The Maximum Order of an Element of a Finite Symmetric Group

William Miller

American Mathematical Monthly, Volume 94, Issue 6 (Jun. - Jul., 1987), 497-506.

The Maximum Order of an Element of a Finite Symmetric Group

WILLIAM MILLER, LEMOYNE COLLEGE

WILLIAM MILLER: I received my doctorate in 1979 from the University of Michigan for work done under the direction of H. L. Montgomery.

Preface. The question, "How large can the order of permutation on n elements be?" is reclusive, eccentric, and charming. It is of common genealogy, the natural offspring of rudimentary concepts from group theory. Yet it shyly declines to appear in modern algebra texts except, occasionally, in the inconspicuous special case where n is small. (See, for example, [**2**], p. 322; [**5**], p. 83; [**6**], p. 158.)

An amusing quirk of the question is its penchant for disguise. It enjoys masquerading in equivalent forms, like the following one.

A deck of n cards is shuffled repeatedly, each shuffle identical to the others. What is the maximum number of shuffles that can be required to restore the deck to its original order? (Here, the term "shuffle" indicates all possible rearrangements of the deck, even those that the best stage magician could not achieve with normal techniques.)

Other known aliases are described in the introduction to [**10**]. (The works cited there are [**16**], [**18**], and [**19**].)

Idiosyncrasies aside, the question possesses a fascinating talent—the uncanny ability to weave seemingly unrelated ideas into a tightly knit and intriguingly artistic fabric. This talent is too delightful for us to leave the question in its present state of obscurity.

1. Introduction. For convenience, let us denote the maximum order of a permutation on n elements by $G(n)$. The goal of this paper is to summarize what is known about $G(n)$ and then present a proof of one of the premier results, namely, that

$$\log G(n) \sim \sqrt{n \log n}\,. \tag{1}$$

(Throughout, "log" denotes the natural logarithm; and, for functions f and g, we write $f(x) \sim g(x)$ and say "f is asymptotic to g" if $\lim_{x\to\infty} f(x)/g(x) = 1$.) For some perspective on this result, recall that the symmetric group on n elements has order $n!$, and that $\log n!$ is asymptotic to $n \cdot \log n$. In this sense, we can regard (1) as quantifying the well-known fact that a symmetric group on more than 2 elements is not cyclic.

The proof of (1) has an aesthetic quality that greatly enhances its appeal: it applies a deep, number-theoretic result to a question from group theory, yet in such

a way that a general reader can appreciate the details. The deep result from number theory is the Prime Number Theorem, which states that if $\pi(x)$ denotes the number of primes not exceeding x, then $\pi(x) \sim x/\log x$. (See [4] for a thorough history of this famous result; a proof is given in [1].)

The remainder of the paper is organized as follows. In Section 2, we review what is known about $G(n)$. Next (Section 3), we discuss some basic notions concerning $G(n)$. Beginning in Section 4, we turn to proving (1). The first step is to make a connection between $G(n)$ and the prime numbers. This connection leads us, in a natural way, to consider a function $F(n)$ that approximates $G(n)$ but is simpler to handle. We then show, in Sections 5 and 6, respectively, that $\log G(n) \sim \log F(n)$ and that $\log F(n) \sim \sqrt{n \log n}$, from which (1) is evident. (The relation $\sim$ is easily seen to be transitive.) Finally, we offer some concluding remarks in Section 7. The arguments of Sections 4 and 5 employ a variety of simple ideas. It is not until Section 6 that we must invoke the Prime Number Theorem.

2. Historical Notes. The papers dealing with $G(n)$ are quite sparse. The first significant information about $G(n)$ was apparently obtained by E. Landau (see [7] and [8], pp. 222–229), who proved (1) in 1903. Thirty-six years later, S. Shah ([15]) refined (1) by providing an estimate for $|\log G(n) - \sqrt{n \log n}|$. In 1980, M. Szalay ([17]) sharpened Shah's estimate somewhat and also gave an estimate for the maximum order of an element of a symmetric semigroup. The estimates of both Shah and Szalay contain noneffective constants. Quite recently, J. Massias ([10]) derived an explicit upper bound for $G(n)$ and determined the value of n at which $(\log G(n) - \sqrt{n \log n})$ attains its maximum.

A few years ago, M. Nathanson ([11]) offered a short, elementary proof showing that $G(n)$ grows more rapidly than any power of n, (a result that is plainly weaker than (1)).

A paper ([12]) of J. Nicolas, which appeared in 1969, exposes a number of interesting properties of $G(n)$. A particularly striking result of that paper is that there are arbitrarily long strings of consecutive integers for which $G(n)$ is stationary. In a second paper ([13]), contemporary with the first, Nicolas described a computer program for calculating $G(n)$.

That very few permutations on n elements have orders as large as $G(n)$ is one result of a 1965 paper of P. Erdös and P. Turán. (See [3].) In fact, "most" (in a sense that Erdös and Turán made precise) permutations on n elements have an order whose logarithm is about $(\log^2 n)/2$.

3. Computing $G(n)$ When n is Given. For a small value of n, it is a routine exercise to calculate $G(n)$. One merely recalls that every finite permutation can be decomposed (uniquely, up to the order in which the factors appear) as a product of disjoint cycles, and that the order of a permutation is the least common multiple of the lengths of its disjoint cycles (see [9], pp. 93–94). Then, using this, one enumerates the possible orders of a permutation on n elements. More explicitly, one considers all distinct representations of n as a sum of positive integers and, for each representation, computes the least common multiple of the integers in the represen-

tation. The largest number thus computed is $G(n)$, and the integers in any representation corresponding to $G(n)$ are the cycle lengths of a permutation on n elements having order $G(n)$. This tedious method can be streamlined, as in [13]; but calculating a particular value of $G(n)$ involves substantial trial and error.

The table below displays the values of $G(n)$ for $n < 20$ and gives the corresponding cycle structures of permutations (on n elements) with order $G(n)$.

n	$G(n)$	cycle lengths	n	$G(n)$	cycle lengths
2	2	2	11	30	1, 2, 3, 5 or 5, 6
3	3	3	12	60	3, 4, 5
4	4	4	13	60	1, 3, 4, 5
5	6	2, 3	14	84	3, 4, 7
6	6	1, 2, 3 or 6	15	105	3, 5, 7
7	12	3, 4	16	140	4, 5, 7
8	15	3, 5	17	210	2, 3, 5, 7
9	20	4, 5	18	210	1, 2, 3, 5, 7 or 5, 6, 7
10	30	2, 3, 5	19	420	3, 4, 5, 7

The unruly behavior of $G(n)$ is apparent even in this brief table.

4. The Prime Connection. Let us consider the question of whether, for a given positive integer m, there is a permutation on n elements having order m. As a specific example, we ask, "Is there a permutation on 52 elements having order 51,480?" Now the prime factorization of 51,480 is $2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13$. Therefore, any permutation with exactly five nontrivial (disjoint) cycles whose lengths are $8, 9, 5, 11, 13$ has order 51,480. Moreover, it is possible to construct such a permutation whenever there are at least $8 + 9 + 5 + 11 + 13$ $(= 46)$ distinct elements available for permuting. We see, then, that there *is* a permutation on 52 elements with order 51,480. (This means, by the way, that there are shuffles that have to be performed exactly 51,480 times to restore a standard deck of 52 cards to its original order.)

In general, if we seek a permutation of order m, then we let the prime factorization of m be $\prod_{j=1}^{s} q_j^{e_j}$. Whenever $\sum_{j=1}^{s} q_j^{e_j} \leqq n$ we form a permutation that has $s + (n - \sum_{j=1}^{s} q_j^{e_j})$ disjoint cycles, the first s of lengths $q_1^{e_1}, \ldots, q_s^{e_s}$, and the remaining ones of length 1. This permutation is a permutation on n elements (since the cycle lengths sum to n) and has order m (since the least common multiple of the cycle lengths is just their product, which is m). Hence, if $\sum_{j=1}^{s} q_j^{e_j} \leqq n$ (where $m = \prod_{j=1}^{s} q_j^{e_j}$), then there is a permutation on n elements having order m. We show in Corollary 1 below that the converse of this statement also holds.

As the preceeding discussion suggests, it is handy to have an abbreviation for the sum associated with the prime factorization of m.

DEFINITION. The function S is defined on the positive integers by $S(1) = 1$ and $S(m) = \sum_{j=1}^{s} q_j^{e_j}$ for $m > 1$, where $\prod_{j=1}^{s} q_j^{e_j}$ is the prime factorization of m.

We have described a procedure for constructing a permutation of given order m. Our procedure requires that we have at least $S(m)$ distinct elements available for

permuting. We want to know that our procedure is an efficient one, that is, that no other procedure can produce a permutation of order m by using fewer than $S(m)$ distinct elements. The next lemma assures us on this point. In reading the lemma, it is helpful (though not essential) to think of the integers $a_1, \ldots, a_k$ as being the cycle lengths of a permutation of order m.

LEMMA 1. *Let $a_1, \ldots, a_k$ be positive integers and let m be their least common multiple. Then $S(m) \leqq \sum_{i=1}^{k} a_i$.*

Proof. We argue that there are no counterexamples to the lemma. Suppose, instead, that the sequence of positive integers $a_1, \ldots, a_k$ forms a counterexample, and further suppose that the sum of $a_1, \ldots, a_k$ is minimal (among counterexamples). After making a few reductions, we shall arrive at an obvious contradiction.

We first note that all the terms of $a_1, \ldots, a_k$ are greater than 1; if not we could delete one of the terms equal to 1 to get a new sequence that would still refute the lemma, but would have a smaller sum than $a_1, \ldots, a_k$.

We next contend that each term of $a_1, \ldots, a_k$ is a (positive, integral) power of a prime. Otherwise, there would be a term, say, a_i, that could be written as a product of two relatively prime integers, say c and d, both greater than 1. Assuming d to be the larger of c and d, we would have that

$$c + d \leqq c + d(c - 1) = cd + (c - d) < cd.$$

Therefore, deleting a_i from the original sequence and inserting c and d would yield a new sequence with smaller sum, yet with the same least common multiple as $a_1, \ldots, a_k$. This would violate the minimality property of $a_1, \ldots, a_k$.

Finally, we observe that the terms of $a_1, \ldots, a_k$ must be powers of *distinct* primes. For, if two of the terms were powers of the same prime, then deleting the term with the smaller power (or deleting either term if the powers were equal) would again yield a new sequence with smaller sum, yet the same least common multiple as $a_1, \ldots, a_k$.

But if $a_1, \ldots, a_k$ are all powers of distinct primes, then the sequence is NOT a counterexample to the lemma. This is because the least common multiple of $a_1, \ldots, a_k$ (which is m) is just their product; moreover, their product is the prime factorization of m, whence $S(m)$ equals the sum of $a_1, \ldots, a_k$. Since the lemma has no counterexample of minimal sum, it must be true.

COROLLARY 1. *There is a permutation on n elements having order m if and only if $S(m) \leqq n$.*

Proof. If $S(m) \leqq n$, then the procedure outlined at the beginning of this section yields a permutation on n elements having order m. Conversely, let $a_1, \ldots, a_k$ be the cycle lengths of a permutation on n elements having order m. Then the sum of the cycle lengths is n and their least common multiple is m. Hence, $S(m) \leqq n$ by Lemma 1.

If we study the table showing values of $G(n)$ for $n < 20$, then we may well anticipate the next corollary.

COROLLARY 2. *Among the permutations on n elements having order $G(n)$, there is at least one whose nontrivial cycles have lengths that are powers of distinct primes.*

Proof. Corollary 1 gives that $S(G(n)) \leqq n$. Therefore, the construction described at the beginning of this section supplies a permutation of order $G(n)$ with the prescribed type of cycle lengths.

We comment that Corollary 2 can be strengthened considerably. It can be shown that if A is a cycle length of a permutation (on n elements) with order $G(n)$, then either A is a power of a prime not dividing any other cycle length, or else $A = 6$. Furthermore, the latter possibility is excluded for all sufficiently large n.

Our final corollary gives a convenient characterization of $G(n)$.

COROLLARY 3. *We have that* $G(n) = \max_{S(m) \leqq n} m$.

Proof. As in the previous proof, $S(G(n)) \leqq n$, so that $G(n)$ cannot exceed the maximum of the m taken over $S(m) \leqq n$. On the other hand, by Corollary 1, if $S(m) \leqq n$, then there is a permutation on n elements having order m. The definition of $G(n)$ thus implies that $m \leqq G(n)$ whenever $S(m) \leqq n$.

5. The Relationship Between $F(n)$ and $G(n)$. The foregoing section tells us that to calculate $G(n)$, we should select powers of distinct primes in such a way that their sum does not exceed n and their product is maximal (subject to the constraint on the sum). One obvious way to select prime powers satisfying the constraint is to choose $2, 3, 5, 7, 11, 13, \ldots$, continuing until the sum of the primes chosen is as large as possible without exceeding n. For instance, if $n = 52$, we select $2, 3, 5, 7, 11$, and 13. The sum of these primes is 41. We cannot include the next prime, 17, for then the sum would exceed 52. The product of the selected primes is 30,030. Let us call this product $F(52)$. It is plain that $F(52) < G(52)$ because, in our selection process, we can choose 17 instead of 7, or 4 instead of 2, or 9 instead of 3 without violating the constraint. However, since it can be checked that $G(52) = 180,180 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, we see that $F(52)$ and $G(52)$ have some common features. In particular, if we compare $G(52)$ and $F(52)$ on a logarithmic scale (a sensible one to use in dealing with products), we discover that the ratio between $\log G(52)$ and $\log F(52)$ is only about 1.2.

It is easy to use our selection process for arbitrary values of n. We select primes in increasing order until we reach a prime, call it P, such that the sum of all primes less than P is no greater than n, but such that the sum of all primes up to and including P is greater than n. Then we let $F(n)$ be the product of the primes less than P. As already announced, we discover that $\log F(n)$ is asymptotic to $\log G(n)$.

THEOREM 1. *Let P be the largest prime with the property that the sum of the primes less than P does not exceed n, and let $F(n)$ be the product of the primes less than P. Then* $\log F(n) \sim \log G(n)$.

We require two lemmas for the proof of Theorem 1. To understand the purposes of the lemmas, first recall that $F(n) \leqq G(n)$. Hence we need only find a suitable

upper bound for $G(n)$ in terms of $F(n)$. If we compare the prime factorizations of $F(52)$ and $G(52)$ given above, we notice immediately that the same primes divide both numbers. The difference is that the smaller primes appear with higher powers in $G(n)$. Thus, when $n = 52$, the product of the primes dividing $G(n)$ equals $F(n)$. In general, the product of the primes dividing $G(n)$ need not equal $F(n)$. However, Lemma 2 below guarantees that the product is never much larger than $F(n)$.

In light of Lemma 2, we see that the only way for $G(n)$ to be much larger than $F(n)$ is for the prime factorization of $G(n)$ to include primes raised to powers greater than 1. Lemma 3 limits the extent to which this can happen. In fact, Lemma 3 corroborates what is suggested by looking at $G(52)$—that only the smaller primes can appear to higher powers in the factorization of $G(n)$, and that the contribution of such higher-power primes is fairly modest.

LEMMA 2 (Shah). *Let $q_1 < \cdots < q_s$ be all the primes dividing $G(n)$, and let P and $F(n)$ be as in Theorem* 1. *Then*

$$\sum_{j=1}^{s} \log q_j < 2 + \log F(n) + \log P.$$

Proof. For future reference, we observe that $(\log x)/x$ is a decreasing function for $x \geqq 3$ (because its derivative is negative there). Hence, if $3 \leqq a \leqq b$, then $(a/\log a)(\log b) \leqq b$ and $a \leqq (b/\log b)(\log a)$. We also note that P is at least 3 unless $n = 1$, in which case the conclusion of the lemma is clearly true.

Now let $q_1, \ldots, q_{t-1}$ be the primes not exceeding P that divide $G(n)$, and let $p_1, \ldots, p_r$ be the odd primes not exceeding P that do not divide $G(n)$. Thus, the list $p_1, \ldots, p_r, q_1, \ldots, q_{t-1}$ contains every prime not exceeding P exactly once, except that 2 might be omitted. Since

$$\sum_{j=1}^{s} q_j \leqq S(G(n)) \leqq n < \sum_{p \leqq P} p,$$

we find, upon canceling common terms in the above inequality, that

$$\sum_{j=t}^{s} q_j \leqq 2 + \sum_{i=1}^{r} p_i. \tag{2}$$

Moreover, because $3 \leqq P \leqq q_j$ for $t \leqq j \leqq s$ and because $3 \leqq p_i \leqq P$ $(1 \leqq i \leqq r)$, our initial observation implies that $(P/\log P)(\log q_j) \leqq q_j$ and that $p_i \leqq (P/\log P)(\log p_i)$. From this and (2) we infer that

$$\sum_{j=t}^{s} \log q_j \leqq 2(\log P/P) + \sum_{i=1}^{r} \log p_i \leqq 2 + \sum_{i=1}^{r} \log p_i.$$

Adding the terms $\log q_j$ for $1 \leqq j \leqq t-1$ to both sides of this inequality and recalling that $p_1, \ldots, p_r, q_1, \ldots, q_{t-1}$ is just a permuted list of the primes not exceeding P (except that 2 might be omitted), we get the conclusion of the lemma.

LEMMA 3. *Let q be a prime, let e be an integer greater than* 1, *and let P be as in Theorem* 1. *If q^e divides $G(n)$, then $q^e \leqq 2P$ and $q \leqq \sqrt{2P}$.*

Proof. Since $e > 1$, the second assertion is an easy corollary of the first. To prove the first assertion, let Q be the smallest prime not dividing $G(n)$. Now the primes less than Q all divide $G(n)$; hence, their sum is at most $S(G(n))$, which is at most n. On the other hand the sum of the primes not exceeding P is greater than n. It follows that $Q \leqq P$. Therefore, it suffices to show that $q^e \leqq 2Q$.

Suppose, to the contrary, that $q^e > 2Q$, and let N be the positive integer satisfying $q < Q^N < qQ$. (Equality is impossible in the last inequality because q divides $G(n)$ while Q does not.) We put $m = (Q^N/q)G(n)$. Then $m > G(n)$ and

$$S(m) = S(G(n)) + \left(Q^N - q^e + q^{e-1}\right).$$

We claim that the last quantity in parentheses is negative. If $q < Q$, this is true because (by definition) $N = 1$ and (since q^e is supposed greater than $2Q$)

$$-q^e + q^{e-1} \leqq -q^e/2 < -(2Q)/2 = -Q.$$

If $q > Q$, it is true because (since $Q^N < qQ$ and $e > 1$),

$$Q^N - q^e + q^{e-1} < qQ - q(q-1) \leqq qQ - q(Q) = 0.$$

Hence, $S(m) < S(G(n)) \leqq n$. Since $m > G(n)$, this contradicts Corollary 3, thereby establishing the lemma.

The proof of Theorem 1 is now straightforward, save for one detail concerning the relative sizes of $F(n)$ and P.

Proof of Theorem 1. Let $\prod_{j=1}^{s} q_j^{e_j}$ be the prime factorization of $G(n)$. We view $\log G(n)$ as the sum of the terms $\log q_j^{e_j}$ and split this sum into two subsums, the first consisting of the terms for which $e_j = 1$, the second consisting of the terms for which $e_j > 1$. By Lemma 2, the first subsum is at most $2 + \log F(n) + \log P$; by Lemma 3, each term of the second subsum is at most $\log 2P$ and there are at most $\sqrt{2P}$ terms. Combining this information with the fact that $F(n) \leqq G(n)$, we deduce that

$$\log F(n) \leqq \log G(n) \leqq 2 + \log F(n) + \log P + \sqrt{2P}\,(\log 2P).$$

In the next section, we shall see that there is a positive constant c such that, for all $n > 1, \log F(n) > cP$. Accepting this fact for the present, we obtain Theorem 1 upon dividing the displayed inequality by $\log F(n)$ and letting n approach infinity. (Note that, from its definition, P clearly approaches infinity with n.)

6. The Size of $F(n)$. The goal of this section is to prove that $\log F(n)$ is asymptotic to $\sqrt{n \log n}$. As an instructive prelude to the proof, let us reason heuristically. To compute $\log F(n)$, we first determine the prime P that satisfies the double inequality

$$\sum_{p<P} p \left(= \sum_{p \leqq P-1} p\right) \leqq n < \sum_{p \leqq P} p.$$

(Here and below, p denotes a generic prime.) Then we calculate

$$\log\left(\prod_{p<P} p\right) = \sum_{p<P} \log p.$$

Suppose that we treat P as an independent variable and regard both the sum of $p(p \leqq P)$ and the sum of $\log p(p \leqq P)$ as functions of P. To emphasize this approach, let us replace P by x and put

$$A(x) = \sum_{p \leqq x} p, \qquad \theta(x) = \sum_{p \leqq x} \log p.$$

Now $A(x)$ and $\theta(x)$ are step functions whose values are tedious to determine. Let us ignore this for the present and argue as follows. Since $A(P-1) \leqq n < A(P)$ and $\log F(n) = \theta(P-1)$, we ought to get a good approximation to $\log F(n)$ by solving the equation $A(x) = n$ for x and plugging the solution into $\theta(x)$.

For this program to succeed, we must be able to approximate $A(x)$ and $\theta(x)$ by appropriate functions. Fortunately, thanks to the Prime Number Theorem, we can! The following two consequences (equivalent forms, actually) of the Prime Number Theorem are just what we need.

$$A(x) \sim x^2/(2\log x) \tag{3}$$

$$\theta(x) \sim x \tag{4}$$

According to our heuristic scheme, then, $\log F(n)$ is approximately equal to the value of x that solves the equation $x^2/(2\log x) = n$. Moreover, as is easily verified, $x = \sqrt{n \log n}$ is "almost" a solution to this equation. Thus we suspect that $\log F(n) \sim \sqrt{n \log n}$.

Before we make this plausibility argument rigorous, let us add a few comments about (3) and (4). The derivations of (3) and (4) are applications of a standard technique based on integration by parts. For those unfamiliar with this useful technique, we sketch the derivation of (4). (Recall below that $\pi(x)$ denotes the number of primes not exceeding x and that the Prime Number Theorem states that $\pi(x) \sim x/(\log x)$.)

From the definitions of $\pi(x)$, $\theta(x)$, and the Stieltjes Integral,

$$\theta(x) = \int_1^x (\log t)\, d(\pi(t)).$$

Integration by parts yields that

$$\theta(x) = \pi(x)(\log x) - \int_2^x (\pi(t))/t\, dt.$$

The last integrand is (by the Prime Number Theorem) no more than a constant multiple of $1/(\log t)$. Moreover, the integral of $1/(\log t)$ from 2 to x is bounded by a constant multiple of $x/(\log x)$, as can be seen by splitting the range of integration at $\sqrt{x}$. Hence, we obtain (4) if we divide the last equation by x, let x approach infinity, and invoke the Prime Number Theorem.

It is evident from (4) that there is a positive constant c' such that $\theta(x) > c'x$ for all $x > 2$. Furthermore, by the definitions of $F(n)$ and $\theta(x)$, we have that $\log F(n) = \theta(P-1)$. Thus, the inequality $\log F(n) > cP$, quoted in the proof of Theorem 1, follows from the Prime Number Theorem. However, this inequality also follows from much weaker statements about the distribution of primes. Relatively

simple arguments (see [**14**], p. 217ff), dating to Chebyshef, show that $\pi(x)(\log x)/x$ is bounded above and below by positive constants; and the technique illustrated in the foregoing paragraph yields corresponding upper and lower bounds for $\theta(x)$. Theorem 1 is therefore independent of deep facts about prime distribution.

To verify that $\log F(n) \sim \sqrt{n \log n}$, we first note that since $\log F(n) = \theta(P - 1)$ and since (with P regarded as a function of n) $P \sim P - 1$, (4) implies that $\log F(n) \sim P$. Thus, it suffices to show that $P \sim \sqrt{n \log n}$.

Now $A(P - 1) \leqq n < A(P)$ by the definitions of $A(x)$ and P. Since it is immediate from (3) that $A(x - 1) \sim A(x)$, we infer that

$$P^2/(2 \log P) \sim n. \tag{5}$$

If P is not asymptotic to $\sqrt{n \log n}$, then there is a positive number $\phi e \to \varepsilon$ such that, for infinitely many values of n, one of the following two inequalities holds:

$$P \leqq (1 - \varepsilon)\sqrt{n \log n} \qquad P \geqq (1 + \varepsilon)\sqrt{n \log n}. \tag{6}$$

Because $x^2/(\log x)$ is an increasing function for $x > \sqrt{e}$, the first inequality of (6) implies that

$$P^2/(2n \log P) \leqq (1 - \varepsilon)^2(\log n)/(\log n + \operatorname{loglog} n + 2 \log(1 - \varepsilon)).$$

As n approaches infinity, the right side of the last inequality approaches $(1 - \varepsilon)^2$, while (by (5)) the left side approaches 1. Hence, the first inequality of (6) cannot hold for infinitely many n. Similarly, the second cannot either; and we conclude that $P \sim \sqrt{n \log n}$. As explained above, this establishes that $\log F(n) \sim \sqrt{n \log n}$.

7. Concluding Remarks. Landau's proof of (1) contains less combinatorial analysis and more frequent use of the Prime Number Theorem than does ours. Our proof is not substantially shorter or simpler than Landau's, but it does furnish a more complete survey of the methods that have been successful in studying $G(n)$. It also illustrates how a weaker version of (1), with $\log G(n)$ bounded above and below by constant multiples of $\sqrt{n \log n}$, can be derived by using Chebyshev's estimates for $\pi(x)$ rather than the more sophisticated Prime Number Theorem.

The kind of combinatorial analysis typified by our proof of Lemma 3 can be employed very effectively to explore the prime factorization of $G(n)$. (See [**12**] for a vivid demonstration of this.) In particular, one can deduce fairly readily that if $\prod_{j=1}^{s} q_j^{e_j}$ is the prime factorization of $G(n)$ and if $q_i < q_j$, then $e_i \geqq e_j - 1$. With more work, one can show that if Q is the largest prime factor of $G(n)$, then "most" (in various senses) primes less than Q divide $G(n)$. This leads to an asymptotic estimate for the number of prime factors of $G(n)$.

The refinements of (1) mentioned in Section 2 are essentially refinements of estimates for $F(n)$. With slightly more care, Theorem 1 can be sharpened to give an estimate for $|\log G(n) - \log F(n)|$ that is commensurate with the estimate for $|\log F(n) - \sqrt{n \log n}|$ that follows from the renowned Riemann Hypothesis. Thus, Theorem 1 is adequate to handle any likely improvements in estimates for $F(n)$.

In the preface, we claimed that this paper's seminal question has a remarkable talent for linking apparently disparate ideas. Can anyone who has seen a question

about card-shuffling linked, in a natural way, to the question (Riemann Hypothesis) of where a certain analytic function has its zeroes dispute the claim?

REFERENCES

1. T. M. Apostol, Introduction to Analytic Number Theory, Springer, New York, 1966.
2. F. J. Budden, The Fascination of Groups, Cambridge University Press, London, 1972.
3. P. Erdös and P. Turán, On Some Problems of Statistical Group Theory, Z fur Wahrscheinlichkeitstheorie und verw. Gebiete, 18 (1965) 151–163.
4. L. J. Goldstein, A History of The Prime Number Theorem, this MONTHLY, 80 (1973) 599–615; correction, 1115.
5. K. H. Kim and F. W. Roush, Applied Abstract Algebra, Elliss Horwood Limited, Chichester, England, 1983.
6. A. I. Kostrikin, Introduction to Algebra, Springer, New York, 1982.
7. E. Landau, Über die Maximalordung der Permutation gegbenen Grades, Archiv der Math. und Phys., Ser. 3, 5 (1903) 92–103.
8. _____, Handbuch der Lehre von der Verteilung der Primzahlen, I, 2nd ed., Chelsea, New York, 1953.
9. S. Mac Lane and G. Birkoff, Algebra, Macmillan, New York, 1967.
10. J. Massias, Majoration explicite de l'ordre maximum d'un élément du group symétrique, Ann. Fac. Sci. Toulouse Math. (5), 6 (1984) no. 3–4, 269–281 (1985).
11. M. B. Nathanson, On the Greatest Order of an Element of the Symmetric Group, this MONTHLY, 79 (1972) 500–501.
12. N. L. Nicolas, Ordre maximal d'un élément du group des permutations et highly composite numbers, Bull. Soc. Math. France, 97 (1969) 129–191.
13. _____, Calcul de l'ordre maximum d'un élément du groupe symétrique, Rev. Francaise Informat. Recherche Operationelle, 3 (1969) 43–50.
14. I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, 4th ed., Wiley, New York, 1980.
15. S. Shah, An Inequality for the Arithmetical Function $g(x)$, J. Indian Math. Soc., 3 (1939) 316–318.
16. A. Schinzel, Reducibility of Lacunary Polynomials, III, Acta Arith., 34 (1978) 227–266.
17. M. Szalay, On the Maximal Order in S_n and S_n^*, Acta Arith., 37 (1980) 321–331.
18. L. G. Valiant and M. S. Paterson, Deterministic One Counter Automata, J. Comp. and System Sci., 10 (1975) 340–350.
19. P. M. B. Vitanyi, On the size of DOL languages, L Systems (Third Open House, Comput. Sci. Dept. Aarhus Univ., Aarhus, 1974) 78–92, 327–328, Lecture Notes in Computer Science, Vol. 15, Springer, Berlin, 1974.