(0) = (1 + 2P_k(0))/3,$$
$$P_{3k+2}(a) = (1 - P_k(0))/3 \qquad (a = 1,\, 2).$$

Proof. Let $k'=3k+m$ $(m=0,\, 1,\, 2)$, and $k<3^s$. If $\alpha\in V_{s+1}$, we may write $\alpha=3\beta+\gamma$ with $\beta\in V_s$ and $\gamma\in V_1$. Then

$$\begin{aligned}(1 + x)^{\alpha_1}&(1 + 2x)^{\alpha_2}\\ &\equiv \left\{(1 + x^3)^{\beta_1}(1 + 2x^3)^{\beta_2}\right\}\left\{(1 + x)^{\gamma_1}(1 + 2x)^{\gamma_2}\right\}\\ &\equiv \left\{1+F_1(\beta)x^3+F_2(\beta)x^6+\cdots\right\}\left\{1+F_1(\gamma)x+\cdots+F_4(\gamma)x^4\right\} \pmod 3.\end{aligned}$$

Comparing coefficients of $x^{k'}$, we get

(14) $$F_{k'}(\alpha) \equiv F_m(\gamma)F_k(\beta) + F_{m+3}(\gamma)F_{k-1}(\beta) \pmod 3.$$

Consider first the case $m=0$. Then

(15) $$F_{3k}(\alpha) \equiv F_k(\beta) + F_3(\gamma)F_{k-1}(\beta) \pmod 3.$$

We shall exhibit the right side of (15) as $F_k(\beta+\delta)$, where δ is a vector depending only on γ. In fact, the coefficient of y^k in the expansion of

$$(1 + F_3(\gamma)y)\left\{(1 + y)^{\beta_1}(1 + 2y)^{\beta_2}\right\}$$

is exactly the right side of (15). Explicitly, then,

$$\delta = (0, 0) \quad \textit{if} \quad F_3(\gamma) \equiv 0 \pmod 3,$$
$$\delta = (1, 0) \quad \textit{if} \quad F_3(\gamma) \equiv 1 \pmod 3,$$
$$\delta = (0, 1) \quad \textit{if} \quad F_3(\gamma) \equiv 2 \pmod 3.$$

Hence

$$F_{3k}(\alpha) \equiv F_{3k}(3\beta + \gamma) \equiv F_k(\beta + \delta) \pmod 3.$$

For each fixed $\gamma \in V_1$, the vector $\beta + \delta$ (mod 3^s) runs over V_s as β does, the correspondence being one-to-one. Thus each of the nine vectors $\gamma \in V_1$ yields a contribution $N_s(3, k, a)$ to the total $N_{s+1}(3, 3k, a)$. Altogether, then, we have $N_{s+1}(3, 3k, a) = 9N_s(3, k, a)$. Dividing by $N(s+1)$, we obtain (i).

Now if $m = 1$, we have, from (14),

$$F_{3k+1}(\alpha) \equiv F_1(\gamma)F_k(\beta) + F_4(\gamma)F_{k-1}(\beta) \pmod 3. \tag{16}$$

Here we have six vectors $\gamma \in V_1$ for which $F_1(\gamma) \not\equiv 0$ (mod 3), three of which yield $F_1(\gamma) \equiv 1$ (mod 3), and three $F_1(\gamma) \equiv 2$ (mod 3). For the first set, we get, precisely as above,

$$F_{3k+1}(\alpha) \equiv F_k(\beta + \delta') \pmod 3,$$

and for the second set,

$$F_{3k+1}(\alpha) \equiv 2F_k(\beta + \delta'') \pmod 3,$$

where δ', δ'' are vectors depending only on γ. Hence, as above, we get contributions of $3N_s(3, k, a)$ and $3N_s(3, k, 2a)$ to $N_{s+1}(3, 3k+1, a)$ from the first and second sets respectively. Of the remaining $\gamma \in V_1$, for which $F_1(\gamma) \equiv 0$ (mod 3), two also give $F_4(\gamma) \equiv 0$, thus contributing $2 \cdot 3^{2s}$ to $N_{s+1}(3, 3k+1, 0)$ and nothing to $N_{s+1}(3, 3k+1, a)$ for $a = 1, 2$. The last vector (2, 2) yields $F_4(2, 2) \equiv 1$ (mod 3), so that

$$F_{3k+1}(\alpha) \equiv F_{k-1}(\beta) \pmod 3.$$

This contributes $N_s(3, k-1, a)$ to $N_{s+1}(3, 3k+1, a)$ for $a = 0, 1, 2$. Collecting all these contributions,

$$N_{s+1}(3, 3k + 1, 0) = 6N_s(3, k, 0) + 2 \cdot 3^{2s} + N_s(3, k - 1, 0),$$
$$N_{s+1}(3, 3k + 1, 1) = 3N_s(3, k, 1) + 3N_s(3, k, 2) + N_s(3, k - 1, 1),$$
$$N_{s+1}(3, 3k + 1, 2) = 3N_s(3, k, 2) + 3N_s(3, k, 1) + N_s(3, k - 1, 2).$$

Dividing by $N(s+1) = 9N(s)$, and using the fact that $P_k(1) + P_k(2) = 1 - P_k(0)$, we obtain (ii).

If $m = 2$, (14) yields

$$F_{3k+2}(\alpha) \equiv F_2(\gamma)F_k(\beta) \pmod 3. \tag{17}$$

A straightforward examination of cases then results in (iii).

COROLLARY 1. *$P_{3k}(a)=P_k(a)$.*

COROLLARY 2. *$P_k(0)\geqq 1/3$ for all $k>0$, and equality holds if and only if $k=3^s$ or $k=2\cdot 3^s$.*

COROLLARY 3. Lim sup $P_k(0)=1$. (*For this we need only observe that $P_{3^s-1}(0)=1-(2/3)^s$.*)

COROLLARY 4. *The generating function for $Q_k=1-P_k(0)$ is*

$$\sum_{k=0}^{\infty} Q_k z^k = \prod_{n=0}^{\infty}\left(1+\frac{2}{3}z^{3^n}+\frac{2}{3}z^{2\cdot 3^n}+\frac{1}{9}z^{4\cdot 3^n}\right).$$

COROLLARY 5. *$P_k(0)\geqq P_k(1)\geqq P_k(2)$ for all $k>0$. Equidistribution holds if and only if $k=3^s$ or $k=2\cdot 3^s$, and the second equality fails if and only if k is of the form $4m$, where the expansion of m in the scale of 3 contains no digit 2.*

6. **Distribution of nonzero residues.** It should be clear by now that the residue 0 plays a special role. In this section we shall prove a theorem concerning the distribution of the nonzero residues[2].

THEOREM 4. *The number of distinct values assumed by $P(p, k, a)$ for $1\leqq a\leqq p-1$ is at most $(k, p-1)$.*

Proof. If a and b are two nonzero residues (mod p) such that ab^{-1} is a kth power residue (mod p), then evidently $P(p, k, a)=P(p, k, b)$. The result follows by a known theorem on kth power residues.

COROLLARY. *If $(k, p-1)=1$, then*

$$P(p, k, 1) = \cdots = P(p, k, p-1).$$

7. **Correlated pairs.** We introduce the notion of a *correlated pair*, or simply a *pair*, by the following illustration. Let k be a positive integer less than p^s, and let $\alpha\in V_s$. Then

$$\begin{aligned}\Phi(\alpha, x) &= \prod_{r=1}^{p-1}(1+rx)^{\alpha_r} \\ &\equiv 1+F_1(\alpha)x+\cdots+F_{k-1}(\alpha)x^{k-1}+F_k(\alpha)x^k+\cdots \pmod{p}.\end{aligned} \tag{18}$$

Now choose an integer n, $0\leqq n<p$, and denote by ξ_n the vector $(0, \cdots, 0, 1, 0, \cdots, 0)$, with the 1 in the nth place, for $0<n<p$, and set $\xi_0=0$. Multiply (18) by $1+nx$ and equate coefficients of x^k. We get

$$F_k(\alpha+\xi_n)\equiv F_k(\alpha)+nF_{k-1}(\alpha) \pmod{p}. \tag{19}$$

For each fixed n, as α runs over V_s, so does $\alpha+\xi_n$ (mod p^s). Thus we obtain

[2] We wish to thank the referee for suggesting the existence of a theorem of this type.

p copies of V_s, each α generating the set $\{\alpha+\xi_n\}$. Consider the set of $\boldsymbol{\alpha}$, say $\mathfrak{N}_s(p,\ k-1,\ \neq 0)$, for which $F_{k-1}(\alpha)\neq 0 \pmod p$, the number in the set being $N_s(p,\ k-1,\ \neq 0)=N(s)-N_s(p,\ k-1,\ 0)$. For each $\alpha\in\mathfrak{N}_s(p,\ k-1,\ \neq 0)$, the set $F_k(\alpha+\xi_n)$ is a complete residue system mod p, and for each $\alpha\in\mathfrak{N}_s(p,\ k-1,\ 0)$, the set $F_k(\alpha+\xi_n)$ consists of the residue $F_k(\alpha)$ taken p times. Hence, if we denote by $\mathfrak{M}_s(k-1,\ a;\ k,\ b)$ the set of $\alpha\in V_s$ such that

$$F_{k-1}(\alpha)\equiv a \quad \textit{and} \quad F_k(\alpha)\equiv b \pmod p, \tag{20}$$

and by $J(k-1,\ a;\ k,\ b)$ the number of elements in this set divided by $N(s)$ (J is clearly independent of s, for $p^s>k$), it is possible to count the number of vectors $\alpha+\xi_n$ for which the right side of (19) is congruent to a particular residue c, mod p. This number is

$$N_s(p,\ k-1,\ \neq 0)+pN(s)J(k-1,\ 0;\ k,\ c). \tag{21}$$

On the other hand, this number is $pN_s(p,\ k,\ c)$. Equating these expressions and dividing by $pN(s)$, we get

$$P_k(c)=\frac{1}{p}(1-P_{k-1}(0))+J(k-1,\ 0;\ k,\ c). \tag{22}$$

The quantity $J(k-1,\ a;\ k,\ b)$ introduced above has the obvious interpretation as the joint frequency function for the elementary symmetric functions of orders $k-1$ and k.

It is clear that (22) yields a great deal of information about the distributions for k and $k-1$. For this reason we introduce the definition of a *pair* $(k,\ k')$ as an ordered couple of integers $k>k'\geqq 0$ for which

$$P_k(c)=\frac{1}{p}(1-P_{k'}(0))+J(k',\ 0;\ k,\ c) \qquad (0\leqq c<p). \tag{23}$$

The definition of J in (23) is the obvious analogue of $J(k-1,\ 0;\ k,\ c)$.

It should also be clear that the analogue of (19),

$$F_k(\alpha+\beta_n)\equiv F_k(\alpha)+nF_{k'}(\alpha) \pmod p \qquad (0\leqq n<p), \tag{24}$$

implies that $(k,\ k')$ is a pair, that is, (23) holds. In fact, the argument given above goes through almost word for word. It is not necessary that the β_n have any special form; they are simply any p vectors for which (24) is satisfied.

Before discussing the properties of correlated pairs and their consequences, we shall exhibit a large class of such pairs. Let $k=tp^s+k'$, $0<t\leqq p$. By Lemma 5, there exists a vector γ such that[3]

$$\Phi(\gamma,\ x)\equiv 1+x^t+O(x^{p+1}) \pmod p. \tag{25}$$

[3] By $O(x^m)$ we mean a power series in which the terms of degree less than m have coefficients divisible by p.

Replacing x by x^{p^s}, we have

$$(26)\qquad \Phi(\gamma, x^{p^s}) \equiv \Phi(\gamma p^s, x) \equiv 1 + x^{tp^s} + O(x^{(p+1)p^s}) \pmod{p}.$$

Raising both sides to the nth power, $0 \leqq n < p$, and defining $v = \min(2t, p+1)$, we obtain

$$(27)\qquad \Phi(n\gamma p^s, x) \equiv 1 + nx^{tp^s} + O(x^{vp^s}) \pmod{p}.$$

Let $\beta_n = np^s\gamma$; multiply (18) by (27) and equate coefficients of x^k. Then

$$(28)\qquad F_k(\alpha + \beta_n) \equiv F_k(\alpha) + nF_{k'}(\alpha) + C_nF_{k-vp^s}(\alpha) + \cdots \pmod{p}.$$

Hence if $tp^s \leqq k < vp^s$, (24) is satisfied and (k, k') is a pair. In particular, if $k = tp^s + k'$ and $0 \leqq k' < p^s$, then k, k' are correlated.

In some cases, it may be possible to improve (25). For example,

$$(29)\qquad \prod_{r=1}^{p-1} (1 + rx) \equiv 1 - x^{p-1} \pmod{p},$$

from which we deduce as above that if $k = (p-1)p^s + k'$, and $0 \leqq k' < (p-1)p^s$, then (k, k') is a pair. The other cases in which $1 - x^t$ factors as in (29) do not appear to yield anything new, since then $t \mid (p-1)$, so $2t \leqq p - 1 < p + 1$, and $v = 2t$.

We may also include the correlated pairs $(k, k - p^s)$ for all $k \geqq p^s$, $s \geqq 0$. To see this, take $\beta_0 = 0$, $\beta_n = (0, \cdots, 0, p^s, 0, \cdots, 0)$ with p^s in the nth place. Then

$$\Phi(\beta_n, x) = (1 + nx)^{p^s} \equiv 1 + nx^{p^s} \pmod{p},$$

from which we obtain, as in (19),

$$F_k(\alpha + \beta_n) \equiv F_k(\alpha) + nF_{k-p^s}(\alpha) \pmod{p}.$$

We summarize our findings on correlated pairs so far in the following theorem.

THEOREM 5. *If (k, k') is a pair, then*

$$(30)\qquad P_k(c) = \frac{1}{p}(1 - P_k(0)) + J(k', 0; k, c) \qquad (0 \leqq c < p).$$

The following are always correlated pairs:

$$(31)\qquad \begin{aligned} &\text{(i)}\quad k \geqq p^s,\ k' = k - p^s;\ s \geqq 0, \\ &\text{(ii)}\quad tp^s \leqq k < vp^s,\ k' = k - tp^s;\ 0 < t \leqq p,\ v = \min(2t, p+1), \\ &\text{(iii)}\quad (p-1)p^s \leqq k < 2(p-1)p^s,\ k' = k - (p-1)p^s. \end{aligned}$$

One immediate consequence of the preceding discussion is that $P_k(c) = 1/p$ for $0 \leqq c < p$ if k is correlated with 0. For then, in (30),

$$P_{k'}(0) = 0, \qquad J(k', 0; k, c) = 0.$$

Taking into account (31), we have the following result:

THEOREM 6. *If $k = tp^s$, $0 < t < p$, $s \geqq 0$, then for all residues c* (mod p),

$$P_k(c) = 1/p.$$

In particular, this is true for all $k \leqq p$.

We have obtained a class of indices $k = tp^s$ for which equidistribution holds, and we strongly suspect that this is true *only if* k belongs to this class.

It is interesting to observe that not only are the random variables $F_1(\alpha), \cdots, F_p(\alpha)$ individually uniformly distributed, but that they are all mutually independent. For let $\alpha \in V_2$, so that $\alpha = \alpha' + p\alpha''$, with α', α'' both in V_1. For a given set of residues $(a_1, a_2, \cdots, a_p)$, we are assured by Lemma 5 that there is at least one $\alpha' \in V_1$ for which

$$(32) \qquad F_1(\alpha') \equiv a_1, \cdots, F_{p-1}(\alpha') \equiv a_{p-1} \pmod{p}.$$

The number of sets $(a_1, \cdots, a_{p-1})$ is $p^{p-1} = N(1)$, so that each one determines a unique $\alpha' \in V_1$, and we have

$$(33) \qquad F_p(\alpha) = F_p(\alpha' + p\alpha'') \equiv F_p(\alpha') + F_1(\alpha'') \pmod{p}.$$

As α'' ranges over V_1, $F_p(\alpha)$ takes on the value a_p exactly p^{p-2} times. Hence the total number of vectors $\alpha \in V_2$ for which (32) and $F_p(\alpha) \equiv a_p$ (mod p) are true is exactly p^{p-2}. We have therefore proved the following theorem.

THEOREM 7. *The random variables $F_1(\alpha), \cdots, F_p(\alpha)$* (mod p) *are mutually independent.*

A simple application of Theorem 7 now yields results on the asymptotic distribution of the residues of other symmetric functions modulo p.

THEOREM 8. *Let*

$$S_k^{(n)} = x_1^k + x_2^k + \cdots + x_n^k, \qquad k > 0,$$

and let $G_k^{(n)}(a)$ be the number of solutions of

$$S_k^{(n)} \equiv a \pmod{p} \quad (0 \leqq x_i < p;\ i = 1, \cdots, n).$$

Then

$$\lim_{n\to\infty} \frac{1}{p^n} G_k^{(n)}(a) = \frac{1}{p}, \qquad 0 \leqq a < p.$$

Proof. For $n \geqq k$, we have

$$S_k^{(n)} = (-1)^{k-1} k U_k^{(n)} + f(U_1^{(n)}, \cdots, U_{k-1}^{(n)}).$$

The right side is a function of $F_1(\alpha), \cdots, F_k(\alpha)$ and so has an asymptotic distribution mod p. If $1 \leqq k < p$, these variables are independent, by Theorem 7, and since

$$S_k^{(n)} \equiv (-1)^{k-1} kF_k(\alpha) + f(F_1(\alpha), \cdots, F_{k-1}(\alpha)) \pmod{p},$$

and $k \not\equiv 0 \pmod{p}$, the theorem is proved for $1 \leqq k < p$; it follows for all $k > 0$, since $S_k^{(n)} \equiv S_{k+p-1}^{(n)} \pmod{p}$.

Another consequence of (30) is obtained by observing that

$$J(k', 0; k, c) \geqq 0, \tag{34}$$

from which we see that

$$pP_k(c) + P_{k'}(0) \geqq 1 \qquad (0 \leqq c < p). \tag{35}$$

In particular, for $c = 0$,

$$pP_k(0) + P_{k'}(0) \geqq 1. \tag{36}$$

It follows that for at least one of a correlated pair, the frequency of 0 exceeds $1/(p+1)$. For this is certainly true if $k' = 0$, and if $k' > 0$, then there is at least one vector α for which $F_k(\alpha) \equiv F_{k'}(\alpha) \equiv 0 \pmod{p}$, so that we have strict inequality in (34), (35), and (36).

An attractive conjecture is that $P_k(0) \geqq 1/p$ for $k > 0$. This is true for $p = 2$, 3, and all the evidence seems to point in this direction, but we have been able to prove only the following weaker approximations.

THEOREM 9. *For* $n \geqq 1$,

$$\frac{1}{n} \sum_{k=1}^{n} P_k(0) > \frac{1}{p+1} \cdot$$

THEOREM 10. *For* $k \geqq 1$, $P_k(0) > p^{-2(p-1)}$.

Proof of Theorem 9. Let $S(n) = \sum_{k=1}^{n} P_k(0)$. For $k \geqq 2$, we have

$$pP_k(0) + P_{k-1}(0) > 1. \tag{37}$$

Summing (37) for $2 \leqq k \leqq n$, we get

$$p(S(n) - 1/p) + S(n-1) > n - 1,$$
$$(p+1)S(n) > pS(n) + S(n-1) > n,$$

from which Theorem 9 follows.

Proof of Theorem 10. Suppose that $p^{s-1} \leqq k < p^s$. The set $\mathfrak{N}_s(p, k, 0)$ includes all those vectors α whose components satisfy $0 \leqq \alpha_r < k/(p-1)$, since the degree of the product $\Phi(\alpha, x)$ is then less than k, so that $F_k(\alpha) = 0$. The number of such vectors is at least

$$\left(\frac{k}{p-1}\right)^{p-1} \geqq \frac{p^{(s-1)(p-1)}}{(p-1)^{p-1}} > p^{s(p-1)}\cdot p^{-2(p-1)}.$$

Hence

$$P_k(0) = p^{-s(p-1)}N_s(p, k, 0) > p^{-2(p-1)}.$$

This result can of course be improved, since the number of vectors $\alpha \in V_s$ such that $\alpha_1 + \alpha_2 + \cdots + \alpha_{p-1} < k$ is given by

$$\binom{k+p-2}{p-1},$$

from which we obtain, for example, for $k \geqq 1$,

(38) $$P_k(0) \geqq p^{2-p}/p!\cdot$$

It does not seem likely that such methods will yield significantly better results, although the true lower bound of $P_k(0)$ is almost certainly of order $1/p$.

On the other hand, we observe that $P_k(0)$ cannot increase too rapidly. For

(39) $$J(k', 0; k, c) \leqq P_{k'}(0) \qquad (0 \leqq c < p),$$

so that (30) yields

(40) $$P_k(c) \leqq \frac{1}{p}(1 - P_{k'}(0)) + P_{k'}(0),$$

or if we write $Q_k = 1 - P_k(0)$ and take $c = 0$ in (40),

(41) $$Q_k \geqq \left(1 - \frac{1}{p}\right)Q_{k'}.$$

Now suppose that k exceeds p, so that

(42) $$k = t_1p^{s_1} + \cdots + t_hp^{s_h} \qquad (0 < t_i < p;\ s_1 > s_2 > \cdots > s_h \geqq 0),$$

with $h > 1$. Then, applying (41) $h-1$ times,

$$Q_k \geqq \left(1 - \frac{1}{p}\right)^{h-1} Q_{t_hp^{s_h}} = \left(1 - \frac{1}{p}\right)^{h},$$

by Theorem 6. Hence we have the following theorem.

THEOREM 11. *If h is the number of nonzero digits in the expansion of k in the scale of p, then*

(43) $$P_k(0) \leqq 1 - \left(1 - \frac{1}{p}\right)^{h}.$$

Since $k \geqq p^{h-1}$, (43) implies

$$P_k(0) \leqq 1 - \left(1 - \frac{1}{p}\right) k^{\log (1-1/p)/\log p}, \tag{44}$$

so that Q_k must be greater than k^{-m} for a certain fixed $m<1$, depending only on $p>2$.

8. **Further results on $P_k(a)$.** Suppose that

$$k = tp^s + R, \qquad s \geqq 0,\ 0 \leqq t \leqq p,\ 0 \leqq R < p^s. \tag{45}$$

The representation (45) is not necessarily unique, but this is unimportant here. A suitable vector space for $F_k(\alpha)$ is then V_{s+2}, since $k<p^{s+1}+p^s<p^{s+2}$. Now write, uniquely, for $\alpha \in V_{s+2}$,

$$\alpha = \beta p^{s+1} + \gamma, \qquad \beta \in V_1,\ \gamma \in V_{s+1}. \tag{46}$$

Then

$$\begin{aligned} \Phi(\alpha, x) &= \Phi(p^{s+1}\beta, x)\Phi(\gamma, x) \equiv \Phi(\beta, x^{p^{s+1}})\Phi(\gamma, x) \\ &\equiv \sum_{m=0}^{D_1} F_m(\beta) x^{mp^{s+1}} \sum_{n=0}^{D_2} F_n(\gamma) x^n \pmod{p}, \end{aligned} \tag{47}$$

and the degree of the second factor is

$$D_2 \leqq \sum_{r=1}^{p-1} \gamma_r \leqq (p-1)(p^{s+1}-1). \tag{48}$$

If we equate coefficients of x^k in (47),

$$F_k(\alpha) \equiv F_t(\beta)F_R(\gamma) + F_{t-1}(\beta)F_{R+p^{s+1}}(\gamma) + \cdots + F_{R+tp^{s+1}}(\gamma) \pmod{p}. \tag{49}$$

We remark that $R+(p-1)p^{s+1} \geqq (p-1)p^{s+1} > D_2$, so we may write

$$F_k(\alpha) \equiv \sum_{n=0}^{p-2} F_{t-n}(\beta)F_{R+np^{s+1}}(\gamma) \pmod{p}. \tag{50}$$

Now for fixed γ, $F_k(\alpha)$ is a linear combination of $F_t(\beta), F_{t-1}(\beta), \cdots, F_0(\beta)$. Once γ is known, it is easy to determine the distribution of this linear combination. For this purpose we separate V_{s+1} into the following classes:

$$\begin{aligned} &\mathfrak{M}_0(c, R, s+1): && F_R(\gamma) \equiv c \not\equiv 0 \pmod{p}, \\ &\mathfrak{M}_1(c, R, s+1): && F_R(\gamma) \equiv 0,\ F_{R+p^{s+1}}(\gamma) \equiv c \not\equiv 0 \pmod{p}, \\ &\cdots\cdots\cdots && \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\mathfrak{M}_{p-2}(c, R, s+1): && F_R(\gamma) \equiv \cdots \equiv F_{R+(p-3)p^{s+1}}(\gamma) \equiv 0, \\ & && F_{R+(p-2)p^{s+1}}(\gamma) \equiv c \not\equiv 0 \pmod{p}, \\ &\mathfrak{M}_\infty(R, s+1): && F_R(\gamma) \equiv \cdots \equiv F_{R+(p-2)p^{s+1}}(\gamma) \equiv 0 \pmod{p}. \end{aligned} \tag{51}$$

Let $M_n(c, R, s+1)=M_n(c)$ be the number of elements in $\mathfrak{M}_n(c, R, s+1)$, $0\leqq n\leqq p-2$, and let

$$(52)\qquad \begin{aligned} Z_n(R, s+1) &= Z_n = \sum_{c=1}^{p-1} M_n(c) \qquad (0 \leqq n \leqq p-2), \\ Z_\infty(R, s+1) &= Z_\infty = \textit{number of elements in } \mathfrak{M}_\infty(R, s+1). \end{aligned}$$

It is clear that any vector γ not appearing in $\mathfrak{M}_\infty(r, s+1)$ must belong to some $\mathfrak{M}_n(c, R, s+1)$, and all these classes are disjoint. Hence

$$(53)\qquad N(s+1) = Z_0 + Z_1 + \cdots + Z_{p-2} + Z_\infty.$$

Now fix $a\not\equiv 0 \pmod p$, and suppose that γ belongs to one of the classes $\mathfrak{M}_n(c, R, s+1)$, $n<t$. Then from (50) and Theorem 7, the number of vectors β for which $F_k(\alpha)\equiv a \pmod p$ is $p^{-1}N(1)$. If $\gamma\in\mathfrak{M}_t(a, R, s+1)$, this number is $N(1)$. For all other $\gamma\in V_{s+1}$, the number is 0. It follows that

$$(54)\qquad N_{s+2}(p, k, a) = N(1)\left\{\frac{1}{p}\sum_{n<t} Z_n + M_t(a)\right\} \qquad (a \not\equiv 0 \pmod p).$$

Hence

$$(55)\qquad P_k(a) = \frac{1}{N(s+1)}\left\{\frac{1}{p}\sum_{n<t} Z_n + M_t(a)\right\} \qquad (a \not\equiv 0 \pmod p).$$

Summing (55) over all $a\not\equiv 0 \pmod p$, and taking into account (52) and (53), we get

$$(56)\qquad P_k(0) = \frac{1}{N(s+1)}\left\{\frac{1}{p}\sum_{n<t} Z_n + \sum_{n>t} Z_n + Z_\infty\right\}.$$

Equations (55) and (56) yield several interesting results. First is the observation that for $t=p-1$ or p, (55) becomes

$$(57)\qquad P_{tp^s+R}(a) = \frac{1}{N(s+1)}\left\{\frac{1}{p}\sum_{n=0}^{p-2} Z_n\right\} = \frac{1}{p}\left\{1 - \frac{Z_\infty}{N(s+1)}\right\} \qquad (t = p-1, p).$$

Hence the nonzero residues all have the same frequency. Also

$$(58)\qquad P_{tp^s+R}(0) = \frac{1}{p} + \left(1 - \frac{1}{p}\right)\frac{Z_\infty}{N(s+1)} \qquad (t = p-1, p),$$

and this is never less than $1/p$. Indeed, if $R\neq 0$, $Z_\infty(R, s+1)/N(s+1)$ exceeds a certain constant, depending only on p. For if we split $\gamma\in V_{s+1}$ into

$$\gamma = \delta + p^{s'}\eta, \qquad \delta \in V_{s'},\ \eta \in V_{s+1-s'},$$

where s' is determined by $p^{s'-1} \leqq R < p^{s'}$, then $Z_\infty(R, s+1)$ is not less than $N(s+1-s')$ multiplied by the number of $\delta \in V_{s'}$ for which $\delta_1 + \cdots + \delta_{p-1} < R$. By exactly the same argument that gave (38), we see that this number, in turn, is not less than $(p^{2-p}/p!)N(s')$. Finally

$$\frac{Z_\infty(R, s+1)}{N(s+1)} \geqq \frac{p^{2-p}}{p!} \cdot \frac{N(s')N(s+1-s')}{N(s+1)} = \frac{p^{2-p}}{p!},$$

$$P_k(0) \geqq \frac{1}{p} + \left(1 - \frac{1}{p}\right)\frac{p^{2-p}}{p!} \tag{59}$$

$$((p-1)p^s < k < p^{s+1};\ p^{s+1} < k < p^{s+1} + p^s).$$

We have therefore proved the following theorem.

THEOREM 12. *If $(p-1)p^s < k < p^{s+1}$, and $k^* = k + p^s$, then*

(i) $$P_k(a) = P_{k^*}(a) \qquad (0 \leqq a < p),$$

(ii) $$P_k(1) = \cdots = P_k(p-1),$$

(iii) $$P_k(0) \geqq \frac{1}{p} + \left(1 - \frac{1}{p}\right)\frac{p^{2-p}}{p!}.$$

Part (iii) of Theorem 12 enables us to improve the average in Theorem 9 in an obvious way, but we shall not take the trouble to state the result, which we feel is far from the optimum. Also, (iii) is uniform in the range of k indicated, and can be improved for special values of k. For example, if $s \geqq 2$, $p \geqq 5$, we can prove

(iv) $$P_{p^s-1}(0) > \frac{1}{p}\left\{1 + \frac{1}{(p-2)!}\right\}.$$

9. **Relations among $P_k(0)$.** In this section we shall deal exclusively with $P_k(0)$, for $k = tp^s + R$, $0 \leqq t < p$, $0 \leqq R < p^s$. We shall write

$$\rho_n = \frac{Z_n}{N(s+1)},$$

$$\rho_\infty = \frac{Z_\infty}{N(s+1)}, \tag{60}$$

$$\phi_t = P_{tp^s+R}(0).$$

Equations (53) and (56) then become

$$\rho_0 + \rho_1 + \cdots + \rho_{p-2} + \rho_\infty = 1, \tag{61}$$

$$\phi_t = \frac{1}{p}\sum_{n<t} \rho_n + \sum_{n>t} \rho_n + \rho_\infty \qquad (t = 0, 1, \cdots, p-1). \tag{62}$$

From (62),

$$(63)\quad \begin{aligned} \phi_i - \phi_{i-1} &= \frac{1}{p}\rho_{i-1} - \rho_i \qquad (i = 1, \cdots, p-2),\\ \phi_{p-1} - \phi_{p-2} &= \frac{1}{p}\rho_{p-2}. \end{aligned}$$

Multiply the ith equation in (63) by p^i, then add, to get

$$(64)\quad \begin{aligned} \rho_0 &= p(\phi_1 - \phi_0) + p^2(\phi_2 - \phi_1) + \cdots + p^{p-1}(\phi_{p-1} - \phi_{p-2})\\ &= -p\phi_0 - p(p-1)\phi_1 - p^2(p-1)\phi_2 - \cdots\\ &\quad - p^{p-2}(p-1)\phi_{p-2} + p^{p-1}\phi_{p-1}. \end{aligned}$$

But by (62) and (61),

$$(65)\qquad \phi_0 = \rho_1 + \rho_2 + \cdots + \rho_{p-2} + \rho_\infty = 1 - \rho_0.$$

Hence (64) becomes

$$(66)\qquad p^{p-1}\phi_{p-1} = 1 + (p-1)\{\phi_0 + p\phi_1 + p^2\phi_2 + \cdots + p^{p-2}\phi_{p-2}\}.$$

If we now define the weights

$$(67)\qquad w_\infty = p^{-(p-1)}; \qquad w_n = p^{-(p-1)}(p-1)p^n \qquad (0 \leqq n \leqq p-2),$$

and remark that $w_\infty + w_0 + \cdots + w_{p-2} = 1$, we have

$$(68)\qquad \phi_{p-1} = w_\infty + w_0\phi_0 + w_1\phi_1 + \cdots + w_{p-2}\phi_{p-2}.$$

THEOREM 13. *For every p, there is a fixed set of weights*

$$w_\infty = p^{-(p-1)}; \qquad w_n = p^{-(p-1)}(p-1)p^n \qquad (0 \leqq n \leqq p-2),$$

such that for all $s \geqq 0$ and $0 \leqq R < p^s$,

$$(69)\qquad P_{(p-1)p^s+R}(0) = w_\infty + \sum_{n=0}^{p-2} w_n P_{np^s+R}(0).$$

As a check, set $p=2$. Then (69) yields

$$P_{2^s+R}(0) = \frac{1}{2} + \frac{1}{2}P_R(0),$$

which agrees with our previously established result.

10. **Conclusion.** It appears, from the results that we have obtained so far, that the function $P(p, k, a)$ is rather complicated. The rôle of the residue 0 is a special one, and all the evidence so far seems to corroborate the conjecture that $P(p, k, 0) \geqq 1/p$ for all $k > 0$. There are several other interesting questions which we should like to see answered. For example, is it true that the limit superior of $P(p, k, 0)$ (as k tends to infinity) is unity? Is it true that $P(p, pk, a)$

$=P(p, k, a)$? Is it true that only in the case $k=tp^s$, $0<t<p$, do we have equidistribution among all the residues, or, even more, that only in this case does $P(p, k, 0)$ take the value $1/p$?

It is possible to extend some of the results obtained here to the case of a composite modulus. For example, Theorem 1 goes through without any difficulty. Furthermore, it is sufficient to consider only prime-power moduli, in view of a lemma of Hull(4), which in our notation would yield

$$P_n(mm', k, a) = P_n(m, k, a)P_n(m', k, a)$$

if $(m, m')=1$.

Bibliography

1. G. H. Hardy and J. E. Littlewood, Math. Zeit. vol. 12 (1922) pp. 161–188.
2. Ralph Hull, Trans. Amer. Math. Soc. vol. 34 (1932) pp. 908–937.
3. André Weil, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 497–508.
4. N. J. Fine and Ivan Niven, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 89–93.
5. E. Lucas, *Théorie des nombres*, pp. 417–420.
6. N. J. Fine, Amer. Math. Monthly vol. 54 (1947) pp. 589–592.

University of Pennsylvania,
Philadelphia, Pa.

[4] See [2, p. 910].