Reprinted from JOURNAL OF NUMBER THEORY
Vol. 31, No. 3, March 1989
Printed in Belgium

Proof of a Conjecture of Erdös and Turán*

ERIC SCHMUTZ[†]

University of Pennsylvania, Philadelphia, Pennsylvania

Communicated by H. Zassenhaus

Received August 7, 1987

We prove a conjecture of Erdös and Turán concerning the average order of the elements in the symmetric group S_n. If μ_n is the expected order of a random permutation, then $\log \mu_n = O(\sqrt{n/\log n})$. © 1989 Academic Press, Inc.

1. INTRODUCTION

For $\sigma \in S_n$ let $\mathrm{N}(\sigma)$ be the order of σ as a group element. The distribution of N was studied by Erdös and Turán in a beautiful series of papes on "statistical group theory." On corollary to their results is that $\mathrm{N}(\sigma) < e^{\log^2 n}$ for almost every σ. On the other hand, there is an old theorem of Landau asserting that $\max_{\sigma \in S_n} \mathrm{N}(\sigma) = e^{\sqrt{n \log n(1+o(1))}}$. Noting the large difference between $e^{\sqrt{n \log n}}$ and $e^{\log^2 n}$, Erdös and Turán asked for the *average* order [1]. Let $\mu_n \stackrel{\text{def}}{=} (1/n!) \sum_{\sigma \in S_n} \mathrm{N}(\sigma)$ be the arithmetic mean or expectation of N. Apparently Turán had a proof that $\log \mu_n = O(\sqrt{n/\log n})$. Unfortunately, when Turán died the proof died with him. As of 1986, Erdös could prove that $\log \mu_n < c\sqrt{n}$. He felt that this could probably be tightened enough to prove that $\log \mu_n = o(\sqrt{n})$. In this paper we resurrect Turán's theorem; we prove that $\log \mu_n = O(\sqrt{n/\log n})$.

For a lower bound, Nicolas observed that μ_n is greater than the number of partitions of n into parts that are distinct primes. Thus $\log \mu_n > (2\pi/\sqrt{6})\sqrt{n/\log n}(1+o(1))$. Perhaps this is sharp. Most of the contribution to μ_n comes from permutations of large order. If σ is a permutation of large order, then the cycle lengths of σ add up to n and have a large least common multiple. This can only happen if the cycle lengths are "close" to being a large set of distinct primes. This is vague and imprecise, but it may help to motivate our slow and non-intuitive proof. There is of course a

* This work is supported in part by the U.S. Office of Naval Research and in part by a Sloan Foundation dissertion fellowship. It forms part of the author's doctoral thesis, written under the direction of H. S. Wilf at the University of Pennsylvania.

[†] Current address: Drexel University, Philadelphia, Pennsylvania 19104.

0022-314X/89 $3.00

competing influence. If the order m is too large, then we expect that there will not be enough permutations of order m. In other words, if m is too near the maximum order, then $m * \text{Prob}(\mathbf{N} = m)$ will not contribute significantly to μ_n. Improved estimates for μ_n will probably require a delicate balancing of these two effects.

2. Preliminaries

We shall use three theorems about partitions in the course of the proof. The statements of these theorems are given here for the convenience of the reader. We then describe a method of decomposing partitions that will be needed in the proof.

Let a_n be the number of (unordered) partitions of n whose parts are "pairwise" relatively prime. In other words, count $\{\lambda : n = \lambda_1 + \lambda_2 + \cdots\}$ iff $\gcd(\lambda_i, \lambda_j) = 1$ for all $i \neq j$. The following theorem is proved in [7]:

Theorem 1. $\log a_n \sim (2\pi/\sqrt{6})\sqrt{n/\log n}$.

Next let W_n be the set of all partitions of n into parts that are 1's or powers of distinct primes. In the language of generating functions, $\# W_n$ is the coefficient of x^n in $(1/1-x)\prod_{\text{primes } p}(1 + x^p + x^{p^2} + \cdots)$. Erdös and Turán proved the following result in [1]:

Theorem 2. *There is a bijection between W_n and the set of all orders of elements in S_n. In other words, $\# W_n = \# \{m \mid m = N(\sigma)$ for some $\sigma \in S_n\}$. Moreover* $\log(\# W_n) \sim (2\pi/\sqrt{6})\sqrt{n/\log n}$.

We shall also need a theorem of Lehmer [4] about reciprocally weighted partitions. If $\omega_1, \omega_2, \ldots$ denote the parts of a partition ω then we have:

Theorem 3. $\sum_{\omega \vdash n} (1/\omega_1\omega_2\omega_3 \ldots) = O(n)$.

Think of partitions as multisets. For example, $\lambda = \{36, 12, 9^{(2)}, 2, 1^{(2)}\}$ is the partition of 70 with two parts of size 1, one part of size 2, etc. For each partition λ, we are going to choose partitions π and ω such that $\lambda = \pi \cup \omega$. In general, this can be done in many ways, but we are going to choose a particular decomposition that has certain useful properties. Suppose λ is a partition. Let m be the least common multiple of the parts of λ, and let $p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be the prime factorization of m ($p_i < p_j$ for $i < j$). Define $\pi = \{\pi_1, \pi_2, \ldots\}$ as follows:

Let π_1 be the smallest part of λ that is divisible by $p_1^{e_1}$. Now suppose that $\pi_1, \pi_2, \ldots, \pi_t$ have been chosen. If each $p_i^{e_i}$ divides some π_j, then stop. Otherwise, let $k := \min\{i \mid p_i^{e_i}$ divides none of $\pi_1, \pi_2, \ldots, \pi_t\}$, and let π_{t+1} be the smallest part of λ that is divisible by $p_k^{e_k}$. This procedure stops for some t, and we set $\pi := \{\pi_1, \pi_2, ..., \pi_t\}$. Define a function Θ by $\Theta(\lambda) = \pi$.

Now, given λ, set $\omega = \lambda - \Theta(\lambda) = \lambda - \pi$. (It is possible that ω will be the empty partition.) Then of course $\lambda = \pi \cup \omega = \Theta(\lambda) \cup \pi$. Our decompositions have the following two properties:

(1) The least common multiple of the parts of π is equal to the least common multiple of the parts of λ.

(2) If $\lambda = \pi \cup \omega$ and $\lambda' = \pi' \cup \omega'$, then $\lambda = \lambda'$ iff $\pi = \pi'$ and $\omega = \omega'$.

One can think of π as a kind of minimal generating set.

EXAMPLE 1. Let $\lambda = \{36, 12, 9^{(2)}, 2, 1^{(2)}\}$. Then $m = 36 = 2^2 3^2$, and therefore $\pi_1 = 12$ and $\pi_2 = 9$. Hence $\Theta(\lambda) = \pi = \{12, 9\}$.

EXAMPLE 2. Let $\lambda' = \{12, 9, 1^{(49)}\}$. Then $\Theta(\lambda') = \pi' = \{12, 9\}$. These examples illustrate the fact that Θ is not injective; $\Theta(\lambda) = \Theta(\lambda')$, even though $\lambda \neq \lambda'$.

There is one subtle point about the generating "sub-partitions" π. It is not necessarily true that $\pi_1 \geqslant \pi_2 \geqslant \cdots \geqslant \pi_t$. Nevertheless, there is a canonical ordering of the parts, namely the order in which they are chosen. It is perhaps not even obvious that this order is well defined. More precisely, suppose that $\pi = \{\pi_1, \pi_2, ..., \pi_t\} = \Theta(\lambda)$, and suppose that $\pi' = \{\pi'_1, \pi'_2, ..., \pi'_t\} = \Theta(\lambda')$. We shall prove that π and π' are equal as multisets (unordered partitions) if and only if they are equal as sequences (ordered partitions). Let $m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be the least common multiple of the parts of π (and therefore also of λ). If $\pi = \pi'$ as multisets, then the least common multiple of the parts of π' (and therefore λ') is also m. We shall prove by induction on h that $\pi_h = \pi'_h$ for all h. By definition π_1 is the smallest part of λ that is divisible by $p_1^{e_1}$. Since $\pi_1 \in \pi \subseteq \lambda$, certainly π_1 is also the smallest part of π that is divisible by $p_1^{e_1}$. By the same argument, π'_1 is the smallest part of π' that is divisible by $p_1^{e_1}$. Since $\pi = \pi'$ as multisets, it follows that $\pi_1 = \pi'_1$. Now suppose that $\pi_i = \pi'_i$ for $i = 1, ..., h$. We must show that $\pi_{h+1} = \pi'_{h+1}$. Let $k = \min\{i \mid p_i^{e_i}$ divides none of $\pi_1, ..., \pi_h\} = \min\{i \mid p_i^{e_i}$ divides none of $\pi'_1, ..., \pi'_h\}$. Then $\pi_{h+1} =$ the smallest part of λ that is divisible by $p_k^{e_k} =$ the smallest part of π that is divisible by $p_k^{e_k} =$ the smallest part of π' that is divisible by $p_k^{e_k} =$ the smallest part of λ' that is divisible by $p_k^{e_k} = \pi'_{h+1}$.

This is a convenient place to define a certain function α, that will play an important role later. Suppose $\pi = \{\pi_1, \pi_2, ...\}$ is in the image of Θ, and suppose $m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ is the least common multiple of the parts of π. Then define

$$\alpha(i, j) = \alpha(i, j, \pi) := \begin{cases} e_j, & \text{if } i = \min\{k \mid p_j^{e_j} \text{ divides } \pi_k\} \\ 0, & \text{else.} \end{cases}$$

For future reference, we make the following simple observation: for each j, $\sum_i \alpha(i, j) = e_j$.

3. A New Upper Bound

With these results in hand, we can prove our main result.

THEOREM 4. $\log \mu_n = O(\sqrt{n/\log n})$.

Proof. Clearly the average order μ_n satisfies

$$\begin{aligned}\mu_n &= \sum_m m * \text{Prob}(\mathbf{N} = m)\\ &< \#\{m \mid m = \mathbf{N}(\sigma) \text{ for some } \sigma\} \cdot \max_m(m * \text{Prob}(\mathbf{N} = m))\\ &= \# W_n \cdot \max_m(m * \text{Prob}(\mathbf{N} = m)).\end{aligned}$$

By Theorem 2, $\# W_n$ is small enough. We shall therefore seek a uniform upper bound for $m * \text{Prob}(\mathbf{N} = m)$. If $\sigma \in S_n$ has order m, then the cycle lengths of σ form a partition of n with the following property: the least common multiple of the parts is m. It is a well-known fact that if $\lambda \vdash n$ has c_i parts of size i $(i = 1 \cdots n)$, then the number of permutations giving rise to λ in this way is

$$\frac{n!}{c_1!\, c_2! \cdots c_n!\, 1^{c_1} 2^{c_2} \cdots n^{c_n}}.$$

Let $\Delta_m := \{\lambda \vdash n \mid \text{the least common multiple of the parts of } \lambda \text{ is } m\}$. Then

$$\begin{aligned}m * \text{Prob}(\mathbf{N} = m) &= m \cdot \frac{1}{n!} \sum_{\lambda \in \Delta_m} \frac{n!}{c_1! \cdots c_n!\, 2^{c_2} \cdots n^{c_n}}\\ &= \sum_{\lambda \in \Delta_m} \frac{m}{c_1! \cdots c_n!\, 2^{c_2} \cdots n^{c_n}} < \sum_{\lambda \in \Delta_m} \frac{m}{2^{c_2} 3^{c_3} \cdots n^{c_n}}.\end{aligned}$$

Next observe that $2^{c_2} 3^{c_3} \cdots n^{c_n} = \lambda_1 \lambda_2 \lambda_3 \cdots$. (Recall that $c_i = c_i(\lambda) =$ the number of parts of size i in λ.) We therefore have

$$\sum_{\lambda \in \Delta_m} \frac{m}{2^{c_2} 3^{c_3} \cdots n^{c_n}} = \sum_{\lambda \in \Delta_m} \frac{m}{\lambda_1 \lambda_2 \lambda_3 \cdots}.$$

If $\lambda = \pi \cup \omega = \Theta(\lambda) \cup \omega$, then $(m/\lambda_1 \lambda_2 \cdots) = (m/\pi_1 \pi_2 \cdots \omega_1 \omega_2 \cdots)$. (Define $\prod_i \omega_i$ to be 1 if ω is empty). We therefore have

$$\sum_{\lambda \in \Delta_m} \frac{m}{\lambda_1 \lambda_2 \cdots}$$

$$= \sum_{\pi \in \Theta(\Delta_m)} \sum_{\{\omega \mid (\pi \cup \omega) \in \Delta_m \,\&\, \Theta(\pi \cup \omega) = \pi\}} \frac{m}{\pi_1 \pi_2 \cdots \omega_1 \omega_2 \cdots}$$

$$= \sum_{\pi \in \Theta(\Delta_m)} \frac{m}{\pi_1 \pi_2 \cdots} \sum_{\{\omega \mid (\pi \cup \omega) \in \Delta_m \,\&\, \Theta(\pi \cup \omega) = \pi\}} \frac{1}{\omega_1 \omega_2 \cdots}.$$

(For the next step, note that if $\pi \cup \omega$ is a partition of n, then ω is a partition of $(n - \sum_i \pi_i)$. Thus the inner sum above is a sum over partitions ω of $(n - \sum \pi_i)$ that satisfy certain conditions. The inequality below is obtained by removing all conditions on the partitions ω)

$$< \sum_{\pi \in \Theta(\Delta_m)} \frac{m}{\pi_1 \pi_2 \cdots} \sum_{\omega \vdash (n - \sum \pi_i)} \frac{1}{\omega_1 \omega_2 \cdots}.$$

The inner sum is clearly $O(n)$, by Theorem 3. Since a factor of n is negligible, we need only estimate

$$\sum_{\pi \in \Theta(\Delta_m)} \frac{m}{\pi_1 \pi_2 \cdots}.$$

There is obviously a lot of cancellation between the numerator and denominator in each term of this sum. To exploit this fact fully, we must factor the π_j's. For $i = 1, \ldots, t$, let

$$d_i = \prod_{j=1}^{s} p_j^{\alpha(i,j)}.$$

(We defined $\alpha(i, j)$ above.) The d_i's have deliberately been chosen in such a way that their product is m; and so that d_i divides π_i for each i (We shall discuss this further later.) For $i = 1, \ldots, t$, let $d_i' = \pi_i / d_i$. Then $\pi_1 = d_1 d_1'$, $\pi_2 = d_2 d_2'$, ..., $\pi_t = d^t d_t'$.

Example. In Examples 1 and 2, we had $\pi = \{12, 9\}$. We therefore get

$$d_1 = 4, \qquad d_1' = 3$$

$$d_2 = 9, \qquad d_2' = 1$$

$$d_1 d_2 = 36 = \mathrm{lcm}(12, 9) = \mathrm{lcm}(36, 12, 9, 2, 1).$$

We now make several simple but important observations:

Observation (1). $\prod_{i=1}^{t} d_i = m$.

Recall that, for each j, $\sum_i \alpha(i, j) = e_j$. Hence $\prod_i d_i = \prod_i \prod_j p_j^{\alpha(i,j)} = \prod_j \prod_i p_j^{\alpha(i,j)} = \prod_j p_j^{e_j} = m$.

Oservation (2). $t \leqslant s$.

Clear from the definitions of t and s.

Observation (3). $\gcd(d_i, d_j) = 1$ for $i \neq j$.

Each prime power $p_j^{e_j}$ divides exactly one of the d_i's, and the d_i's have no other divisors outside the set $\{p_1^{e_1}, p_2^{e_2}, ..., p_s^{e_s}\}$.

Observation (4). Let $k(i) := \min\{h \mid p_h^{e_h} \text{ divides } d_i\}$. Then for $i < j$, $k(i) < k(j)$.

Assume $i < j$. Let $k := \min\{h \mid \text{for } l < i,\ p_h^{e_h} \text{ does not divide } \pi_l\}$. By definition, π_i is the smallest part of λ that is divisible by $p_k^{e_k}$, and therefore $p_k^{e_k}$ divides d_i. Hence $k(i) \leqslant k$. On the other hand, $p_{k(j)}^{e_{k(j)}}$ divides d_j. Therefore (by the definition of d_j), for $l < j$, $p_{k(j)}^{e_{k(j)}}$ does not divide λ_l. Since $i < j$, this certainly implies that, for $l < i$, $p_{k(j)}^{e_{k(j)}}$ does ot divide λ_l. Thus $k \leqslant k(j) \Rightarrow k(i) \leqslant k(j)$. By Observation 3, $k(i) \neq k(j)$, which in turn implies that $k(i) < k(j)$.

Observation (5). $d_i \geqslant q_i$ ($q_i = i$th prime, i.e., $q_1 = 2$, $q_2 = 3$, etc.).

Certainly $d_i \geqslant p_{k(i)}^{e_{k(i)}}$. On the other hand, $k(i) \geqslant i$ (by Observation 4), and consequently $p_{k(i)}^{e_{k(i)}} \geqslant p_i^{e_{k(i)}} \geqslant p_i \geqslant q_i$.

Observation (6). $\sum_{i=1}^{t} d_i d_i' \leqslant n$. $\sum_{i=1}^{t} d_i d_i' = \sum_{i=1}^{t} \pi_i \leqslant \sum_j \lambda_j = n$.

Now for $\pi \in \Theta(\Delta_m)$, define $\Psi(\pi)$ to be the sequence $\langle d_i \rangle_{i=1}^{t}$. (We shall also use the notation $\vec{d}$; i.e., $\Psi(\pi) = \vec{d} = \langle d_i \rangle$). Then, returning to the proof, we have

$$\sum_{\pi \in \Theta(\Delta_m)} \frac{m}{\pi_1 \pi_2 \cdots}$$

$$= \sum_{\vec{d} \in \Psi(\Theta(\Delta_m))} \sum_{\{\langle d_i' \rangle \mid \Psi(\{(d_1 d_1'), (d_2 d_2'), ...\}) = \vec{d}\}} \frac{m}{(d_1 d_1')(d_2 d_2') \cdots}$$

(recall that $d_i d_i' = \pi_i$; the double summation is obtained by grouping together terms that correspond to the same $\vec{d}$)

$$= \sum_{\vec{d} \in \Psi(\Theta(\Delta_m))} \sum_{\{\langle d_i' \rangle \mid \Psi(\{(d_1 d_1'), (d_2 d_2'), ...\}) = \vec{d}\}} \frac{1}{d_1' d_2' \cdots}. \tag{1}$$

(Here we have used Observation 1 to cancel the m with the d_i's.) Now by Observations 5 and 6, we have

$$n \geqslant \sum_{i=1}^{t} d_i d_i' \geqslant \sum_{i=1}^{t} q_i d_i'.$$

Thus the inner sum of the right side of Eq. 1 is an sum over certain sequences $\langle d_i' \rangle$ for which $2d_1' + 3d_2' + 5d_3' + \cdots + q_t d_t' \leqslant n$. It is therefore less than the quantity obtained by summing over *all* sequences $\langle j_i \rangle_{i=1}^{t}$ of t positive integers for which $2j_1 + 3j_2 + 5j_3 + \cdots + q_t j_t \leqslant n$. In other words, the right side of Eq. (1) is less than or equal to

$$\sum_{\vec{d} \in \Psi(\Theta(\Delta_m))} \sum_{\{\langle j_i \rangle_{i=1}^{t} \mid 2j_1 + 3j_2 + 5j_3 + \cdots + q_t j_t \leqslant n\}} \frac{1}{j_1 j_2 \cdots}.$$

The inner sum depends on $\vec{d}$ in the following way: t is the length or number of terms in the sequence $\vec{d} = \langle d_i \rangle_{i=1}^{t}$. In general, $\Psi(\Theta(\Delta_m))$ contains sequences of many different lengths. But by Observation 2, none of them have length greater than s. Hence, the last expression is less than or equal to

$$\sum_{\vec{d} \in \Psi(\Theta(\Delta_m))} \max_{t^* \leqslant s} \left(\sum_{\{\langle j_i \rangle_{i=1}^{t^*} \mid 2j_1 + 3j_2 + 5j_3 \cdots + q_{t^*} j_{t^*} \leqslant n\}} \frac{1}{j_1 j_2 \cdots} \right).$$

This in turn is equal to

$$\max_{t^* \leqslant s} \left(\sum_{\{\langle j_i \rangle_{i=1}^{t^*} \mid 2j_1 + 3j_2 + 5j_3 \cdots + q_{t^*} j_{t^*} \leqslant n\}} \frac{1}{j_1 j_2 \cdots} \right) \sum_{\vec{d} \in \Psi(\Theta(\Delta_m))} 1.$$

By Observation 3, each $\vec{d}$ is an ordered partition of some $n' \leqslant n$ into parts that are pairwise relatively prime. The order is uniquely determined (Observation 4), which implies that

$$\sum_{\vec{d} \in \Psi(\Theta(\Delta_m))} 1 \leqslant \sum_{k=1}^{n} a_k.$$

(Recall a_n is the number of partitions of n into parts that are pairwise relatively prime.) It is easy to see that $\langle a_n \rangle$ is increasing (again by padding with ones). We therefore have $\sum_{k=1}^{n} a_k \leqslant n a_n$. Now, by Theorem 1, $n a_n = e^{O(\sqrt{n/\log n})}$. All that remains is to estimate

$$\max_{t \leqslant s} \left(\sum_{\{\langle j_i \rangle_{i=1}^{t} \mid 2j_1 + 3j_2 + 5j_3 + \cdots q_t j_t \leqslant n\}} \frac{1}{j_1 j_2 \cdots} \right).$$

Instead of quoting a theorem, we prefer to give a novel proof.

First we shall bound s. The following lemma is implicit in Landau [3]:

LEMMA 1 (Landau). $s < c\sqrt{n/\log n}$.

Proof. If $m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ is the order of $\sigma \in S_n$, then each $p_i^{e_i}$ divides some cycle length of σ. Since $a \cdot b \geqslant a + b$ for $a, b \geqslant 2$, it follows that

$$n \geqslant \sum_{i=1}^{s} p_i^{e_i}.$$

But

$$\begin{aligned}\sum_{i=1}^{s} p_i^{e_i} &\geqslant \sum_{i=1}^{s} p_i \\ &\geqslant \sum_{i=1}^{s} q_i \geqslant cs^2 \log s \\ &\Rightarrow s < c\sqrt{\frac{n}{\log n}}.\end{aligned}$$

Now define

$$\Sigma_t := \sum_{\{\langle j_i \rangle_{i=1}^{t} \mid 2j_1 + 3j_2 + 5j_3 + \cdots + q_t j_t \leqslant n\}} \frac{1}{j_1 j_2 \cdots j_t}.$$

We must that $\Sigma_t = e^{O(\sqrt{n/\log n})}$ uniformly for $t < c\sqrt{n/\log n}$.

Let $\lg_k n$ be the k-times iterated logarithm, i.e., $\lg_k n := \log_e(\lg_{k-1} n)$. Let $\omega(n) := \max\{k \mid \lg_k n > 2\}$. We are going to partition the integers from 1 to n into $\omega(n)+1$ blocks. Let $\beta_0 := n$, and for $k = 1, ..., \omega(n)$, let $\beta_k(n) := \lceil \lg_k(n) \rceil^3$. Then for $k = 1, ..., \omega(n)$, let block k be the interval $(\beta_k, \beta_{k-1}]$. Finally, let block $(\omega(n) + 1)$ be the remaining interval, namely $[1, \lceil \log_{\omega(n)}(n) \rceil^3]$. Schematically

$$\underbrace{1, 2, ..., \lceil \log_{\omega(n)} n \rceil^3}_{\text{block } (\omega(n)+1)} \underbrace{, \ldots}_{\text{block } \omega(n)} \cdots \underbrace{\cdots \lceil \log n \rceil^3}_{\text{block } 2} \underbrace{..., n-1, n}_{\text{block } 1}.$$

Let F_1 be the set of all functions g from $[t]$ to $[\omega(n)+1]$. Then

$$\begin{aligned}&\sum_{\{\langle j_i \rangle_{i=1}^{t} \mid 2j_1 + 3j_2 + 5j_3 + \cdots + q_t j_t \leqslant n\}} \frac{1}{j_1 j_2 \cdots j_t} \\ &\quad = \sum_{g \in F_1} \sum_{\{\langle j_i \rangle_{i=1}^{t} \mid j_i \in \text{block } g(i), \ \& \ 2j_1 + 3j_2 + 5j_3 \cdots + q_t j_t \leqslant n\}} \frac{1}{j_1 j_t \cdots j_t}.\end{aligned}$$

To estimate these sums, we shall need the following lemma:

LEMMA 2. *If* $3j_1+3j_2+5j_3+\cdots+q_tj_t\leqslant n$, *then for* $k=1,2,\ldots,\omega(n)$, *we have* $\#\{i\mid j_i>\beta_k\}<c\sqrt{n/\log n\beta_k}$.

Proof. Suppose that $j_{i_1}\geqslant j_{i_2}\geqslant\cdots\geqslant j_{i_r}>\beta_k$. We must show that $r<c\sqrt{n/\log n\beta_k}$. By assumption $n\geqslant\sum_{i=1}^{t}q_ij_i$. But

$$\begin{aligned}\sum_{i=1}^{t}q_ij_i &\geqslant \sum_{l=1}^{r}q_{i_l}j_{i_l}\\ &>\beta_k\sum_{l=1}^{r}q_{i_l}\geqslant\beta_k\sum_{l=1}^{r}q_l\\ &>\beta_kcr^2\log r\Rightarrow r<c\sqrt{\frac{n}{\log n\beta_k}}.\end{aligned}$$

COROLLARY 1. *If* $2j_1+3j_2+5j_3+\cdots+q_tj_t\leqslant n$, *then* $\#\{i\mid j_i\in\text{block }k\}<c\sqrt{n/\log n\beta_k}$.

Proof. Recall block k is the interval $(\beta_k,\beta_{k-1}]$. Hence $\#\{i\mid j_i\in\text{block}\,k\}\leqslant\#\{i\mid j_i>\beta_k\}$.

COROLLARY 2. *Let* $g:[t]\to[\omega(n)+1]$, *and suppose that* $2j_1+3j_2+5j_3+\cdots+q_tj_t\leqslant n$. *If* $j_i\in\text{block }g(i)$, $\forall i$, *then* $\#g^{-1}([k])<c\sqrt{n/\log n\beta_k}$.

Proof. $\#g^{-1}([k])=$ (the number of indices i for which ($j_i\in\text{block }l$ for some $l\leqslant k$)) $=$ (the number of indices i for which $j_i>\beta_k$) $<c\sqrt{n/\log n\beta_k}$.

Let

$$F_2:=\left\{g:[t]\to[\omega(n)+1]\mid \text{for }k=1,\ldots,\omega(n),\ \#g^{-1}([k])<c\sqrt{\frac{n}{\log n\beta_k}}\right\}.$$

Now consider again the double summation that we are trying to estimate:

$$\sum_{g\in F_1}\ \sum_{\{j\mid j_i\in\text{block }g(i)\,\&\,2j_1+3j_2+5j_3+\cdots+q_tj_t\leqslant n\}}\frac{1}{j_1j_2\cdots j_t}.$$

By Corollary 2, the inner summation is empty unless $g\in F_2$. Hence this expression is *equal* to

$$\sum_{g\in F_2}\ \sum_{\{j\mid j_i\in\text{block }g(i)\,\&\,2j_1+3j_2+5j_3+\cdots+q_tj_t\leqslant n\}}\frac{1}{j_1j_2\cdots j_t}.$$

Roughly speaking, Corollary 1 tells us that the contribution to this expression from j's in block k is bounded above by $(\sum_{j \in \text{block } k} 1/j)^{c\sqrt{n/\log n\beta_k}}$. Hence

$$\sum_{g \in F_2} \sum_{\{j \mid j_i \in \text{block } g(i)\ \&\ 2j_1 + 3j_2 + 5j_3 \cdots + q_t j_t \leqslant n\}} \frac{1}{j_1 j_2 \cdots j_t}$$

$$\leqslant \sum_{g \in F_2} \prod_{k=1}^{\omega(n)} \left(\sum_{j=\beta_k}^{\beta_{k-1}} \frac{1}{j} \right)^{c\sqrt{n/\log n\beta_k}} \cdot \left(\sum_{h=1}^{\beta_{\omega(n)}} \frac{1}{h} \right)^t$$

$$= \underbrace{\left(\sum_{h=1}^{\beta_{\omega(n)}} \frac{1}{h} \right)^t}_{\text{factor 1}} \cdot \underbrace{\prod_{k=1}^{\omega(n)} \left(\sum_{j=\beta_k}^{\beta_{k-1}} \frac{1}{j} \right)^{\sqrt{n/\log n\beta_k}}}_{\text{factor 2}} \cdot \underbrace{\sum_{g \in F_2} 1}_{\text{factor 3}}.$$

We shall estimate each of these three factors seprately.

(1) For the first factor, note that $\beta_{\omega(n)} = \lceil \lg_{\omega(n)}(n) \rceil^3 \leqslant \lceil e^2 \rceil^3$, and therefore $(\sum_{h=1}^{\beta_{\omega(n)}} 1/h)$ is certainly bounded. Since $t < c\sqrt{n/\log n}$, it follows that $(\text{factor 1}) = e^{O(\sqrt{n/\log n})}$.

(2)

$$(\text{factor 2}) = \prod_{k=1}^{\omega(n)} \left(\sum_{j=\beta_k}^{\beta_{k-1}} \frac{1}{j} \right)^{c\sqrt{n/\log n\beta_k}}$$

$$< \prod_{k=1}^{\omega(n)} (\log \beta_{k-1})^{c\sqrt{n/\log n\beta_k}}$$

$$= \exp\left[\sum_{k=1}^{\omega(n)} c \sqrt{\frac{n}{\log n\beta_k}} \log\log \beta_{k-1} \right]$$

$$= \exp\left[c \sqrt{\frac{n}{\log n}} \sum_{k=1}^{\omega(n)} \frac{\log\log \beta_{k-1}}{\sqrt{\beta_k}} \right]$$

$$= \exp\left[c \sqrt{\frac{n}{\log n}} \left(\frac{\log\log n}{\lceil \log n \rceil^{3/2}} + \sum_{k=2}^{\omega(n)} \frac{\log\log(\lceil \lg_{k-1}(n) \rceil^3)}{\lceil \log_k(n) \rceil^{3/2}} \right) \right]. \quad (2)$$

Now choose $c' > 0$ so that $\log\log([x]^3)/\lceil \log x \rceil^{3/2} < c'/\log x$ for all $x > 2$. By taking $x = \lg_{k-1}(n)$, we see that the quantity in Eq. (2) is less than

$$\exp\left[c'' \sqrt{\frac{n}{\log n}} \sum_{k=1}^{\omega(n)} \frac{1}{\lg_k n} \right].$$

Claim. $\sum_{k=1}^{\omega(n)} (1/\lg_k(n)) < 1$.

To verify the claim, let $r := \lg_{\omega(n)}(n)$. Then (in reverse order)

$$\sum_{k=1}^{\omega(n)} \frac{1}{\lg_k(n)} = \frac{1}{r} + \frac{1}{e^r} + \frac{1}{e^{e^r}} + \cdots + \frac{1}{\log n}$$

$$< \frac{1}{2} + \frac{1}{e^2} + \frac{1}{e^{e^2}} + \cdots$$

$$< \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots = 1.$$

This verifies the claim, and thereby proves that (factor 2) $= e^{O(\sqrt{n/\log n})}$.

(3) To simplify notation, let $T := c\sqrt{n/\log n}$ where c is large enough so that no $\sigma \in S_n$ has more than T distinct primes dividing its order (see Lemma 1). Then

(factor 3)

$$= \# \left\{ g : [t] \to [\omega(n)+1] : \text{for } k = 1, ..., \omega(n),\ \# g^{-1}([k]) < \frac{cT}{\sqrt{\beta_k}} \right\}$$

$$\leqslant \# \left\{ g : [T] \to [\omega(n)+1] : \text{for } k = 1, ..., \omega(n),\ \# g^{-1}([k]) < \frac{cT}{\sqrt{\beta_k}} \right\}.$$

To further simplify notation, let $M_k := cT/\sqrt{\beta_k}$. A function g from $[T]$ to $[\omega(n)+1]$ can be specified in the following way: First choose $g^{-1}([\omega(n)])$. Then, from among the elements of $g^{-1}([\omega(n)])$, choose $g^{-1}([\omega(n)-1])$. Then, from among the elements of $g^{-1}([\omega(n)-1])$, choose $g^{-1}([\omega(n)-2])$, etc. Obviously 2^T is an upper bound for the number of ways that $g^{-1}([\omega(n)])$ can be chosen. Since $\# g^{-1}([\omega(n)]) < M_{\omega(n)}$, the number of ways to choose $g^{-1}([\omega(n)-1])$ from among the elements of $g^{-1}([\omega(n)])$ is bounded above by $2^{M_{\omega(n)}}$. Similarly, the number of ways that $g^{-1}([\omega(n)-2])$ can be chosen from among the elements of $g^{-1}([\omega(n)-1])$ is bounded above by $2^{M_{\omega(n)-1}}$, and so on. Combining these bounds, we get

$$\# \{ g : [T] \to [\omega(n)+1] \mid \text{for } k = 1, ..., \omega(n),\ \# g^{-1}([k]) < M_k \}$$

$$< 2^T \cdot 2^{M_{\omega(n)}} \cdot 2^{M_{\omega(n)-1}} \cdot 2^{M_{\omega(n)-2}} \cdots$$

$$= \exp\left[\log 2 \left(T + \sum_{k=1}^{\omega(n)} M_k \right) \right]$$

$$= \exp\left[O\left(\sqrt{\frac{n}{\log n}} \left(1 + \sum_{k=1}^{\omega(n)} \frac{1}{\lg_k(n)} \right) \right) \right]$$

$$= e^{O(\sqrt{n/\log n})}.$$

It is now established that $c_1\sqrt{n/\log n} < \log \mu_n < c_2\sqrt{n/\log n}$ for n sufficiently large. (In the interest of better communication, we remark that $\log \mu_n = \Theta(\sqrt{n/\log n})$ is the computer scientists' standard notation for this.) For the upper bound, one can take $c_2 = 7.7$. The constant 7.7 can be improved slightly, but our methods alone do not seem strong enough to yield an asymptotic formula. We therefore close with the following problem:

PROBLEM. *Prove or disprove that* $\log \mu_n \sim (2\pi/\sqrt{6})\sqrt{n/\log n}$.

ACKNOWLEDGMENTS

Herbert Wilf suggested this problem, and also contributed much of his time, ideas, and encouragement. I am also indebted to Andrew Odlyzko for a helpful conversation.

REFERENCES

1. P. ERDÖS AND P. TURÁN, On some problems of a statistical group theory, IV, *Acta Math. Acad. Sci. Hungar.* **19** (1968), 413–435.
2. P. ERDÖS, personal communication, 1987.
3. E. LANDAU, "Handbuch der Lehre von der Verteilung der Primzahlen," 2nd ed., Chelsea, New York, 1953.
4. D. H. LEHMER, On reciprocally weighted partitions, *Acta Arith.* **21** (1972), 379–388.
5. J. NICOLAS, Distribution statistique de l'ordere d'un elemente du groupe symmetrique, *Acta Math. Hungar.* **45** (1985), 69–84.
6. PÁLFY AND SZALAY, On a problem of P. Turán concerning Sylow subgroups, *in* "Studies in Pure Mathematics, to the memory of Paul Turán" (P. Erdös, Ed.), Birkhäuser Verlag, Basel, 1983.
7. E. SCHMUTZ, Partitions whose parts are pairwise relatively prime, *Discrete Math.*, in press.
8. R. TARJAN, Efficiency of a good but not linear set union algorithm, *J. Assoc. Comput. Mach.* **22** (1975), 215–225.
9. H. S. WILF, Three problems in combinatorial asymptotics, *J. Combin. Theory Ser. A* **35** No. 2 (1983), 199–207.

Printed by Catherine Press, Ltd., Tempelhof 41, B-8000 Brugge, Belgium