The proof of (7) (using the unproved conjecture (3)) would be similar to the proof of our theorem. Instead of the decomposition (5) we would have to put $a_i = C_iD_i$ where all prime factors of C_i are less than $\log n$ and all prime factors of D_i are $\geqq \log n$. We suppress the details.

Very likely

$$\lim_{n=\infty} \log (f_t(n)) \cdot \frac{\log \log n}{\log n} \tag{8}$$

exists and perhaps it might be possible to determine its value, but it will probably not be possible to express $f_t(n)$ by a simple function of n and t (even for $t = 3$).

If t is large compared to n our method used in the proof of our theorem no longer gives a good estimation, but it is not difficult to prove by a different method the following result. Let $1 \leqq a_1 < a_2 < \cdots < a_l \leqq n$, $l = Cn$ be given, then there are always n^{ϵ_C} integers $a_{i_1}, \cdots, a_{i_r}$ which have pairwise the same common factor (ϵ_C depends only on C), but we do not investigate this question here any further.

I have not been able to decide if to every $\alpha > 0$ there is an $n_0(\alpha)$ so that if $n > n_0(\alpha)$ and

$$1 \leqq a_1 < a_2 < \cdots < a_l \leqq n, \qquad l \geqq \alpha n,$$

is any sequence of integers, then there always are three a's which have pairwise the same least common multiple. This is certainly true (and trivial) if α is close enough to 1; perhaps the whole question is trivial and I overlooked an obvious approach.

McMaster University
Hamilton, Ontario

1. P. Erdös, "Extremal problems in number theory," *Mat. Lapok*, v. 13, 1962, p. 228–255. (Hungarian)
2. P. Erdös & R. Rado, "Intersection theorems for systems of sets," *J. London Math. Soc.*, v. 35, 1960, p. 85–90.
3. P. Erdös & G. Szekeres, "Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem," *Acta Sci. Math. (Szeged)*, v. 7, 1934, p. 94–102.

On Maximal Gaps between Successive Primes

By Daniel Shanks

In personal correspondence Paul A. Carlson asked the author if he could give a rough "ball-park" estimate of where one would first find a run of a million or more consecutive composite integers. For notation let us define $p(g)$ to be the first prime that follows a gap of g or more consecutive composites. Thus $p(1) = 5$, $p(2) = p(3) = 11$, $p(4) = p(5) = 29$, $p(6) = p(7) = 97$, etc. We seek to estimate $p(10^6)$. Conversely, by $g(n)$ we mean the largest gap that occurs below any prime $p \leqq n$. We may call these values of g *maximal gaps*.

That $p(g)$ is finite for every g is well known. The famous proof by Lucas [1] merely notes that the g consecutive integers:

$$(g+1)!+2, (g+1)!+3, (g+1)!+4, \cdots, (g+1)!+g+1$$

Received April 27, 1964.

are divisible, respectively, by 2, 3, 4, etc. Therefore $p(g) \leqq$ the first prime greater than $(g + 1)(g! + 1)$.

Since, by Bertrand's "Postulate," there is always a prime between any N and $2N$ we have the rigorous, but very weak partial answer to Carlson's question:

$$p(10^6) < 2000002(1000000! + 1) = 1.65 \cdot 10^{5565715}. \tag{1}$$

More generally, from Stirling's formula, we would have, for large g:

$$\log p(g) < g \log g. \tag{2}$$

A more sophisticated proof that $p(g)$ is always finite, cf. [2], utilizes the Prime Number Theorem. Assume, on the contrary, that all gaps are less than g. Then in every g consecutive integers there is at least one prime. Therefore, if $\pi(p)$ is the number of primes $\leqq p$, we have

$$\pi(p) > \frac{p}{g}.$$

But this contradicts the Prime Number Theorem:

$$\pi(p) \sim \frac{p}{\log p}$$

since $\log p \to \infty$.

In order to use such ideas to obtain a bound on $p(g)$, however, the Prime Number Theorem as given above does not suffice, since bounds are needed for the error, $\pi(p) - p/\log p$. Particularly neat bounds have been obtained recently by Rosser and Schoenfeld [3]. They give

$$\frac{p}{\log p - \frac{1}{2}} < \pi(p) < \frac{p}{\log p - \frac{3}{2}} \qquad (p \geqq 67).$$

Thus the *average* difference between successive primes up to p, which is given by $p/\pi(p)$, is also bounded:

$$\log p - \tfrac{3}{2} < \frac{p}{\pi(p)} < \log p - \tfrac{1}{2} \qquad (p \geqq 67).$$

Since a maximal difference $g + 1$ must exceed the average difference we therefore have

$$\log p(g) < g + \tfrac{5}{2} \qquad (p \geqq 67). \tag{3}$$

In particular, we have

$$p(10^6) < 3.70 \cdot 10^{434295}. \tag{4}$$

Here, again, we may declare our dissatisfaction with these bounds. While they are improved somewhat over (2) and (1), the right side of (3) is surely of too high an order.* Correspondingly, the right side of (4) is surely a gross over-estimate. It is not in the right "ball park," and thus does not satisfactorily answer Carlson's

* Utilizing difficult analysis many authors have obtained slightly better bounds. As is usual in prime number theory these hard-to-come-by estimates are disappointingly weak in comparison with what are conjectured to be the true results. See [10] for a survey of these investigations.

question. A heuristic probability argument suggests instead the conjecture:

$$\log p(g) \sim \sqrt{g}, \tag{5}$$

but to obtain this result we must forego an exact treatment, and proceed as follows.

Consider each interval of length g contained in a much larger interval from 1 to N. What is the expected number, call it $E(N, g)$, of these g-length intervals such that all g numbers therein are composite? By the Prime Number Theorem:

$$\pi(N) \sim \int_2^N \frac{dx}{\log x},$$

the probability that x is composite is $(1 - 1/\log x)$. For an interval of g numbers surrounding x, with $g \ll x$, the probability that all g numbers are composite is $(1 - 1/\log x)^g$. Thus we estimate

$$E(N, g) = \int_g^N \left(1 - \frac{1}{\log x}\right)^g dx.$$

Let $u = \log x$. Then

$$E(N, g) = \int_{\log g}^{\log N} \left(1 - \frac{1}{u}\right)^g e^u \, du.$$

Since

$$\log\left(1 - \frac{1}{u}\right) = -\frac{1}{u} - \frac{1}{2u^2} + O(u^{-3}).$$

we have

$$E(N, g) = \int_{\log g}^{\log N} e^{u - g/u - g/2u^2 + gO(u^{-3})} \, du.$$

Now let $u = \sqrt{g} + s$ and

$$\log N = \sqrt{g} + A.$$

Thus

$$E(N, g) = \int_{\log g - \sqrt{g}}^{A} e^{2s - 1/2 + O(1/\sqrt{g})} \, ds.$$

If g is large and $A = \frac{1}{4}$ we have

$$E(N, g) \approx \tfrac{1}{2},$$

while if g is large and $A = \frac{1}{4} + \log 2/2 = 0.59657$, we have

$$E(N, g) \approx 1.$$

If A is increased beyond 0.59657, $E(N, g)$ rises rapidly, while if A is diminished below 0.25, $E(N, g)$ falls rapidly. Because of this rapid variation with A we therefore expect $\log p(g)$ to be in the neighborhood of $\sqrt{g} + 0.6$. It follows that $\log p(g)/\sqrt{g}$ should approach 1 as $g \to \infty$. But this is the conjectured relation (5).

TABLE 1
Maximal Gaps

g	$p(g)$	$\log p(g)/\sqrt{g}$
1	5	1.609
3	11	1.384
5	29	1.506
7	97	1.729
13	127	1.344
17	541	1.526
19	907	1.562
21	1151	1.538
33	1361	1.256
35	9587	1.550
43	15727	1.474
51	19661	1.384
71	31469	1.229
85	156007	1.297
95	360749	1.313
111	370373	1.217
113	492227	1.233
117	1349651	1.305
131	1357333	1.234
147	2010881	1.197
153	4652507	1.241
179	17051887	1.245
209	20831533	1.166
219	47326913	1.194

Professor Paul T. Bateman has kindly informed us that H. Cramér long ago gave a similar conjecture. But Cramér's formulation is somewhat weaker; he does not assert asymptotic equality. He writes [4, p. 27]:

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} = 1 \tag{5a}$$

where p_n is the nth prime. This implies that some subsequence of $\log p(g)$ is asymptotic to $\sqrt{g}$, but leaves it open whether other subsequences may not behave differently. It is the stronger assertion (5) that we wish to utilize here.

Empirically, the exact facts are known out to $g = 209$ thanks to an often-quoted but still not published study of D. H. Lehmer [5] concerning the distribution of primes out to $37 \cdot 10^6$. Previously, less complete tables were given by Western [6] and by Glaisher [7], and subsequently a larger gap of $g = 219$ was included in a table of Appel and Rosser [8]. There is no gap >219 up to 10^8. From these results (slightly reinterpreted) we have given in Table 1 a list of maximal gaps up to $g = 219$. In the last column we list the quantities $\log p(g)/\sqrt{g}$, and these are plotted versus $\sqrt{g}$ in Fig. 1. The agreement with the foregoing prediction is satisfactory; aside from the expected fluctuations the behavior of the graph is consistent with the expected slow convergence to unity.

Allowing a generous safety factor one can therefore estimate, with considerable confidence, that

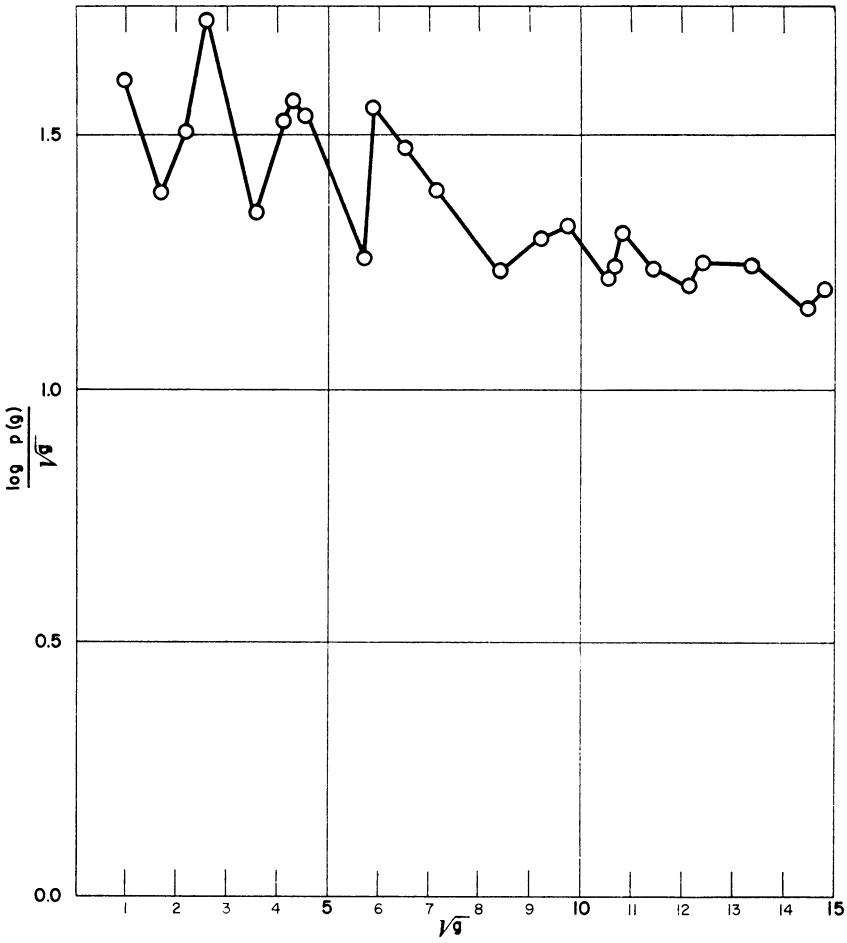

FIG. 1. The Maximal Gap Conjecture

$$10^{300} < p(10^6) < 10^{600}. \tag{6}$$

Almost surely $p(10^6)$ is greater than a googol, that is, 10^{100}. On the other hand [9], eight known Mersenne primes, namely $M_p = 2^p - 1$ for $p = 2203$, 2281, 3217, 4253, 4423, 9689, 9941, and 11213, exceed 10^{600}, and almost surely $p(10^6)$ is less than any of these. In fact, it is probable that somewhere below M_{11213} there is a gap of fifty million or more consecutive composites.

Applied Mathematics Laboratory
David Taylor Model Basin
Washington, D. C. 20007

1. E. LUCAS, *Théorie des Nombres*, Vol. 1, Gauthier-Villars, Paris, 1891, p. 360.
2. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, Vol. 1, Spartan, Washington, 1962, p. 201.
3. J. BARKLEY ROSSER & LOWELL SCHOENFELD, "Approximate formulas for some functions of prime numbers," *Illinois J. Math.*, v. 6, 1962, p. 64–94.
4. HARALD CRAMÉR, "On the order of magnitude of the difference between consecutive prime numbers," *Acta Arith.*, v. 2, 1937, p. 23–46.

5. D. H. LEHMER, "Tables concerning the distribution of primes up to 37 millions," 1957, copy deposited in the UMT File and reviewed in *MTAC*, v. 13, 1959, p. 56–57.
6. A. E. WESTERN, "Note on the magnitude of the difference between successive primes," *J. London Math. Soc.*, v. 9, 1934, p. 276–278.
7. J. W. L. GLAISHER, "On long successions of composite numbers," *Messenger of Mathematics*, v. 7, 1877, p. 102, 171.
8. KENNETH I. APPEL & J. BARKLEY ROSSER, *Table for Estimating Functions of Primes*, IDA-CRD Technical Report Number 4, 1961, p. 102. (Reviewed in RMT **55**, *Math. Comp.*, v. 16, 1962, p. 500–501.)
9. D. B. GILLIES, "Three new Mersenne primes and a statistical theory," *Math. Comp.*, v. 18, 1964, p. 93.
10. KARL PRACHAR, *Primzahlverteilung*, Springer, Berlin, 1957, p. 154–164.

Iteration of Triangular Matrices

By Lester J. Senechalle

1. Introduction. In order to calculate scalar functions of a matrix A, it is desirable to have a simple formula for the integral iterates A^n of A. Such a formula was first discovered by Sylvester [1], who expressed A^n as, essentially, a divided difference of the function $f(x) = x^n$. However, Sylvester's formula applies only to the case where the eigenvalues of A are distinct; the case of multiple eigenvalues was subsequently treated by Buchheim [2], and leads to confluent divided differences.

In this paper we give an especially simple formula for A^n when A is an upper triangular matrix. Our algorithm yields only the upper right hand entry of A^n, but this is adequate since every nonzero element of A^n is in fact the upper right-hand entry of the nth iterate of some triangular submatrix of A.

2. Notation. Let $[a_{ij}]$ be an $m \times m$ upper triangular matrix, so that $a_{ij} = 0$ if $i > j$, and for any nonnegative integer n let $[a_{ij}^{(n)}]$ denote the nth iterate of $[a_{ij}]$ under matrix multiplication. The matrix $[a_{ij}^{(n)}]$ is also upper triangular. Moreover, $[a_{ij}^{(0)}] = [\delta_{ij}]$, and $[a_{ij}^{(n+1)}] = [\sum_{k=1}^{m} a_{ik}^{(n)} \cdot a_{kj}]$.

If $(\lambda_1, \cdots, \lambda_k)$ is a chain of complex numbers, then $C(\lambda_1, \cdots, \lambda_k)$ denotes the set of all subchains which have λ_1 as their first element and λ_k as their last element. If $k \geqq 2$ and $i < k$, then $C_i(\lambda_1, \cdots, \lambda_k)$ denotes the set of chains belonging to $C(\lambda_1, \cdots, \lambda_k)$ which have λ_i as their next to last element. Thus $C(\lambda_1, \cdots, \lambda_k) = \bigcup_{i=1}^{k-1} C_i(\lambda_1, \cdots, \lambda_k)$ is a decomposition of $C(\lambda_1, \cdots, \lambda_k)$ into mutually disjoint subsets. For example, $C(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = \{(\lambda_1, \lambda_4), (\lambda_1, \lambda_2, \lambda_4), (\lambda_1, \lambda_3, \lambda_4), (\lambda_1, \lambda_2, \lambda_3, \lambda_4)\}$ and $C_3(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = \{(\lambda_1, \lambda_3, \lambda_4), (\lambda_1, \lambda_2, \lambda_3, \lambda_4)\}$.

If $\gamma = (\lambda_1, \cdots, \lambda_k)$ is a chain of distinct complex numbers and n is a nonnegative integer, then $q_n(\gamma)$ denotes the divided difference $[\lambda_1 \cdots \lambda_k]$ of the function $f(x) = x^n$ [3, Chapter 1]. Thus

$$q_n(\gamma) = \sum_{i=1}^{k} \frac{{\lambda_i}^n}{\prod_{j=1; j\neq i}^{k} (\lambda_i - \lambda_j)}.$$

In particular, $q_n(\gamma) = 0$ for $0 \leqq n < k$, and $q_n(\gamma) = {\lambda_1}^n$ if $\gamma = (\lambda_1)$. Furthermore, if $k \geqq 2$, $q_n'(\gamma)$ is defined as $q_n(\gamma')$, where $\gamma' = (\lambda_1, \cdots, \lambda_{k-1})$.

Received March 9, 1964.