Acta Mathematica Academiae Scientiarum Hungaricae
Tomus 18 (1—2), 1967, pp. 151—163.

ON SOME PROBLEMS OF A STATISTICAL GROUP-THEORY. II

By

P. ERDŐS and P. TURÁN (Budapest), members of the Academy

1. In the first paper of this series[1] we showed that for almost all elements P of the symmetric group S_n of n letters (i.e. apart from at most $o(n!)$ P's) the order $\mathbf{O}(P)$ of P satisfies the inequality

$$\left|\log \mathbf{O}(P) - \frac{1}{2}\log^2 n\right| < \omega(n)\log^{\frac{3}{2}} n \tag{1.1}$$

if only $\omega(n) \to \infty$ with n. Hence $\log \mathbf{O}(P)$ is for almost all P's much less than its maximum, which is as LANDAU [2] proved, $\sim \sqrt{n \log n}$. Though several questions in the first paper were left to later papers of this series and we intend indeed to return to them in paper III, in this paper we launch another trend which seems to us equally interesting in itself and perhaps even more inherent to the algebraic aspects. This refers to the arithmetical structure of the order $\mathbf{O}(P)$. We assert the following theorems.[3]

THEOREM I. *If $\omega(n) \to \infty$ with n arbitrarily slowly then for almost all P's the order $\mathbf{O}(P)$ is divisible by all prime-powers not exceeding* A[4]

$$A \overset{\text{def}}{=} \frac{\log n}{\log_2 n}\left\{1 + 3\frac{\log_3 n}{\log_2 n} - \frac{\omega(n)}{\log_2 n}\right\}. \tag{1.2}$$

As an immediate corollary of this theorem we remark that "almost no" P's have a square-free order $\mathbf{O}(P)$ and for arbitrarily large integer b the order $\mathbf{O}(P)$ is for almost all P's divisible by b.

How far is this Theorem I best-possible? We shall prove that replacing in (1. 2) the term $\left(-\frac{\omega(n)}{\log_2 n}\right)$ by $\left(+\frac{\omega(n)}{\log_2 n}\right)$ then only $o(n!)$ P's have this property. However we shall state this in a slightly stronger form as

[1] *Zeitschr. für Wahrscheinlichkeitstheorie und verw. Gebiete*, **4** (1965), pp. 175—186.

[2] *Handbuch der Lehre von der Verteilung der Primzahlen*, 1909, Bd. I. p. 222.

[3] The starting point of these investigations was the question of A. SCHINZEL, whether or not for almost all P's $\mathbf{O}(P)$ is even.

[4] Throughout this paper $\log_v n$ means v-times iterated logarithms.

THEOREM II. *If $\omega(n)\to\infty$ arbitrarily slowly with n then for almost all P's the order $\mathbf{O}(P)$ is not divisible by some prime not exceeding*

$$B \overset{\text{def}}{=} \frac{\log n}{\log_2 n}\left\{1+3\frac{\log_3 n}{\log_2 n}+\frac{\omega(n)}{\log_2 n}\right\}. \tag{1.3}$$

For the sake of orientation we remark that for primes $>c\log n$ much more is true. We formulate the

THEOREM III. *If α is fixed positive number and p_0 is any prime of form $(\alpha+o(1))\log n$ we have for the number $b(n)$ of P's with the property $\mathbf{O}(P)$ being not divisible by p_0 the relation*

$$\lim_{n\to\infty}\frac{b(n)}{n!}=e^{-\frac{1}{\alpha}} \tag{1.4}$$

holds.

In particular if $\omega(n)\to\infty$ arbitrarily slowly with n and $p_0>\omega(n)\log n$, then for almost all P's $\mathbf{O}(P)$ is not divisible by p_0.

2. What are the corresponding theorems for "large" prime-factors of $\mathbf{O}(P)$? As to this we assert the

THEOREM IV. *If $\varepsilon(n)$ is positive and tends with $1/n$ to zero arbitrarily slowly, then for almost all P's $\mathbf{O}(P)$ is not divisible by any prime*

$$>ne^{-\varepsilon(n)\sqrt{\log n}}. \tag{2.1}$$

Again we shall prove that this theorem is essentially best possible by showing that replacing in (2.1) $\varepsilon(n)$ by $1/\varepsilon(n)$ the situation completely changes. We assert this fact as

THEOREM V. *If $\omega(n)$ tends to infinity with n whatever slowly then for almost all P's $\mathbf{O}(P)$ has a prime-factor*

$$>ne^{-\omega(n)\sqrt{\log n}} \tag{2.2}$$

From theorems IV and V one has the following somewhat surprising

COROLLARY. *If $\omega(n)$ tends to ∞ with n arbitrarily slowly then for almost all P's the maximal prime-factor of $\mathbf{O}(P)$ is between $ne^{-\omega(n)\sqrt{\log n}}$ and $ne^{-\frac{1}{\omega(n)}\sqrt{\log n}}$.*

Further we proved that for an arbitrarily small $\varepsilon>0$ for almost all P's the number of prime-factors of $\mathbf{O}(P)$ (counting with or without multiplicity) is between $(1\pm\varepsilon)\log n\cdot\log_2 n$. Since the proof does not differ essentially from that of Theorem II, we shall not go into details.

As one can easily see from our subsequent proofs we laid no particular stress to squeeze out sharpest possible laws. E.g. our proof for Theorem V would result also that for almost all P's $\mathbf{O}(P)$ has not only one but several prime-factors satisfying (2.2). We could show that the number of P's whose group-order $\mathbf{O}(P)$ is divisible by all prime-powers not exceeding

$$\frac{\log n}{\log_2 n}\left\{1+3\frac{\log_3 n}{\log_2 n}-\frac{c}{\log_2 n}\right\} \qquad (c \text{ real})$$

divided by $n!$ has a distribution function $f_1(c)$ and the same holds for the number of P's whose order is not divisible by any prime greater than

$$ne^{-e^c\sqrt{\log n}} \qquad (c \text{ real}).$$

Our theorems refer to the group S_n; obviously the same holds for the alternating group A_n of n letters too.

We call the attention also to Theorem VI in **8**.

As the first of us remarked that by the same method as used in the proof of Theorem II, combined with the sharpened form of the prime number theorem for arithmetical progressions he can prove the following theorem. Let $\omega(n) \to \infty$ arbitrarily slowly then for almost all integers $m \leqq n$ the Euler-function $\varphi(m)$ is divisible by all primes not exceeding

$$\frac{\log_2 n}{\log_3 n}\left\{1+3\,\frac{\log_4 n}{\log_3 n}-\frac{\omega(n)}{\log_3 n}\right\}$$

and $\varphi(m)$ has $(1+o(1))\,\frac{1}{2}\,(\log\log n)^2$ prime factors.

3. Next we turn to the proof of our theorems. We represent P uniquely as union of disjoint cycles; let P consist of m_1 cycles of length n_1, m_2 cycles of length n_2, ... so that

$$n_1 < n_2 < \ldots < n_k, \qquad k = k(P) \tag{3.1}$$

$$n = m_1 n_1 + m_2 n_2 + \ldots + m_k n_k. \tag{3.2}$$

The number of those P's with prescribed k, m_ν's and n_ν's is, as remarked by Cauchy[5]

$$\frac{n!}{m_1!\, m_2! \ldots m_k!\, n_1^{m_1} n_2^{m_2} \ldots n_k^{m_k}}. \tag{3.3}$$

It is well-known that

$$\mathbf{O}(P) = [n_1, n_2, \ldots, n_k]. \tag{3.4}$$

Let p^α be an arbitrary prime-power $\leqq n$ and $f(n, p^\alpha)$ be the number of P's such that $\mathbf{O}(P)$ is *not* divisible by p^α. Then Theorem I will be any easy consequence of the

LEMMA I. *For $f(n, p^\alpha)$ we have the nice exact formula*

$$\frac{f(n,p^\alpha)}{n!} = \left(1-\frac{1}{p^\alpha}\right)\left(1-\frac{1}{2p^\alpha}\right)\ldots\left(1-\frac{1}{\left[\dfrac{n}{p^\alpha}\right]p^\alpha}\right). \tag{3.5}$$

For the proof we remark first that the left-side of (3. 5) is owing to (3. 3) nothing else than the coefficient of z^n in

$$\prod_\nu{}' \left\{1+\frac{1}{1!}\,\frac{z^\nu}{\nu}+\frac{1}{2!}\left(\frac{z^\nu}{\nu}\right)^2+\ldots\right\}$$

[5] See e. g. J. RIORDAN's book *An introduction to combinatorial analysis*, New York, 1958.

where the prime means that the product is to be extended to all v's divisible by the $(\alpha-1)$th power of p at most. But this can be written for $|z|<1$ as

$$\prod_{v}{}' \exp\frac{z^v}{v} = \exp\left\{\sum_{v=1}^{\infty}\frac{z^v}{v} - \sum_{v=1}^{\infty}\frac{z^{vp^\alpha}}{vp^\alpha}\right\} = \frac{(1-z^{p^\alpha})^{\frac{1}{p^\alpha}}}{1-z} = \left(\frac{1+z+z^2+\ldots+z^{p^\alpha-1}}{(1-z)^{p^\alpha-1}}\right)^{\frac{1}{p^\alpha}} =$$

$$= (1+z+z^2+z^3+\ldots+z^{p^\alpha-1})(1-z^{p^\alpha})^{-\frac{p^\alpha-1}{p^\alpha}} =$$

$$= (1+z+z^2+\ldots+z^{p^\alpha-1})\left[1+\sum_{m=1}^{\infty}\left(1-\frac{1}{p^\alpha}\right)\left(1-\frac{1}{2p^\alpha}\right)\left(1-\frac{1}{3p^\alpha}\right)\ldots\left(1-\frac{1}{mp^\alpha}\right)z^{mp^\alpha}\right],$$

which proves the lemma at once.

For later use we remark that if p, q are different primes and $g(n, p, q)$ is the number of P's such that $\mathbf{O}(P)$ is divisible neither by p nor by q then the same reasoning gives that $\frac{1}{n!}g(n, p, q)$ equals the coefficient of z^n in the MacLaurin series of

$$\frac{(1-z^p)^{\frac{1}{p}}(1-z^q)^{\frac{1}{q}}}{(1-z)(1-z^{pq})^{\frac{1}{pq}}} \overset{\text{def}}{=} G_{p,q}(z). \tag{3.6}$$

4. For the proof of Theorem I we estimate $\frac{1}{n!}f(n, p^\alpha)$ from above using Lemma I. This gives for $p^\alpha \leqq n$

$$\frac{1}{n!}f(n,p^\alpha) < \exp\left\{-\frac{1}{p^\alpha}\sum_{1\leqq v\leqq\left[\frac{n}{p^\alpha}\right]}\frac{1}{v}\right\} <$$

$$< \exp\left\{-\frac{\log\left[\frac{n}{p^\alpha}\right]}{p^\alpha}\right\} < 3\exp\left\{-\frac{\log\frac{n}{p^\alpha}}{p^\alpha}\right\}. \tag{4.1}$$

Hence the number of P's whose order is not divisible by a prime-power p^α not exceeding A (in (1.2)) we get the upper bound [6]

$$S \overset{\text{def}}{=} 3\sum_{p^\alpha\leqq A}\exp\left\{-\frac{\log\frac{n}{p^\alpha}}{p^\alpha}\right\} < c_1\sum_{p^\alpha\leqq A}\exp\left\{-\frac{\log n}{p^\alpha}\right\} < c_2\int_2^A\frac{1}{\log x}\exp\left\{-\frac{\log n}{x}\right\}dx.$$

Since

$$A < \frac{\log n}{\log_2 n}\cdot\frac{1}{1-3\frac{\log_3 n}{\log_2 n}+\frac{\omega(n)}{2\log_2 n}} \overset{\text{def}}{=} A_1$$

[6] $c_1, c_2, \ldots$ denote positive numerical constants.

we have

$$S < c_2 \int_2^{A_1} \frac{1}{\log x} \exp\left\{-\frac{\log n}{x}\right\} dx. \tag{4.2}$$

The integral over $\left(2, \frac{\log n}{\log_2 n}\right)$ is evidently

$$< c_3 \frac{\log n}{\log_2 n} \cdot \frac{1}{\log n} = \frac{c_3}{\log_2 n}. \tag{4.3}$$

For the remaining integral S' we get substituting

$$x = \frac{\log n}{\log_2 n - y}$$

$$S' = c_2 \int_0^{3\log_3 n - \frac{1}{2}\omega(n)} \frac{e^y dy}{\left(1 - \frac{\log(\log_2 n - y)}{\log_2 n}\right)\left(1 - \frac{y}{\log_2 n}\right)^2} \cdot \frac{1}{(\log_2 n)^3} <$$

$$< \frac{c_3}{(\log_2 n)^3} \int_0^{3\log_3 n - \frac{1}{2}\omega(n)} e^y dy < c_3 e^{-\frac{1}{2}\omega(n)} \to 0$$

if $n \to \infty$, which together with (4. 3) and (4. 2) proves the theorem.

The proof of Theorem III follows also easily from Lemma I. This gives namely

$$\frac{1}{n!} f(n, p_0) = \prod_{1 \leqq v \leqq \left[\frac{n}{p_0}\right]} \left(1 - \frac{1}{v p_0}\right) = \exp\left\{-\frac{1}{p_0} \sum_{1 \leqq v \leqq \left[\frac{n}{p_0}\right]} \frac{1}{v} + O\left(\frac{1}{p_0^2}\right)\right\} =$$

$$= (1 + o(1)) \exp\left(-\frac{\log n}{p_0}\right)$$

which already proves Theorem III. [7]

5. For the proof of Theorem II we shall need as to the coefficient of z^n in (3. 6) the

LEMMA II. *If*

$$\log^{\frac{3}{4}} n \leqq p < q \leqq 10 \frac{\log n}{\log_2 n} \tag{5.1}$$

and n is sufficiently large then

$$\frac{1}{n!} g(n, p, q) = n^{-\frac{1}{p} - \frac{1}{q}} \left\{1 + O(\log^{-\frac{1}{2}} n)\right\}.$$

[7] The ordo-sign refers throughout this paper to $n \to \infty$.

If p and q were fixed and $n \to \infty$, the relation

$$\text{coeffs } z^n \text{ in } G_{p,q}(z) \sim \frac{p^{\frac{1}{p}} q^{\frac{1}{q}}}{(pq)^{\frac{1}{pq}}} \cdot \frac{n^{-\frac{1}{p}-\frac{1}{q}+\frac{1}{pq}}}{\Gamma\left(\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\right)}$$

would follow from known result of Darboux; [8] but here p and q vary with n as restricted by (5. 1). A sketch of the rather technical proof we shall postpone to an Appendix. A more direct (real-variable or algebraic) approach to the determination of this coefficient would be desirable. [9]

6. The proof of Theorem II (and also Theorem V) will be based on an idea which was introduced into arithmetics in 1934 by one of us;[10] this is on the way to become a part of the folklore in this subject. Let (with B in (1. 3))

$$\frac{1}{2}\frac{\log n}{\log_2 n} \leqq p_1 < p_2 < \ldots < p_l \leqq B \tag{6.1}$$

be all primes in this interval; if n is sufficiently large, we have

$$\frac{1}{10}\frac{\log n}{(\log_2 n)^2} < l < 3\frac{\log n}{(\log_2 n)^2}. \tag{6.2}$$

We introduce the function $h(P)$ of P as the number of the p_j's from (6. 1) which do *not* divide $\mathbf{O}(P)$. For this $h(P)$ we shall prove two simple lemmata.

LEMMA III. *Putting* $S_1 = \frac{1}{n!}\sum_P h(P)$ *we have*

$$S_1 = \sum_{\nu=1}^{l} \exp\left\{-\frac{\log n}{p_\nu}\right\} + O(1).$$

For the proof we remark first that with notation of Lemma I we have

$$S_1 = \frac{1}{n!}\sum_{\nu=1}^{l} f(n, p_\nu). \tag{6.3}$$

Applying Lemma I this gives

$$S_1 = \sum_{\nu=1}^{l}\left(1-\frac{1}{p_\nu}\right)\left(1-\frac{1}{2p_\nu}\right)\ldots\left(1-\frac{1}{\left[\frac{n}{p_\nu}\right]p_\nu}\right).$$

[8] G. DARBOUX, Memoire sur l'approximation des fonctions de très grands nombres etc., *Journ. de math. pures et appl.*, Ser. **III**. Tome **IV** (1878).

[9] The same holds for the functions $(1-z)^{pq}(1-z^{pq})(1-z^p)^{-q}(1-z^q)^{-p}$ which — and their obvious generalization — reminds one to the cyclotomic polynomials.

[10] P. TURÁN, On a theorem of Hardy and Ramanujan, *Journ. London Math. Soc.*, **9** (**4**) (1934), pp. 274—276 and Über einige Verallgemeinerungen eines Satzes von Hardy und Ramanujan, *ibid.*, **11** (1936), pp. 125—133. See also the beautiful booklet of M. KAC, Statistical independence in probability, analysis and number theory, *Carus Math. Monographs*, No. **12**.

Using (6. 1) (and (1. 3)) the product is

$$\exp\left\{-\frac{1}{p_\nu}\log\frac{n}{p_\nu}+O\left(\frac{1}{p_\nu}\right)\right\}=\exp\left\{-\frac{\log n}{p_\nu}+O\left(\frac{\log p_\nu}{p_\nu}\right)\right\}=$$

$$=\left\{1+O\left(\frac{(\log_2 n)^2}{\log n}\right)\right\}\exp\left\{-\frac{\log n}{p_\nu}\right\}$$

and thus, using (6. 2)

$$S_1=\sum_{\nu=1}^{l}\exp\left\{-\frac{\log n}{p_\nu}\right\}+O(1)$$

as stated.

Further we need the

LEMMA IV. *Putting* $S_2=\frac{1}{n!}\sum_P h(P)^2$ *we have*

$$S_2<\left\{\sum_{\nu=1}^{l}\exp\left(-\frac{\log n}{p_\nu}\right)\right\}^2\left(1+O\left(\frac{1}{\sqrt{\log n}}\right)\right)+\sum_{\nu=1}^{l}\exp\left(-\frac{\log n}{p_\nu}\right)+O(1).$$

For the proof we write (p_j's in (6. 1))

$$S_2=\frac{1}{n!}\sum_P\Big(\sum_{p_\mu\mid O(P)}1\Big)\Big(\sum_{p_\nu\mid O(P)}1\Big).$$

The contribution of the pairs with $\mu=\nu$ is obviously S_1; hence

$$S_2=S_1+2\sum_{1\le\mu<\nu\le l}\left(\frac{1}{n!}\sum_{\substack{p_\mu\mid O(P)\\ p_\nu\mid O(P)}}1\right)=S_1+2\sum_{1\le\mu<\nu\le l}\frac{1}{n!}g(n,p_\mu,p_\nu) \tag{6.4}$$

with the notation of (3. 6). Using the remark (3. 6) and Lemma II we get

$$S_2=S_1+2\left(\sum_{1\le\mu<\nu\le l}n^{-\frac{1}{p_\mu}-\frac{1}{p_\nu}}\right)\left(1+O\left(\frac{1}{\sqrt{\log n}}\right)\right).$$

Using also Lemma III we get

$$S_2<\sum_{\mu=1}^{l}\exp\left(-\frac{\log n}{p_\mu}\right)+O(1)+\left(1+\frac{O(1)}{\sqrt{\log n}}\right)\left(\sum_{\mu=1}^{l}\exp\left(-\frac{\log n}{p_\mu}\right)\right)^2$$

as stated.

7. Lemma III and IV give quickly the proof of Theorem II. We form the expression

$$Z\overset{\text{def}}{=}\frac{1}{n!}\sum_P\left(h(P)-\sum_{\mu=1}^{l}\exp\left(-\frac{\log n}{p_\mu}\right)\right)^2. \tag{7.1}$$

Lemma III and IV give at once

$$Z=O\left(\frac{1}{\sqrt{\log n}}\right)\left(\sum_{\mu=1}^{l}\exp\left(-\frac{\log n}{p_\mu}\right)\right)^2+O(1)\left\{1+\sum_{\mu=1}^{l}\exp\left(-\frac{\log n}{p_\mu}\right)\right\}. \tag{7.2}$$

Let U be the set of P's with

$$h(P)=0$$

and $|U|$ their number; (7. 1) and (7. 2) give a fortiori

$$\frac{|U|}{n!} < O(1)\left\{\frac{1}{\sqrt{\log n}}+\left(\sum_{\mu=1}^{l}\exp\left(-\frac{\log n}{p_\mu}\right)\right)^{-1}+\left(\sum_{\mu=1}^{l}\exp\left(-\frac{\log n}{p_\mu}\right)\right)^{-2}\right\}. \tag{7.3}$$

If we succeed in proving

$$V \overset{\text{def}}{=} \sum_{\mu=1}^{l}\exp\left(-\frac{\log n}{p_\mu}\right)\to\infty$$

with n we are ready. But

$$V > \sum_{\left|p-\frac{\log n}{\log_2 n}\left(1+3\frac{\log_3 n}{\log_2 n}\right)\right|\leqq\omega(n)\frac{\log n}{(\log_2 n)^2}}\exp\left(-\frac{\log n}{p}\right)$$

which is analogously as in **4.**

$$> \frac{c_4}{(\log_2 n)^3}\int_{3\log_3 n-\frac{1}{2}\omega(n)}^{3\log_3 n+\frac{1}{2}\omega(n)}\frac{e^y\,dy}{\left(1-\frac{y}{\log_2 n}\right)^2\left(1-\frac{\log(\log_2 n-y)}{\log_2 n}\right)} >$$

$$> \frac{c_5}{(\log_2 n)^3}\int_{3\log_3 n-\frac{1}{2}\omega(n)}^{3\log_3 n+\frac{1}{2}\omega(n)} e^y\,dy\to\infty$$

indeed.

8. The proof of Theorem IV, once having Lemma I is again easy. This gives namely if $\bar{f}(n, p)$ stands for the number of those P's, whose order $\mathbf{O}(P)$ is divisible by p the exact formula

$$\frac{\bar{f}(n,p)}{n!}=1-\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{\left[\frac{n}{p}\right]p}\right) < 1-\exp\left(-\frac{1}{p}\log\frac{n}{p}+O\left(\frac{1}{p}\right)\right)$$

i. e., if $p>\sqrt{n}$ say,

$$\frac{\bar{f}(n,p)}{n!} < \frac{\log\frac{n}{p}}{p}+O\left(\frac{1}{p}\right). \tag{8.1}$$

Hence for the proof of our Theorem IV we have only to show that

$$\sum_{n\exp(-\varepsilon(n)\sqrt{\log n})\leqq p\leqq n}\left\{\frac{1}{p}\log\frac{n}{p}+O\left(\frac{1}{p}\right)\right\}\to 0.$$

For the second sum this is well-known; for the first it follows easily since it cannot exceed

$$\varepsilon(n)\sqrt{\log n} \sum_{n\exp(-\varepsilon(n)\sqrt{\log n}) \leqq p \leqq n} \frac{1}{p}$$

which tends to 0 indeed.

9. The proof of Theorem V will be easy after having the Theorem VI, which is of independent interest. This is the following.

THEOREM VI. *Let*

$$1 \leqq a_1 < a_2 < \ldots < a_s \leqq n \tag{9. 1}$$

be a sequence of integers. Then the number of P's having no cycles with the length a_1 or a_2 ... or a_s, cannot exceed the quantity

$$\frac{n!}{\sum_{\nu=1}^{s} \frac{1}{a_\nu}}.$$

Hence if $\sum_{\nu=1}^{s} a_\nu^{-1}$ tends with n to ∞, then almost all P's have at least one cycle the length of which is among the numbers in (9. 1).

The proof of Theorem VI will be based again on the dispersion-idea. Let $L(P)$ be the number of the a_ν's from (9. 1) with the property that P has a cycle with length a_ν. Then we assert the

LEMMA V. *Denoting the expression*

$$\frac{1}{n!} \sum_{P} L(P)$$

by H_1 we have

$$H_1 = \sum_{\nu=1}^{s} \frac{1}{a_\nu}.$$

For the proof we start from the fact that

$$H_1 = \sum_{\nu=1}^{s}{}' \left(\frac{1}{n!} \sum_{P}{}' 1 \right) \tag{9. 2}$$

where the summation within the bracket refers to all P's containing a cycle with the length a_ν (ν fixed). But what is the value of this sum? The elements of this cycle can be selected in $\binom{n}{a_\nu}$ ways; after selection each can be written down on $a_\nu!$ ways. Since a cyclic permutation gives the same cycle, our selection gives rise to

$$\binom{n}{a_\nu} a_\nu! \frac{1}{a_\nu} = \frac{n!}{a_\nu (n-a_\nu)!}$$

different cycles of length a_ν. Each can be completed to a P by permuting the remaining $(n-a_\nu)$ elements. Hence the value of the inner bracket is for fixed ν $1/a_\nu$, which proves the lemma.

We need further the

LEMMA VI. *Denoting the expression*

$$\frac{1}{n!}\sum_P L(P)^2$$

by H_2 *we have*

$$H_2 \leqq \sum_{\nu=1}^{s}\frac{1}{a_\nu}+\left(\sum_{\nu=1}^{s}\frac{1}{a_\nu}\right)^2.$$

For the proof we start from the fact that

$$H_2 = \frac{1}{n!}\sum_P\Big(\sum_{a_\mu \text{ in } P}1\Big)\Big(\sum_{a_\nu \text{ in } P}1\Big) = H_1+2\sum_{\substack{1\leqq\mu<\nu\leqq S\\ a_\mu+a_\nu\leqq n}}\left(\frac{1}{n!}\sum_P{}''1\right) \tag{9.3}$$

where the $\sum''$ is to be extended to all P's having two cycles with the length a_μ and a_ν respectively. What is the value of the inner sum in (9. 3)? The cycle of length a_μ can be filled as before in $\dfrac{n!}{a_\mu(n-a_\mu)!}$ ways; the cycle of length a_ν afterwards in

$$\frac{(n-a_\mu)!}{a_\nu(n-a_\mu-a_\nu)!}$$

ways. Each can be completed to a P in $(n-a_\mu-a_\nu)!$ ways. Hence the value of the expression in the bracket in (9. 3) is $1/a_\mu a_\nu$. Hence

$$H_2 = \sum_{\nu=1}^{s}\frac{1}{a_\nu}+2\sum_{\substack{1\leqq\mu<\nu\leqq s\\ a_\mu+a_\nu\leqq n}}\frac{1}{a_\mu a_\nu} < \sum_{\nu=1}^{s}\frac{1}{a_\nu}+\left(\sum_{\nu=1}^{s}\frac{1}{a_\nu}\right)^2 \tag{9.4}$$

indeed.

In order to prove Theorem V we consider the expression

$$Z_1 \overset{\text{def}}{=} \frac{1}{n!}\sum_P\left(L(P)-\sum_{\nu=1}^{s}\frac{1}{a_\nu}\right)^2. \tag{9.5}$$

From Lemma V and VI we get

$$Z_1 < \sum_{\nu=1}^{s}\frac{1}{a_\nu}. \tag{9.6}$$

Denoting by U_1 the set of P's with $L(P)=0$ and by $|U_1|$ the number of P's in U_1 (9. 5) and (9. 6) give

$$\frac{|U_1|}{n!} < \left(\sum_{\nu=1}^{s}\frac{1}{a_\nu}\right)^{-1}$$

i.e. Theorem VI is proved already.

10. In order to deduce Theorem V from Theorem VI we define the a_ν's as all multiples of all primes in the interval

$$I: \quad n\exp\left(-\omega(n)\sqrt{\log n}\right) \leqq p \leqq n \tag{10.1}$$

which do not exceed n. The sum of their reciprocals is

$$\sum_{p\subset I}\frac{1}{p}\sum_{\nu\leqq\frac{n}{p}}\frac{1}{\nu} = \sum_{p\subset I}\frac{1}{p}\log\frac{n}{p}+O(1)\sum_{p\subset I}\frac{1}{p} = \sum_{p\subset I}\frac{1}{p}\log\frac{n}{p}+O(1). \tag{10.2}$$

The remaining sum is

$$> \sum_{p\subset I_1}\frac{1}{p}\log\frac{n}{p}$$

where I_1 stands for the interval

$$n\exp\left\{-\omega(n)\sqrt{\log n}\right\} \leqq p \leqq n\exp\left\{-\frac{\omega(n)}{2}\sqrt{\log n}\right\};$$

hence this sum is

$$> \frac{\omega(n)}{2}\sqrt{\log n}\sum_{p\subset I_1}\frac{1}{p} > \frac{\omega(n)}{2}\sqrt{\log n}\cdot\frac{\omega(n)}{3}\cdot\frac{1}{\sqrt{\log n}} = \frac{\omega(n)^2}{6}.$$

Hence with exception of at most

$$\frac{6}{\omega(n)!^2}n!$$

P's the other ones are such that $\mathbf{O}(P)$ is divisible by a prime p in I. Q.e.d.

Appendix

We sketch the proof of Lemma II. We have for $n \geqq 10$ obviously

$$\frac{1}{n!}g(n,p,q) = \sum_{\nu=0}^{pq-1}\frac{1}{2\pi i}\int_{(D_\nu)}G_{pq}(z)z^{-n-1}\,dz, \tag{1}$$

where D_ν means the following path of integration. We cut off the plane along the segment

$$z = re^{\frac{2\pi i\nu}{pq}}, \qquad r \geqq 1$$

then D_ν comes from infinity along the ray

$$\arg z = \frac{2\pi\nu}{pq}-0$$

encircles the point $z=e^{\frac{2\pi iv}{pq}}$ in negative sense with a "small" circle and then goes to infinity along the ray

$$\arg z = \frac{2\pi v}{pq} + 0.$$

The contribution of the "small" circles goes obviously to 0 and hence

$$\frac{1}{n!}\, g(n,p,q) = \sum_{v=0}^{pq-1} I_v, \tag{2}$$

where

$$I_v = \lim_{\varepsilon \to +0} \left\{ e^{-\frac{2\pi v n i}{pq}} \int_1^{\infty} \frac{G_{pq}\left(r \exp i\left(\frac{2\pi v}{pq}+\varepsilon\right)\right) - G_{pq}\left(r \exp i\left(\frac{2\pi v}{pq}-\varepsilon\right)\right)}{r^{n+1}}\, dr \right\}. \tag{3}$$

We consider first the I_v's with

$$1 \leqq v \leqq pq-1.$$

We have (roughly)

$$|G_{pq}(z)| < \frac{10pq}{(r^{pq}-1)^{\frac{1}{pq}}} < \frac{10pq}{(r-1)^{\frac{1}{pq}}}$$

and hence

$$\sum_{v=1}^{pq-1} |I_v| < 10(pq)^2 \int_1^{\infty} \frac{dr}{r^{n+1}(r-1)^{\frac{1}{pq}}} = 10(pq)^2 \int_0^1 t^{-\frac{1}{pq}} (1-t)^{n-1+\frac{1}{pq}}\, dt$$

on putting $r = \frac{1}{1-t}$. Using the well-known formula

$$\int_0^1 t^{\alpha}(1-t)^{\beta}\, dt = \frac{\Gamma(\alpha+1)\Gamma(\beta+1)}{\Gamma(\alpha+\beta+2)} \qquad (\alpha > -1,\ \beta > -1) \tag{4}$$

we get for $n > n_0$

$$\sum_{v=1}^{pq-1} |I_v| < 20(pq)^2 \frac{\Gamma\left(n+\frac{1}{pq}\right)}{\Gamma(n+1)} < (pq)^3 n^{\frac{1}{pq}-1}$$

and hence

$$\left| g(n,p,q)\frac{1}{n!} - I_0 \right| < (pq)^3 n^{\frac{1}{pq}-1}. \tag{5}$$

As to I_0, putting

$$\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = \lambda$$

and

$$g(r) = \left(\frac{r^p-1}{r-1}\right)^{\frac{1}{p}} \left(\frac{r^q-1}{r-1}\right)^{\frac{1}{q}} \left(\frac{r-1}{r^{pq}-1}\right)^{\frac{1}{pq}}$$

we get

$$I_0 = \frac{\sin \pi\lambda}{\pi} \int_1^\infty \frac{g(r)\,dr}{r^{n+1}(r-1)^\lambda}.$$

The contribution of $r > 1 + 100\,\frac{\log n}{n}$ is $O(n^{-50})$ quite roughly; replacing on the remaining interval $g(r)$ by

$$\frac{p^{\frac{1}{p}} q^{\frac{1}{q}}}{(pq)^{\frac{1}{pq}}}$$

gives an error of $O(n^{-1}\log^2 n)$. Completing again the integration range to $(1, \infty)$ we get

$$(6) \qquad I_0 = \frac{\sin \pi\lambda}{\pi} \frac{p^{\frac{1}{p}} q^{\frac{1}{q}}}{(pq)^{\frac{1}{pq}}} \{1 + O(n^{-1}\log^2 n)\} \int_1^\infty \frac{dr}{r^{n+1}(r-1)^\lambda} + O(n^{-50}).$$

Substituting again r by $\frac{1}{1-t}$ and applying (4) we get for the main term in (6)

$$\{1 + O(n^{-1}\log^2 n)\} \frac{p^{\frac{1}{p}} q^{\frac{1}{q}}}{(pq)^{\frac{1}{pq}}} \cdot \frac{\sin \pi\lambda \cdot \Gamma(1-\lambda)\Gamma(n+\lambda)}{\pi\Gamma(n+1)} =$$

$$= \{1 + O(n^{-1}\log^2 n)\} \frac{p^{\frac{1}{p}} q^{\frac{1}{q}}}{(pq)^{\frac{1}{pq}}} \frac{\Gamma(n+\lambda)}{\Gamma(\lambda)\Gamma(n+1)} = \{1 + O(n^{-1}\log^2 n)\} \frac{p^{\frac{1}{p}} q^{\frac{1}{q}}}{(pq)^{\frac{1}{pq}}} \cdot$$

$$\cdot \frac{n^{-\frac{1}{p}-\frac{1}{q}+\frac{1}{pq}}}{\Gamma(\lambda)}.$$

But in our case

$$\frac{p^{\frac{1}{p}} q^{\frac{1}{q}}}{(pq)^{\frac{1}{pq}}} \cdot \frac{n^{\frac{1}{pq}}}{\Gamma(\lambda)} = 1 + O(\log^{-\frac{1}{2}} n)$$

the proof of Lemma II is complete.

(Received 15 January 1966)