MATHEMATICS OF COMPUTATION, VOLUME 33, NUMBER 147
JULY 1979, PAGES 1073–1080

Greatest of the Least Primes in Arithmetic Progressions Having a Given Modulus

By Samuel S. Wagstaff, Jr.

Abstract. We give a heuristic argument, supported by numerical evidence, which suggests that the maximum, taken over the reduced residue classes modulo k, of the least prime in the class, is usually about $\phi(k)\log k\log\phi(k)$, where ϕ is Euler's phi-function.

1. Introduction. When $(k, l) = 1$, let $P(k, l)$ denote the least prime in the arithmetic progression $l + kn$, $n \geqslant 0$. Let $P(k) = \max_l P(k, l)$, where the maximum is taken over all l for which $0 < l < k$ and $(k, l) = 1$.

In 1944, Linnik [5] proved that $P(k, l) < k^A$ for some large absolute constant A. Since then, several authors have found successively smaller, but still large, explicit values for A. Titchmarsh showed (Theorem 6 of [11]) that the Extended Riemann Hypothesis (ERH) for L-functions of characters modulo k implies that $P(k, l) \ll (\phi(k))^2 (\log k)^4$. Kanold [3] conjectured that $P(k, l) < k^2$ always. Heath-Brown [2] remarked that presumably $P(k, l) \ll k(\log k)^2$. Turán [12], also assuming the ERH, proved that for each $\delta > 0$, we have

$$P(k, l) < \phi(k)\log^{2+\delta} k \tag{1}$$

for almost all residue classes l, i.e., the inequality fails for at most $o(\phi(k))$ of the l's as $k \longrightarrow \infty$. His result, in contrast to the preceding statements, says nothing about $P(k)$. We mention it here because we will argue below that (1) holds for *all* l.

In the other direction, Landau (see Section 62 of [4]) proved the elementary result $P(k) > k + 1$ for every $k > 30$. From the Prime Number Theorem it is clear that for every positive ϵ, we have $P(k) > (1 - \epsilon)\phi(k)\log k$ for all $k > K(\epsilon)$. Erdös [1] proved that there is an $\epsilon > 0$ so that $P(k) > (1 + \epsilon)\phi(k)\log k$ for infinitely many k's. Prachar [8] and Schinzel [10] have shown that there is a $c > 0$ so that for every l there are infinitely many k for which $P(k, l) > ck\log k\log_2 k\log_4 k/(\log_3 k)^2$, where $\log_r k$ is the r-fold iterated logarithm. Pomerance [7] has shown that

$$P(k) > (e^\gamma - o(1))\phi(k)\log k\log_2 k\log_4 k/(\log_3 k)^2$$

except for a set of k's of asymptotic density zero.

In summary, it is known that $P(k)$ almost always exceeds $\phi(k)\log k$ and is always less than k^A for some large A, but even the ERH does not seem to yield $P(k) = o(k^2)$. We will present a heuristic argument that $P(k)$ is usually close to $\phi(k)\log k\log\phi(k)$ for large k. Since $\log\phi(k) \sim \log k$ as $k \longrightarrow \infty$, our reasoning says also that $P(k)$ is

Received August 25, 1978; revised September 22, 1978.
AMS (MOS) subject classifications (1970). Primary 10H20.
Key words and phrases. Least prime in an arithmetic progression.

0025-5718/79/0000-0116/$03.00

approximately $\phi(k)\log^2 k$ for most large k. We retain the $\log \phi(k)$ in the expression because it arises naturally in the argument and because the formula with it fits the numerical data slightly more closely.

2. **The Heuristic Estimate of $P(k)$.** Let $X = mk \log k$, where $m = m(k)$ will be chosen later. The number of positive integers below X and relatively prime to k is about $X\phi(k)/k$, and about $X/\log X$ of these are prime. Thus, the conditional probability that a number below X is prime, given that it is relatively prime to k, is approximately $k/(\phi(k)\log X)$. If $0 < l < k$ and $(k, l) = 1$, then the probability that all $[X/k]$ of the numbers

$$l,\ l + k,\ l + 2k,\ \ldots,\ l + [m \log k - 1]\,k$$

(omitting l if $l = 1$) are composite is about

$$\left(1 - \frac{k}{\phi(k)\log X}\right)^{m \log k}.$$

If we now require that $m \ll \log^3 k$, say, so that $\log X \sim \log k$ as $k \longrightarrow \infty$, then the latter probability is approximately

$$\left(1 - \frac{k}{\phi(k)\log k}\right)^{m \log k} \approx e^{-mk/\phi(k)}. \tag{2}$$

A. For any l, note that X will be a rough approximation to $P(k, l)$ if we choose m just large enough so that the probability (2) is neither very close to 0 nor to 1, say, $e^{-mk/\phi(k)} \approx e^{-c}$, where c is some positive constant of moderate size. We find $m \approx c\phi(k)/k$, so that $P(k, l) \approx X \approx c\phi(k)\log k$. This estimate is consistent with the results of Erdös [1] and may be obtained more directly by noting that there are about c primes below $c\phi(k)\log k$ in each of the classes relatively prime to k.

B. To estimate $P(k)$ by X, we want m to be so large that each residue class prime to k will have a good chance of containing a prime below X. From (2), the probability that every class does contain one (assuming independence of the classes) is about

$$(1 - e^{-mk/\phi(k)})^{\phi(k)}.$$

As in A, we ask that this probability be $\approx e^{-c}$. Then

$$e^{-mk/\phi(k)} \approx 1 - e^{-c/\phi(k)} \approx c/\phi(k),$$

or

$$P(k) \approx X \approx \phi(k)\log k(\log \phi(k) - \log c) \sim \phi(k)\log k \log \phi(k)$$

as $k \longrightarrow \infty$. This time c becomes less and less significant as k increases. This is the desired estimate of $P(k)$.

To obtain greater assurance that every class contains at least one prime, we could let $c \longrightarrow 0$ as $k \longrightarrow \infty$. With $c = 1/\log k$, for example, we see that $P(k) < (1 + \epsilon)\phi(k)\log k \log \phi(k)$ for almost all large k. A similar argument with $c = \log k$ shows that $P(k) > (1 - \epsilon)\phi(k)\log k \log \phi(k)$ for almost all large k. This reasoning suggests, indeed, that if we disregard a small set (i.e., of asymptotic density zero) of exceptions, then $P(k) \sim \phi(k)\log k \log \phi(k)$ as $k \longrightarrow \infty$.

TABLE 1

Typical values of P(k)

k	φ(k)	ℓ	P(k)	P(k)/est	[P(k)/k]
11	10	10	43	0.78	3
12	4	1	13	0.94	1
13	12	12	103	1.35	7
14	6	1	29	1.02	2
15	8	1	31	0.69	2
1000	400	921	13921	0.84	13
1001	720	74	33107	1.01	33
1002	332	391	13417	1.01	13
1003	928	822	43951	1.00	43
1004	500	371	18443	0.86	18
10000	4000	7461	477461	1.56	47
10001	9792	3382	873469	1.05	87
10002	3332	9937	209977	0.84	20
10003	8568	5919	806159	1.13	80
10004	4800	4565	374713	1.00	37
49996	24080	37163	2236987	0.85	44
49997	46784	32740	5582407	1.03	111
49998	15360	1813	1301761	0.81	26
49999	49998	13525	6213401	1.06	124
50000	20000	15219	2615219	1.22	52
97651	97650	92811	12787441	0.99	130
97652	48824	62001	6897641	1.14	70
97653	63504	24581	9985187	1.24	102
97654	48360	76247	5935487	0.99	60
97655	78120	56096	9723941	0.96	99
510521	464100	388050	80539847	1.01	157
510522	170172	384341	29994617	1.11	58
510523	466464	504724	83719973	1.05	163
510524	218784	123199	33307259	0.94	65
510525	272160	420388	37688713	0.84	73
999996	330672	764329	54764113	0.94	54
999997	997920	532429	222531763	1.17	222
999998	480060	382501	89382323	1.03	89
999999	466560	550894	71550823	0.85	71
1000000	400000	484781	72484781	1.02	72

3. The Numerical Evidence. Perhaps the foregoing heuristic argument can be improved. In any case, we can report that the empirical results given below do show that $P(k)/\phi(k)\log k \log \phi(k)$ is usually near 1. We give special attention to the exceptional k below, listing all those where this ratio is not so close to 1. We computed $P(k)$ for many values of k. Let S be the set of integers k in the intervals $11 \leqslant k \leqslant 50000$, $95001 \leqslant k \leqslant 100000$, $510501 \leqslant k \leqslant 510550$, and $999951 \leqslant k \leqslant 1000000$, together with $k = 115147, 357819$, and 636184. For each k in S, we computed $P(k)$ and recorded the l for which $P(k, l)$ is greatest. We could not extend the calculation beyond 1000000 because of space and time limitations. The block of 50 numbers beginning with 510501 was included because $510510 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$ is the

TABLE 2

Examples with small ratio $P(k)$/est

k	$\phi(k)$	l	P(k)	P(k)/est	[P(k)/k]
102	32	95	197	0.384	1
150	40	143	293	0.396	1
210	48	209	419	0.422	1
130	48	129	389	0.430	2
51	32	44	197	0.452	3
420	96	361	1201	0.454	2
228	72	77	761	0.455	3
246	80	145	883	0.458	3
312	96	217	1153	0.458	3
75	40	68	293	0.460	3
110	40	1	331	0.477	3
105	48	104	419	0.485	3
462	120	323	1709	0.485	3
528	160	361	2473	0.486	4
570	144	511	2221	0.489	3

TABLE 3

Examples with large ratio $P(k)$/est

k	$\phi(k)$	l	P(k)	P(k)/est	[P(k)/k]	Factorization
1623	1080	1478	123203	2.209	75	3·541
636184	315840	629991	116415479	2.178	182	8·281·283
461	460	22	37363	2.160	81	461
23636	11160	9451	2183963	2.085	92	4·19·311
3246	1080	3101	123203	2.020	37	2·3·541
1945	1552	722	169937	1.968	87	5·389
10948	4224	7989	642973	1.960	58	4·7·17·23
922	460	483	37363	1.941	40	2·461
40952	39600	38984	8352037	1.876	203	31·1321
19815	10560	3058	1806223	1.866	91	3·5·1321
32844	8448	27521	1472657	1.854	44	4·3·7·17·23
22505	15408	7419	2753029	1.849	122	5·7·643
541	540	18	39511	1.848	73	541
2732	1364	1587	143651	1.844	52	4·683
7049	5616	4420	786859	1.832	111	7·19·53

number below 1000000 for which $\phi(k)/k$ is least. We computed $P(k)$ for the three special values of k because we thought there was a reason (see below) why $P(k)$ might be unusually large for these k. The nine cases $2 \leqslant k \leqslant 10$ are left as an exercise for the reader.

Table 1 illustrates typical results from the huge table in our possession. The particular intervals of length 5 given here were chosen to be representative of the nearby numbers. In each table, "est" stands for the estimate $\phi(k)\log k \log \phi(k)$. It appears that, in fact, the larger k is, the more likely $P(k)$/est is to be close to 1. The column headed l gives the (necessarily unique) l for which $P(k, l) = P(k)$. The last column $[P(k)/k]$ gives the number of composites before the first prime in the arithmetic progression $l + kn$.

TABLE 4

Distribution of $P(k)$/est in intervals of length 0.1

Endpoints of intervals

k-interval	0.6 tail	0.7	0.8	0.9	1.0	1.1	1.2	1.3	1.4	1.5 tail
11-5010	100	357	877	1171	1067	695	371	187	86	47	42
5001-10000	2	72	540	1328	1335	854	496	218	92	36	27
10001-15000	0	40	439	1293	1393	976	491	230	85	27	26
20001-25000	0	15	262	1192	1549	1104	531	227	69	20	31
30001-35000	0	8	244	1107	1538	1206	537	213	95	33	19
45001-50000	0	3	169	1063	1602	1219	579	240	67	32	26
95001-100000	0	1	108	848	1797	1273	608	225	90	35	15
11-25000	102	503	2466	6125	6884	4674	2410	1099	420	160	147
25001-50000	0	30	1055	5457	8004	5946	2746	1094	399	162	107
510501-510550	0	0	1	8	16	17	7	0	0	1	0
999951-1000000	0	0	0	10	7	20	11	2	0	0	0

In Tables 2 and 3 we list the 15 moduli $k \in S$ for which $P(k)/\text{est}$ is smallest and greatest. Note that the k's in Table 2 are all small, while several quite large numbers k appear in Table 3. This happens because a single bad arithmetic progression can inflate $P(k)$, but a very great deal of good luck is required for every one of the $\phi(k)$ progressions to contain a small prime. Note also that $102 = 2 \cdot 51$, $150 = 2 \cdot 75$, $210 = 2 \cdot 105$, $3246 = 2 \cdot 1623$, and $922 = 2 \cdot 461$, and that in each case the same progression causes that large $P(k)$ for both the odd number and its double. Moreover, $1623 = 3 \cdot 541$, but different progressions inflate $P(k)$ for 1623 and 541.

The heuristic argument predicts that the distribution of $P(k)/\phi(k) \log k \log \phi(k)$ should have mean 1 and should peak more and more sharply about 1 as k increases. Table 4, which gives the distribution of this ratio for seven intervals of 5000 values of k each, supports this prediction well. (The statistics for four other intervals, two longer and two shorter than 5000, are also given at the end of Table 4.) The two center intervals of length 0.1 contain more and more of the ratios as the size of k increases. The size of the tails continually decreases. We have already explained why the upper tail is larger than the lower tail. The mean values of the ratio seem to converge slowly to 1.

Low [6] and Purdy [9] found three values of k for which a certain Dirichlet L-function $L_{-k}(s)$ with modulus k comes very close to 0 at $s = \frac{1}{2}$. Although there is no known connection between $P(k)$ and $L_{-k}(\frac{1}{2})$, we once thought that a small value of the latter would cause a large value of the former. It was at that time that we computed $P(k)$ for $k = 115147$, 357819, and 636184. The first two k produced ordinary ratios $P(k)/\phi(k) \log k \log \phi(k)$ of 1.20 and 1.03, but the third modulus did have the unusually high ratio shown in Table 3. The modulus 636184 deserves more study to determine if there really is a connection.

We became interested in studying $P(k, l)$ during the calculations of [13], where we had to compute $P(p, 1)$ for many primes p. We observed there that $P(p, 1)$ is about $p \log p$ on the average, which agrees with A of Section 2. The values of $P(p)$ for $p \in S$ seem to be statistically indistinguishable from those for $P(k)$ for all $k \in S$. There is nothing special about a prime modulus (except, of course, that $\phi(p) = p - 1$). For very small k, the value 1 often appears as the l for which $P(k) = P(k, l)$. For $k > 500$, however, the residue class 1 (mod k) is almost never the one with the greatest least prime. In fact, the numbers l/k, where $P(k, l) = P(k)$, seem to have a uniform distribution in the unit interval (0, 1).

After he conjectured that $P(k)/\phi(k) \log k$ tends to infinity as $k \longrightarrow \infty$, Pomerance [7] remarked that, in proving a lower bound for $P(k)$, the hardest values of k to treat seem to be the products of the first r primes for various r. We see from Table 5 that $P(k)/\phi(k) \log k \log \phi(k)$ really is a bit low for these numbers. Since the k's in Table 2 have only small prime divisors, it would be tempting to conjecture that the ratio will always be small for such numbers. However, the ratio is 1.352 for $k = 675 = 3^3 \cdot 5^2$ and 1.960 for $k = 10948 = 2^2 \cdot 7 \cdot 17 \cdot 23$. The numbers whose prime divisors are as small as possible are the powers of 2. Some of these are listed in Table 5. The ratios for these k are a little low, but definitely not unusually so.

TABLE 5

$P(k)$ *for* $k = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p_r$ *and* $k = 2^n$

k	$\phi(k)$	ℓ	P(k)	P(k)/est	[P(k)/k]
30	8	1	31	0.548	1
210	48	209	419	0.422	1
2310	480	697	14557	0.634	6
30030	5760	14111	464561	0.903	13
510510	92160	126449	10336649	0.747	20
16	8	9	41	0.889	2
32	16	1	97	0.631	3
64	32	57	313	0.679	4
128	64	85	853	0.660	6
256	128	125	3709	1.077	14
512	256	1	7681	0.867	15
1024	512	441	20921	0.945	20
2048	1024	1939	38803	0.717	18
4096	2048	4017	106417	0.819	25
8192	4096	2159	321647	1.048	39
16384	8192	16071	638663	0.892	38
32768	16384	28569	1634201	0.989	49

The maximum of $P(k)/k$ with $k \in S$ occurred at $k = 510533$. The ratio was 247.98 $l = 499932$, and $P(k) = 126601583$. Among the first 50000 numbers k, the greatest $P(k)/k$ was 204.98 at $k = 47903$, with $P(k) = 9819037$ and $l = 46825$.

The author warmly thanks Professor Douglas Hensley for a valuable discussion of the heuristic argument. He is grateful to the Computing Services Office of the University of Illinois for letting him use so much computer time.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

1. P. ERDÖS, "On some applications of Brun's method," *Acta Sci. Math.* (*Szeged*), v. 13, 1949, pp. 57–63.

2. D. R. HEATH-BROWN, "Almost-primes in arithmetic progressions and short intervals," *Math. Proc. Cambridge Philos. Soc.*, v. 83, 1978, pp. 357–375.

3. H.-J. KANOLD, "Über Primzahlen in arithmetischen Folgen," *Math. Ann.*, v. 156, 1964, pp. 393–395.

4. E. LANDAU, *Handbuch der Lehre von der Verteilung der Primzahlen,* Band I, Teubner, Leipzig-Berlin, 1909. Reprinted by Chelsea, New York, 1953.

5. U. V. LINNIK, "On the least prime in an arithmetic progression. I. The basic theorem," *Rec. Math.* (*N.S.*), v. 15 (57), 1944, pp. 139–178.

6. M. E. LOW, "Real zeros of the Dedekind zeta function of an imaginary quadratic field," *Acta Arith.*, v. 14, 1968, pp. 117–140.

7. C. POMERANCE, "A note on the least prime in an arithmetic progression." (To appear.)

8. K. PRACHAR, "Über die kleinste Primzahl einer arithmetischen Reihe," *J. Reine Angew. Math.*, v. 206, 1961, pp. 3–4.

9. G. B. PURDY, *Some Extremal Problems in Geometry and the Theory of Numbers,* Ph.D. thesis, University of Illinois at Urbana-Champaign, 1972.

10. A. SCHINZEL, "Remark on the paper of K. Prachar 'Über die kleinste Primzahl einer arithmetischen Reihe'," *J. Reine Angew. Math.*, v. 210, 1962, pp. 121–122.

11. E. C. TITCHMARSH, "A divisor problem," *Rend. Circ. Mat. Palermo*, v. 54, 1930, pp. 414–429.

12. P. TURÁN, "Über die Primzahlen der arithmetischen Progression," *Acta Sci. Math. (Szeged)*, v. 8, 1936/37, pp. 226–235.

13. S. S. WAGSTAFF, JR., "The irregular primes to 125000," *Math. Comp.*, v. 32, 1978, pp. 583–591.