MATHEMATICS OF COMPUTATION
Volume 71, Number 240, Pages 1781–1797
S 0025-5718(01)01382-5
Article electronically published on November 28, 2001

NUMERICAL CALCULATION OF THE DENSITY OF PRIME NUMBERS WITH A GIVEN LEAST PRIMITIVE ROOT

A. PASZKIEWICZ AND A. SCHINZEL

ABSTRACT. In this paper the densities $D(i)$ of prime numbers p having the least primitive root $g(p) = i$, where i is equal to one of the initial positive integers less than 32, have been numerically calculated. The computations were carried out under the assumption of the Generalised Riemann Hypothesis. The results of these computations were compared with the results of numerical frequency estimations.

1. AN OUTLINE OF THE METHOD OF COMPUTATION

Let $g(p)$ denote the least primitive root modulo p and $D(i)$ the density of prime numbers with the least primitive root equal to i, that is

$$D(i) = \lim_{x\to\infty} \pi(x)^{-1} \sum_{\substack{p\le x \\ g(p)=i}} 1.$$

In [3] Elliott and Murata gave the formula

$$D(i) = \sum_{M} (-1)^{|M|-1} A_M, \tag{1}$$

where M runs over all the subsets of the set $\{2, 3, \dots, i\}$ containing i. Here A_M denotes the conjectural density of primes p such that each $a_i \in M$ is a primitive root modulo p, expressed by the formula in Lemma 11.5, page 140 of Matthews [4]:

$$A_M = \prod_{p} (1 - c(p)) \sum_{a\in G(a_1,\dots,a_n)} \omega(a) f(a), \tag{2}$$

where $M = \{a_1, \dots, a_n\}$ and $G(a_1, \dots, a_n\}$ is the set of squarefree integers of the form $a = \kappa(a_1^{\varepsilon_1}, \dots, a_n^{\varepsilon_n}) \equiv 1 (\mathrm{mod}\, 4)$, $\varepsilon_i = 0, 1$, $\omega(a) = (-1)^{\sum_i \varepsilon_i}$ and $\kappa(b)$ is the squarefree part of the number b

$$f(b) = \mu(b) \prod_{p|b} \frac{c(p)}{1 - c(p)}.$$

Here $c(p)$ is the natural density of the set of primes $\{q : q \equiv 1 (\mathrm{mod}\, p),\ q \nmid a_1, \dots, a_n,$ and at least one of the numbers $a_1, \dots, a_n$ is a pth power residue modulo $q\}$.

Received by the editor November 29, 1999 and, in revised form, December 26, 2000.
2000 *Mathematics Subject Classification.* Primary 11Y16; Secondary 11A07, 11M26.
Key words and phrases. Prime, generators, primitive roots, extended Riemann hypothesis.

Formula (2) is based on the assumption that if $a_1^{\varepsilon_i}, \dots, a_n^{\varepsilon_n} = b^2$, then $S = \sum_i \varepsilon_i$ is even. If S is odd, then $A_M = 0$. There is a factor $1/2^n$ missing in (1.4) page 114 of Matthews [4], and this error is repeated in the paper of Elliott and Murata.

In [3] Elliott and Murata derived formulas for the density of prime numbers whose least primitive roots are the initial natural numbers $2, 3, 5, 6$ and 7. They are as follows:

$$D(2) = \Delta,$$

$$D(3) = \Delta_1 - \Delta_2,$$

$$D(5) = \frac{20}{19}\Delta_1 - \frac{200}{91}\Delta_2 + \frac{500}{439}\Delta_3,$$

$$D(6) = \Delta_1 - \frac{282}{91}\Delta_2 + \frac{1000}{439}\Delta_3,$$

$$D(7) = \Delta_1 - \left(4 + \frac{9}{91} + \frac{5}{281}\right)\Delta_2 + \left(6 + \frac{183}{439} + \frac{4826}{67585} + \frac{147193}{29669815}\right)\Delta_3 - \left(3 + \frac{1107}{2131} + \frac{71825}{1290197} + \frac{26503425}{2749409807}\right)\Delta_4,$$

where the initial Δ_i $(i = 1, 2, 3, 4)$ are

$$\Delta_1 = \prod_{p \geq 2}\left(1 - \frac{1}{p(p-1)}\right), \text{ Artin's constant,}$$

$$\Delta_2 = \prod_{p \geq 2}\left(1 - \frac{2}{p(p-1)} + \frac{1}{p^2(p-1)}\right),$$

$$\Delta_3 = \prod_{p \geq 2}\left(1 - \frac{3}{p(p-1)} + \frac{3}{p^2(p-1)} - \frac{1}{p^3(p-1)}\right),$$

$$\Delta_4 = \prod_{p \geq 2}\left(1 - \frac{4}{p(p-1)} + \frac{6}{p^2(p-1)} - \frac{4}{p^3(p-1)} + \frac{1}{p^4(p-1)}\right).$$

The calculation of the successive values of $D(i)$ is illustrated with an example for $i = 10$. According to (1),

$$D(10) = \sum_M (-1)^{|M|-1} A_M,$$

where M runs over all the subsets of the set $\{2, 3, 5, 6, 7, 10\}$ containing 10 (from the set of all natural numbers ≤ 10, we remove the powers $1, 4, 8, 9$, which can never be least primitive roots). Observe that if M contains a, b and ab, then $A_M = 0$, because if a, b are primitive roots for p, then ab is not. Therefore,

$$\begin{aligned} D(10) = {} & A_{\{10\}} - A_{\{2,10\}} - A_{\{3,10\}} - A_{\{5,10\}} - A_{\{6,10\}} \\ & - A_{\{7,10\}} + A_{\{2,3,10\}} + A_{\{2,6,10\}} + A_{\{2,7,10\}} \\ & + A_{\{3,5,10\}} + A_{\{3,6,10\}} + A_{\{3,7,10\}} + A_{\{5,6,10\}} \\ & + A_{\{5,7,10\}} + A_{\{6,7,10\}} - A_{\{2,3,7,10\}} - A_{\{2,6,7,10\}} \\ & - A_{\{3,5,7,10\}} - A_{\{3,6,7,10\}} - A_{\{5,6,7,10\}} \\ & - A_{\{3,5,6,10\}} + A_{\{3,5,6,7,10\}}. \end{aligned}$$

Now, for each of the 22 sets M, listed above we calculate $c(p)$, which we denote by $c(p, M)$ in order to avoid ambiguity. So, if the elements $a_1, \dots, a_n$, of the set M are

multiplicatively independent (that is they do not satisfy any relation of the form $a_1^{\alpha_1}a_2^{\alpha_2}\cdots a_n^{\alpha_n}=1$, where α_i $(i=1,2,\dots,n)$ are integers not all equal to 0), then

$$c(p,M)=\frac{1}{p-1}\left(1-\left(1-\frac{1}{p}\right)^{|M|}\right); \tag{3}$$

hence,

$$\prod_{p\geq 2}(1-c(p,M))=\Delta_{|M|}.$$

The assumption of the multiplicative independence of the elements holds for all the sets listed above except for $\{3,5,6,10\}$ and $\{3,5,6,7,10\}$ (we have $3\cdot 5^{-1}\cdot 6^{-1}\cdot 10=1$). In order to apply Matthews's formula (2) we compute the sum

$$S(M)=\sum_{\substack{\varepsilon_1=0\\ a=\kappa(a_1^{\varepsilon_1}\cdots a_n^{\varepsilon_n})}}^{1}\cdots\equiv\sum_{\substack{\varepsilon_n=0\\ 1(\mathrm{mod}\,4)}}^{1}(-1)^{\sum_i\varepsilon_i}f(|a|,M),$$

where the additional argument of the function f was added in order to avoid ambiguity, e.g.,

$$\text{for } M=\{10\}, S(M)=f(1,M)=1,$$

$$\text{for } M=\{2,10\}, S(M)=f(1,M)+f(5,M)=1-\frac{c(5,M)}{1-c(5,M)}=1-\frac{9}{91}=\frac{82}{91}.$$

The first summand corresponds to the choice $\varepsilon_1=\varepsilon_2=0$; the second to the choice $\varepsilon_1=\varepsilon_2=1$, etc. The calculation of the values of the coefficients A_M for the remaining sets M proceeds similarly up to the set $M=\{5,6,7,10\}$ inclusive. For $M=\{5,6,7,10\}$ we have

$$\begin{aligned}S(M)&=f(1,M)-f(5,M)+f(21,M)-f(105,M)\\&=1+\frac{c(5,M)}{1-c(5,M)}+\frac{c(3,M)}{1-c(3,M)}\cdot\frac{c(7,M)}{1-c(7,M)}\\&\quad+\frac{c(5,M)}{1-c(5,M)}\cdot\frac{c(3,M)}{1-c(3,M)}\cdot\frac{c(7,M)}{1-c(7,M)}.\end{aligned}$$

The first summand corresponds to the choice $\varepsilon_1=\varepsilon_2=\varepsilon_3=\varepsilon_4=0$; the second to the choice $\varepsilon_1=1,\varepsilon_2=\varepsilon_3=\varepsilon_4=0$; the third to $\varepsilon_1=\varepsilon_2=\varepsilon_3=\varepsilon_4=1$; and the fourth to $\varepsilon_1=0,\varepsilon_2=\varepsilon_3=\varepsilon_4=1$.

It remains to consider two special sets $M_1=\{3,5,6,10\}$ and $M_2=\{3,5,6,7,10\}$. For these sets the formula (3) is not valid and is replaced with

$$\begin{aligned}c(p,M_1)&=\frac{4}{p(p-1)}-\frac{6}{p^2(p-1)}+\frac{3}{p^3(p-1)},\\S(M_1)&=2f(1,M_1)-2f(5,M_1)=2+2\frac{c(5,M_1)}{1-c(5,M_1)}.\end{aligned}$$

The first summand corresponds to the choice $\varepsilon_1 = \varepsilon_3 = \varepsilon_4 = \varepsilon_2$; the second to the choice $\varepsilon_1 = \varepsilon_3 = \varepsilon_4 \neq \varepsilon_2$:

$$\begin{aligned} c(p, M_2) &= \frac{5}{p(p-1)} - \frac{10}{p^2(p-1)} + \frac{9}{p^3(p-1)} - \frac{3}{p^4(p-1)}; \\ S(M_2) &= 2f(1, M_2) - 2f(5, M_2) + 2f(21, M_2) - 2f(105, M_2) \\ &= 2 + 2\frac{c(5, M_2)}{1 - c(5, M_2)} + 2\frac{c(3, M_2)}{1 - c(3, M_2)} \cdot \frac{c(7, M_2)}{1 - c(7, M_2)} \\ &\quad + 2\frac{c(3, M_2)}{1 - c(3, M_2)} \cdot \frac{c(5, M_2)}{1 - c(5, M_2)} \cdot \frac{c(7, M_2)}{1 - c(7, M_2)}. \end{aligned}$$

The first summand corresponds to the choice $\varepsilon_1 = \varepsilon_3 = \varepsilon_3$, $\varepsilon_4 = \varepsilon_1 + \varepsilon_3$, $\varepsilon_5 = \varepsilon_3$; the second to the chioce $\varepsilon_1 = \varepsilon_3 \neq \varepsilon_2$, $\varepsilon_4 = \varepsilon_1 + \varepsilon_3$, $\varepsilon_5 = \varepsilon_3$; the third to the choice $\varepsilon_2 = \varepsilon_3 \neq \varepsilon_1$, $\varepsilon_4 = \varepsilon_1 + \varepsilon_3$, $\varepsilon_5 = \varepsilon_3$; the fourth to the choice $\varepsilon_1 = \varepsilon_2 \neq \varepsilon_3$, $\varepsilon_4 = \varepsilon_1 + \varepsilon_3$, $\varepsilon_5 = \varepsilon_3$.

Proceeding in this way, we can calculate densities $D(i)$ for any positive integer i. Beyond $i = 10$, the derivation of formulas for $D(i)$ ceases to make sense due to their length. However, the use of a computer makes it possible to extend the computations to some extent. In this paper, by designing an algorithm corresponding to the computational process described above, we computed the values of $D(i)$ for all positive integers $i < 32$, which are not powers of integers.

2. Results of numerical computations

The following numerical investigations were carried out:

- The densities $D(i)$ of prime numbers p having the least primitive root $g(p)$ equal to i were calculated; the results are illustrated in Table 3.
- For every prime number $p < 4 \cdot 10^{10}$, the value of its least primitive root was determined.
- The computed densities of prime numbers with given least primitive roots were compared with numerical frequency estimates; the respective values are shown side by side in Table 3.
- The graphs of densities $D(i)$ for initial values of i were prepared and tabulated with step equal to 10^9, the behaviour of the frequencies of prime numbers with a given least primitive root are illustrated in Figures 1–24. From the figures it may be concluded that the densities $D(i)$ are very stable. Oscillations have limited amplitude and a tendency to damp out.
- A graph of the average value of the least primitive root of prime numbers not exceeding $4 \cdot 10^{10}$ was prepared (Figure 25) and tabulated with a step equal to 10^9 (Table 1).
- The growth rate of the least primitive root of a prime number was numerically investigated (see Table 2). The value $g(p)$ of the least primitive root of a prime number p is well majorised by a second degree polynomial of the natural logarithm of p, which agrees with the conjecture by E. Bach [1] about the least primitive prime roots modulo a prime number.

All computations were performed with the aid of more than ten desktop IBM PC computers from Pentium 100 to Pentium III 500 during their idle time. The computations lasted approximately one year. The computational procedures (with some small exceptions) were written in a high level language in order to minimise the risk of programming error. Most of the results were verified using popular

numerical packages, e.g., MAPLE, GP/PARI. The verification required more time than the actual computations. For checking the number of primes generated, we used Mapes's algorithm, which was found to be the most computationally effective within the range of computations performed.

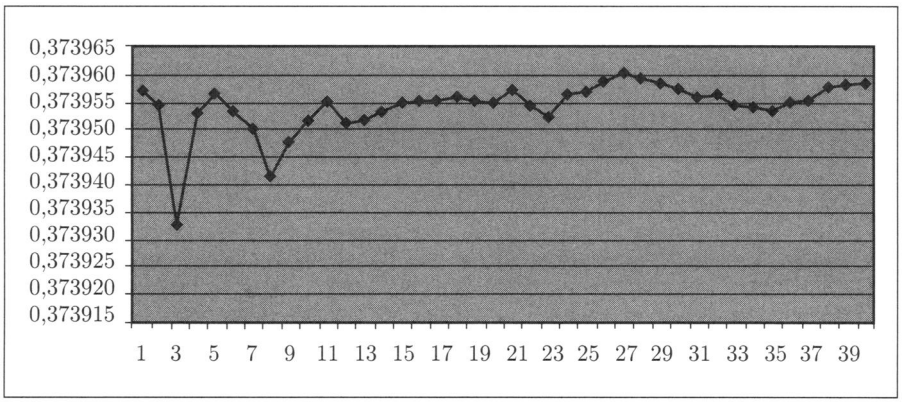

FIGURE 1. The density $D(2)$ of prime numbers with the least primitive root equal to 2

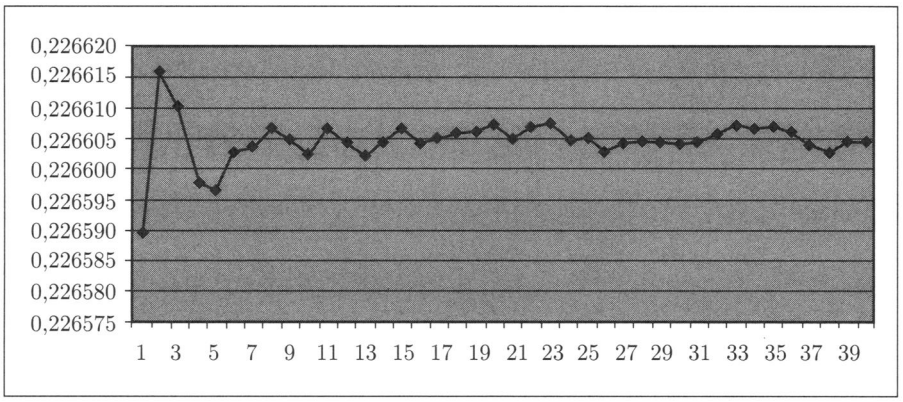

FIGURE 2. The density $D(3)$ of prime numbers with the least primitive root equal to 3

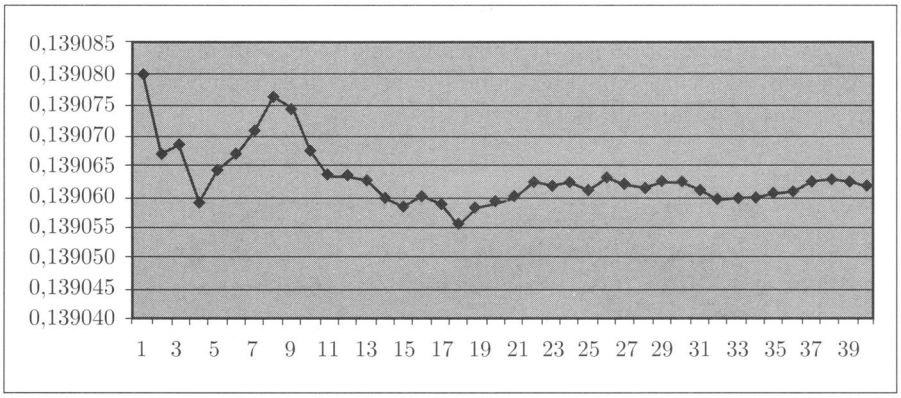

FIGURE 3. The density $D(5)$ of prime numbers with the least primitive root equal to 5

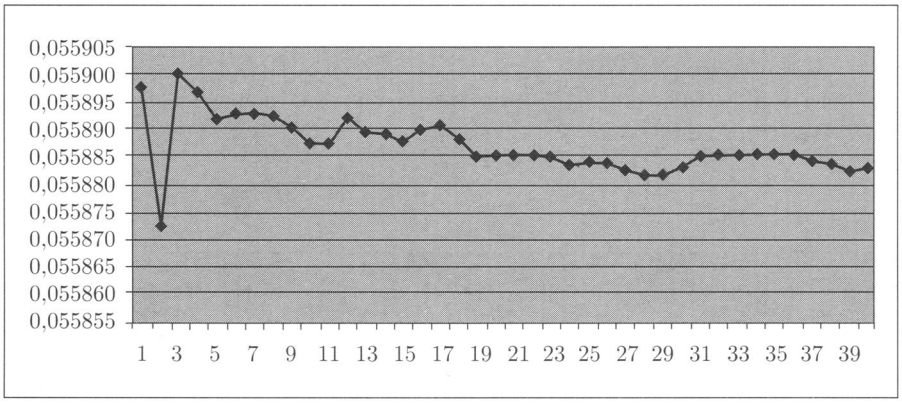

FIGURE 4. The density $D(6)$ of prime numbers with the least primitive root equal to 6

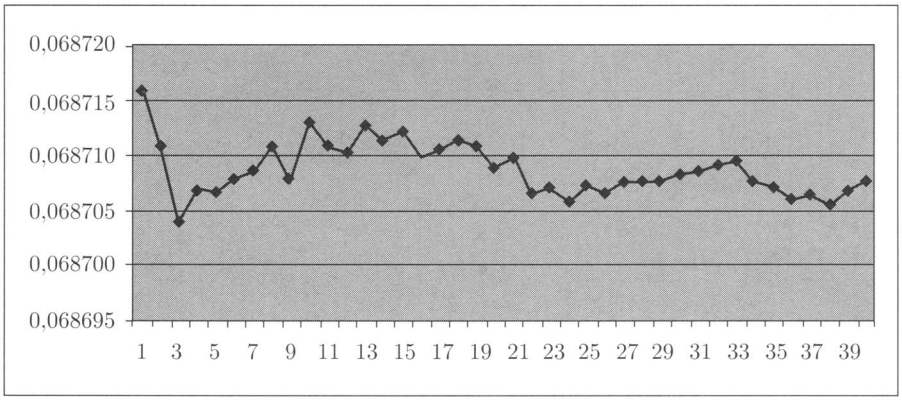

FIGURE 5. The density $D(7)$ of prime numbers with the least primitive root equal to 7

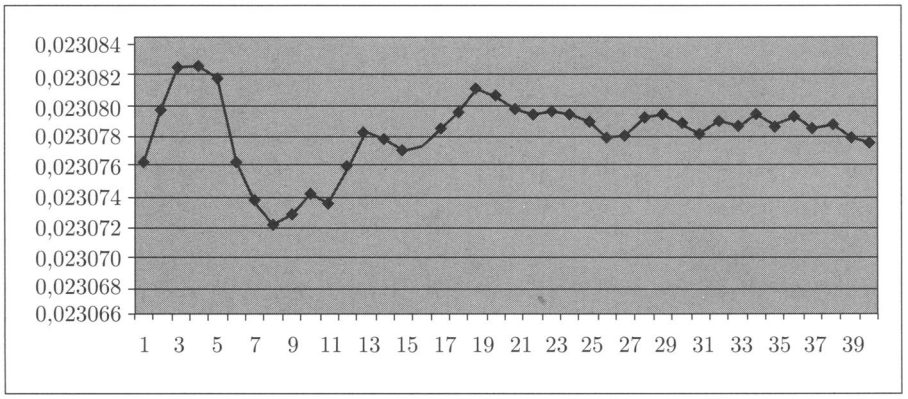

FIGURE 6. The density $D(10)$ of prime numbers with the least primitive root equal to 10

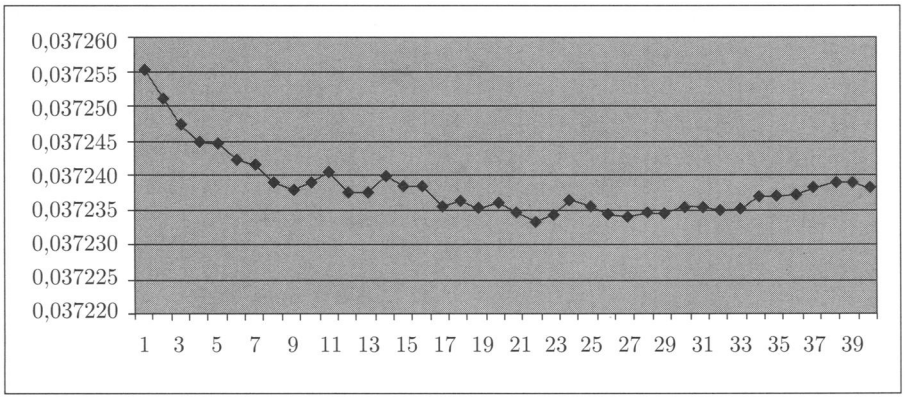

FIGURE 7. The density $D(11)$ of prime numbers with the least primitive root equal to 11

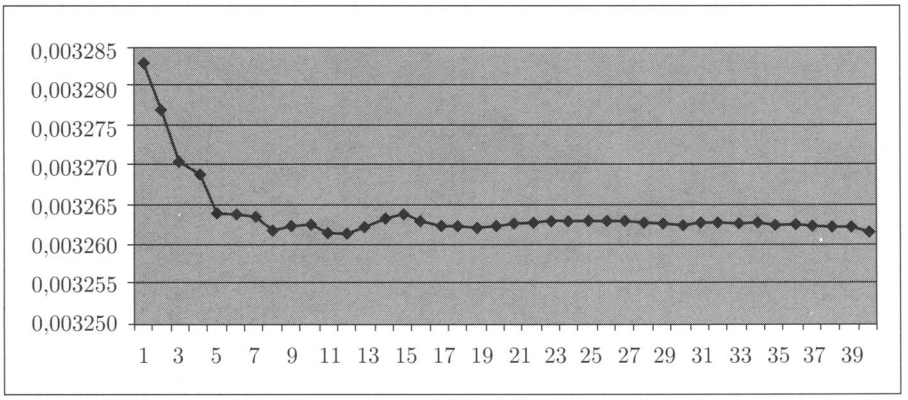

FIGURE 8. The density $D(12)$ of prime numbers with the least primitive root equal to 12

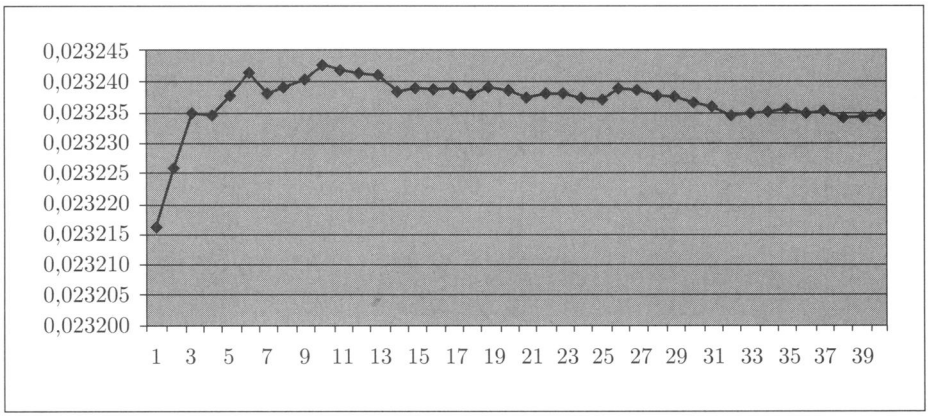

FIGURE 9. The density $D(13)$ of prime numbers with the least primitive root equal to 13

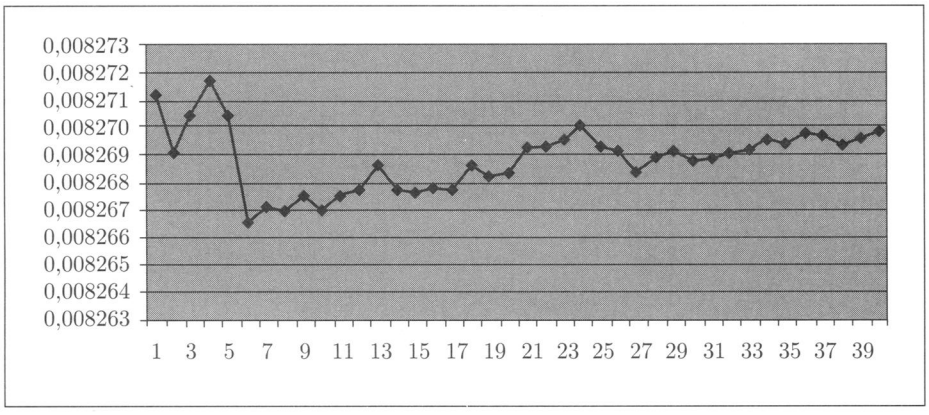

FIGURE 10. The density $D(14)$ of prime numbers with the least primitive root equal to 14

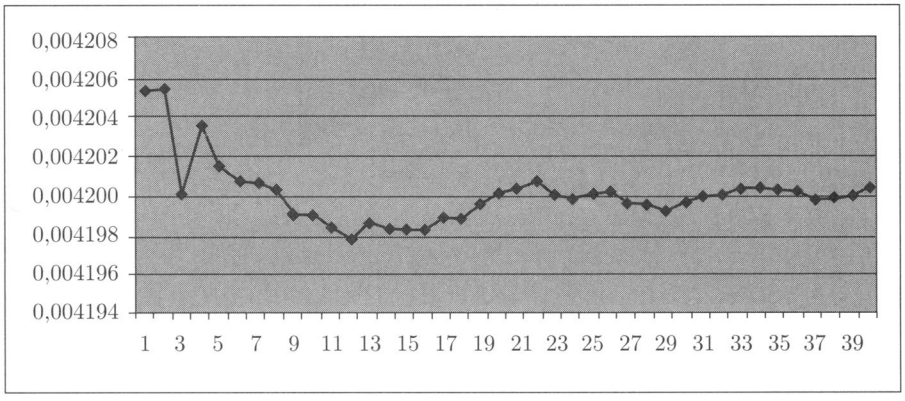

FIGURE 11. The density $D(15)$ of prime numbers with the least primitive root equal to 15

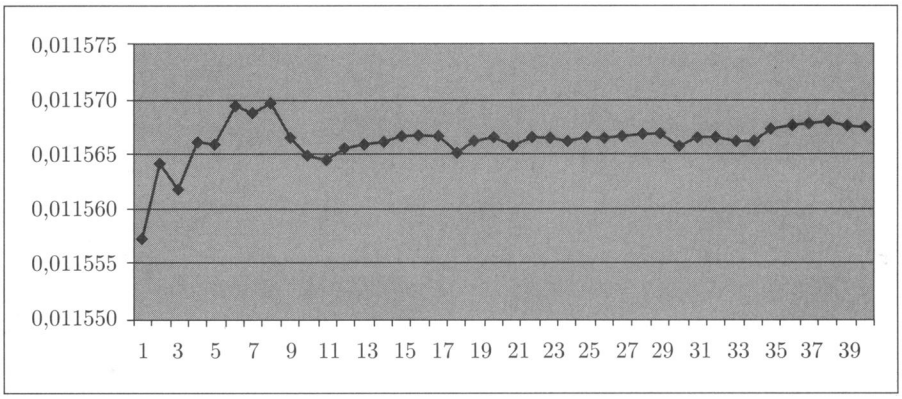

FIGURE 12. The density $D(17)$ of prime numbers with the least primitive root equal to 17

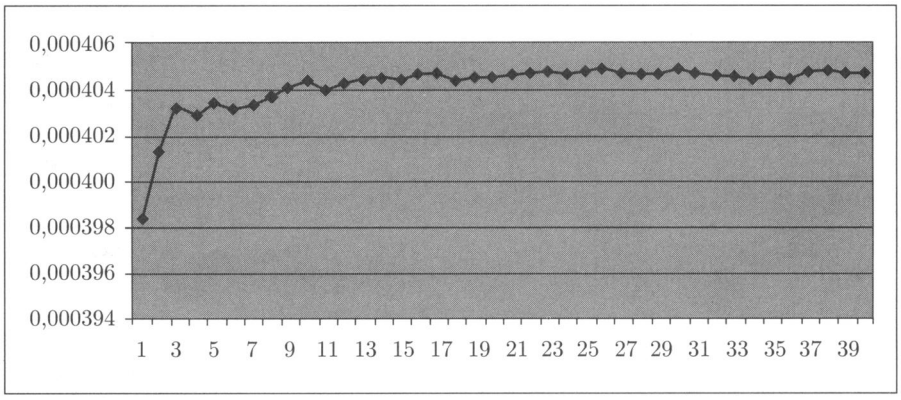

FIGURE 13. The density $D(18)$ of prime numbers with the least primitive root equal to 18

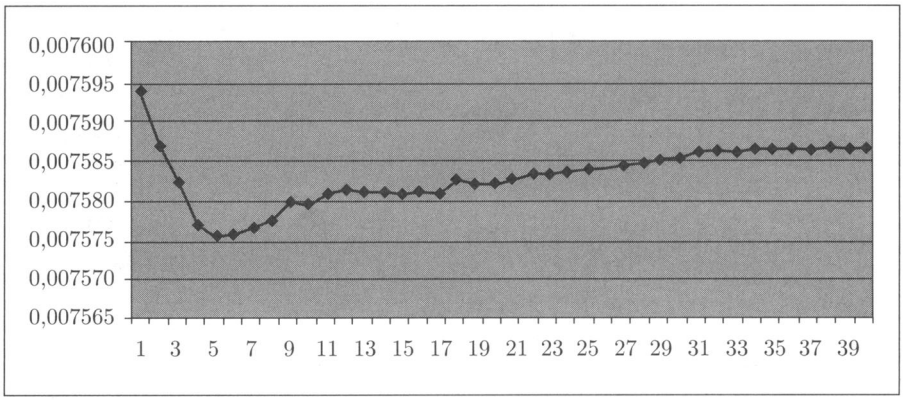

FIGURE 14. The density $D(19)$ of prime numbers with the least primitive root equal to 19

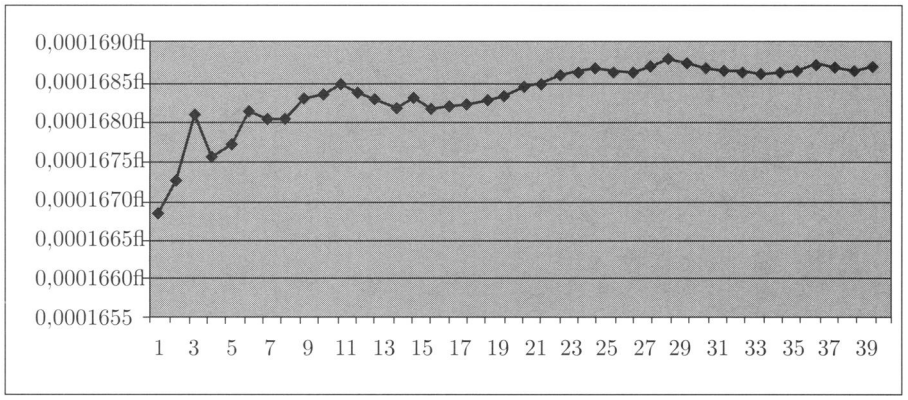

FIGURE 15. The density $D(20)$ of prime numbers with the least primitive root equal to 20

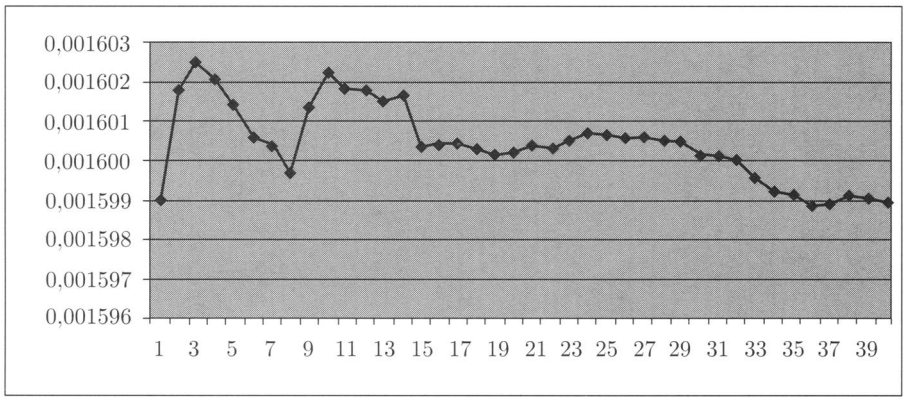

FIGURE 16. The density $D(21)$ of prime numbers with the least primitive root equal to 21

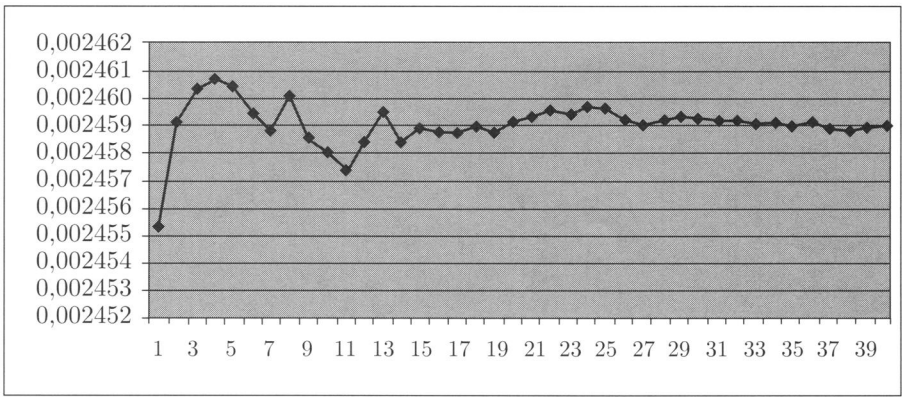

FIGURE 17. The density $D(22)$ of prime numbers with the least primitive root equal to 22

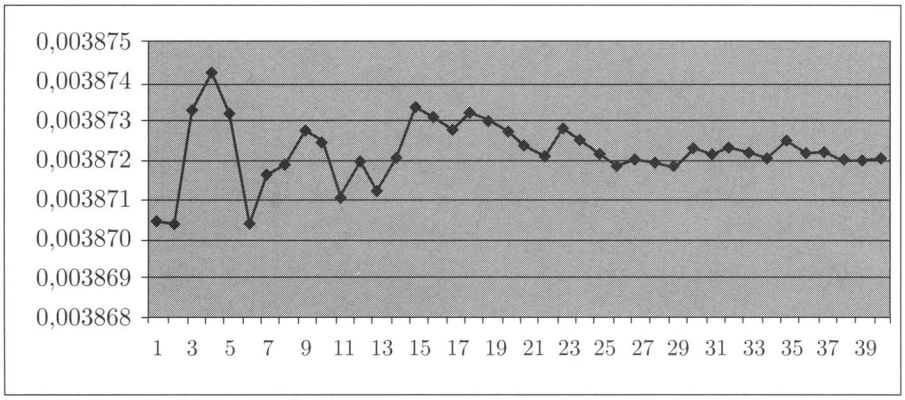

FIGURE 18. The density $D(23)$ of prime numbers with the least primitive root equal to 23

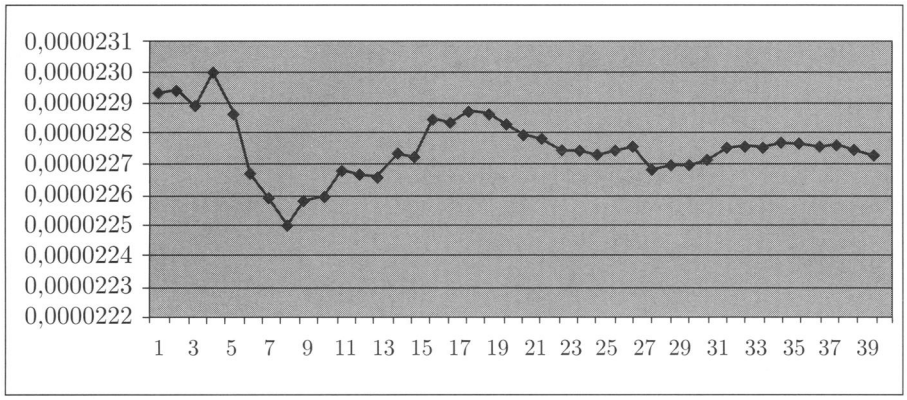

FIGURE 19. The density $D(24)$ of prime numbers with the least primitive root equal to 24

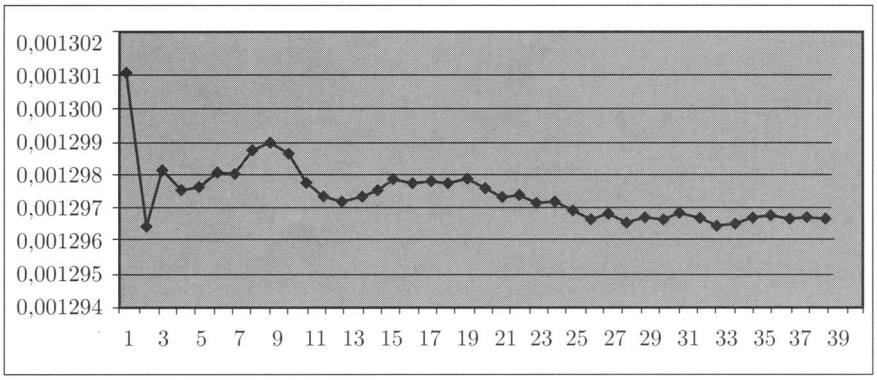

FIGURE 20. The density $D(26)$ of prime numbers with the least primitive root equal to 26

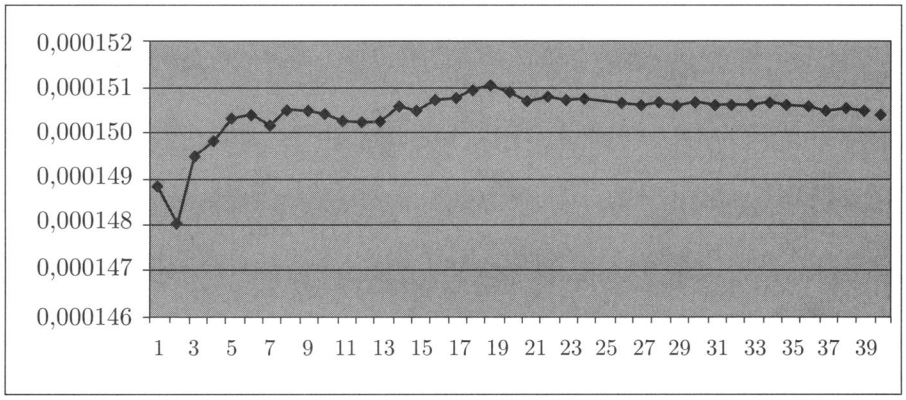

FIGURE 21. The density $D(28)$ of prime numbers with the least primitive root equal to 28

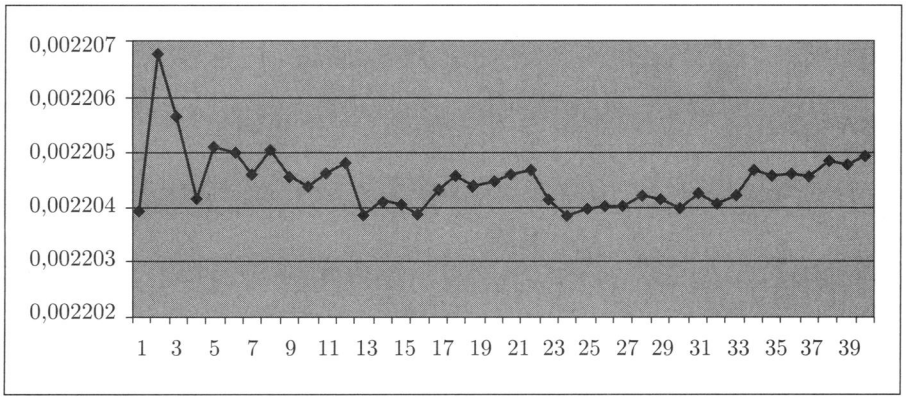

FIGURE 22. The density $D(29)$ of prime numbers with the least primitive root equal to 29

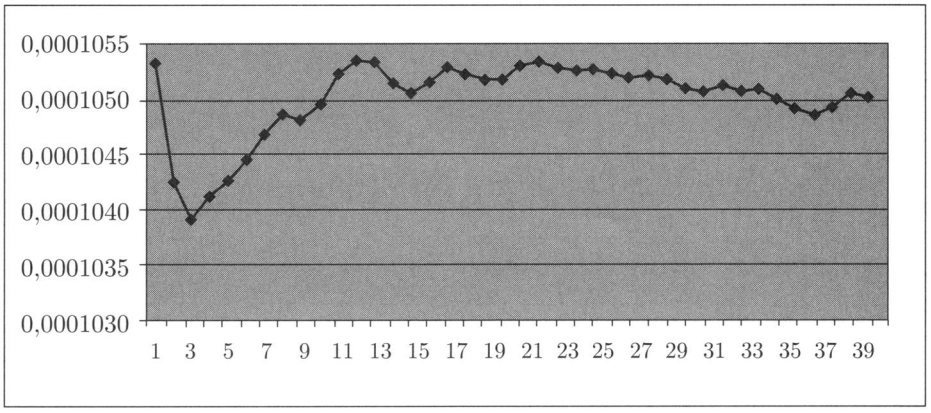

FIGURE 23. The density $D(30)$ of prime numbers with the least primitive root equal to 30

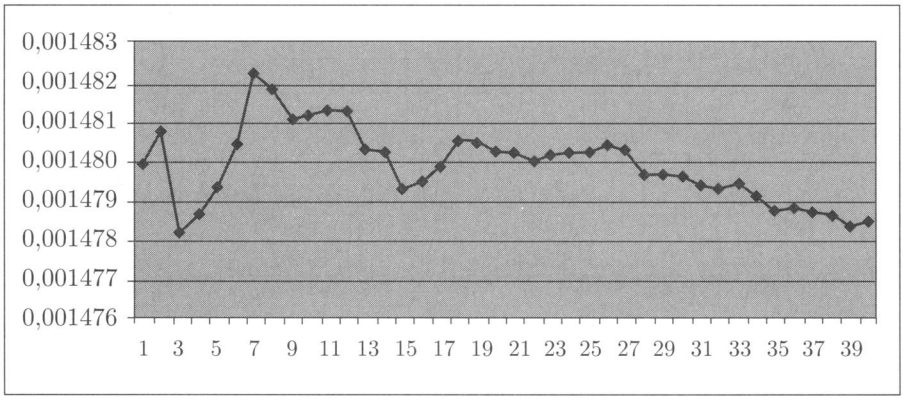

FIGURE 24. The density $D(31)$ of prime numbers with the least primitive root equal to 31

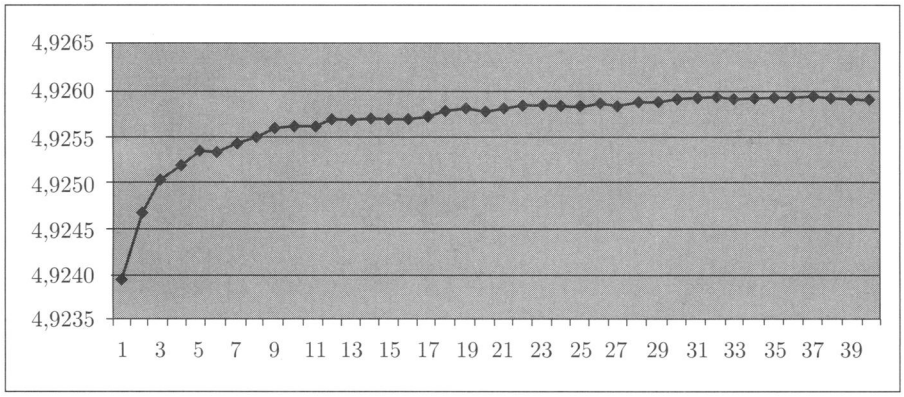

FIGURE 25. The average value of the least primitive root. The range of computations covers prime numbers less than $4 \cdot 10^{10}$.

TABLE 1. The average value of the least primitive root

n	$\pi(n \cdot 10^9)$	$\frac{1}{\pi(n \cdot 10^9)} \sum_{p<n \cdot 10^9} g(p)$	n	$\pi(n \cdot 10^9)$	$\frac{1}{\pi(n \cdot 10^9)} \sum_{p<n \cdot 10^9} g(p)$
1	50847534	4.923965712871	21	924324489	4.925797855823
2	98222287	4.924663401493	22	966358351	4.925832422385
3	144449537	4.925051147795	23	1008309544	4.925843984674
4	189961812	4.925188058325	24	1050186367	4.925846754020
5	234954223	4.925341307870	25	1091987405	4.925855088048
6	279545368	4.925330900136	26	1133717820	4.925866737278
7	323804352	4.925440477091	27	1175385155	4.925842229139
8	367783654	4.925509101064	28	1216987937	4.925879767368
9	411523195	4.925580522868	29	1258528162	4.925900388393
10	455052511	4.925611642211	30	1300005926	4.925903390845
11	498388617	4.925607016827	31	1341430624	4.925932161364
12	541555851	4.925698972831	32	1382799415	4.925928524492
13	584570200	4.925693412013	33	1424115489	4.925920066307
14	627440336	4.925695173988	34	1465374659	4.925939629611
15	670180516	4.925693396312	35	1506589876	4.925939416709
16	712799821	4.925704473484	36	1547756812	4.925945180075
17	755305935	4.925719780025	37	1588873108	4.925950159639
18	797703398	4.925784038089	38	1629945987	4.925942955189
19	840000027	4.925795219053	39	1670972264	4.925921554372
20	882206716	4.925790644287	40	1711955433	4.925920544687

TABLE 2. The growth rate of the least primitive root modulo a prime number. The range of computations covers all prime numbers less than $4 \cdot 10^{10}$.

$g(p)$	p	$\frac{g(p)}{\ln(p)}$	$\frac{g(p)}{\ln^2(p)}$	$\frac{g(p)}{\ln^3(p)}$	$\frac{3^{-\gamma} g(p)}{\ln(p)(\ln\ln(p))^2}$
3	7	1.541695	0.792274	0.407148	1.953083
5	23	1.594644	0.508578	0.162200	0.685570
6	41	1.615695	0.435078	0.117159	0.527004
7	71	1.642159	0.385241	0.090375	0.438590
19	191	3.617481	0.688745	0.131132	0.738260
21	409	3.492017	0.580675	0.096558	0.609157
23	2161	2.995444	0.390116	0.050807	0.404762
31	5881	3.571641	0.411504	0.047411	0.429429
37	37761	3.510758	0.333119	0.031608	0.355390
38	55441	3.478873	0.318488	0.029157	0.341698
44	71761	3.935213	0.351952	0.031477	0.379080
69	110881	5.939973	0.511352	0.044020	0.554523
73	760321	5.390837	0.398097	0.029398	0.445765
94	5109721	6.085459	0.393966	0.025504	0.455971
97	17551561	5.815119	0.348614	0.020899	0.412241
101	29418841	5.873067	0.341514	0.019858	0.407471
107	33358081	6.176826	0.356571	0.020583	0.426360
111	45024841	6.298685	0.357418	0.020281	0.429585
113	90441961	6.168048	0.336679	0.018377	0.409520
127	184254841	6.673031	0.350624	0.018423	0.431661
137	324013369	6.991117	0.356757	0.018205	0.443395
151	831143041	7.352113	0.357970	0.017429	0.451916
164	1685283601	7.719390	0.363347	0.017102	0.464042
179	6064561441	7.946469	0.352773	0.015660	0.459908
194	7111268641	8.551926	0.376986	0.016618	0.492719
197	9470788801	8.575852	0.373326	0.016251	0.490148
227	28725635761	9.426496	0.391448	0.016255	0.522907

TABLE 3. The frequencies of occurrence of prime numbers with a given least primitive root. $D(i)$ denotes the frequency of prime numbers with the least primitive root equal to i, calculated with the aid of theoretical considerations.

i	$D(i)$	$\frac{1}{\pi(a)} \sum_{\substack{p<a, g(p)=i \\ (a=4\cdot 10^{10})}} 1$
2	0.373955	0.3739585
3	0.226606	0.2266042
5	0.139065	0.1390616
6	0.055881	0.0558824
7	0.068702	0.0687077
10	0.023074	0.0230774
11	0.037238	0.0372384
12	0.003263	0.0032617
13	0.023229	0.0232346
14	0.008270	0.0082698
15	0.004200	0.0042004
17	0.011568	0.0115673
18	0.000404	0.0004047
19	0.007586	0.0075864
20	0.000168	0.0001687
21	0.001600	0.0015989
22	0.002459	0.0024589
23	0.003873	0.0038720
24	0.000022	0.0000227
26	0.001297	0.0012966
28	0.000150	0.0001503
29	0.002203	0.0022049
30	0.000104	0.0001050
31	0.001479	0.0014784

3. Acknowledgments

The referee informed us that in the Ph.D. thesis of Bob Buttsworth, University of Queensland 1983 [2], the formula for $D(i)$ is transformed using finite difference methods, into a form which allows one to prove that $D(i)$ is positive if i is not a perfect power, for which we are grateful.

The first author was technically supported during computations by the grant of Polish Committee for Scientific Research Nr. 8 T11 D 011 12.

References

1. E. Bach, *Comments on search procedures for primitive roots*, Math. Comp. **66** (1997), 1719–1727. MR **98a:**11187
2. R. N. Buttsworth, *A general theory of inclusion-exclusion with application to the least primitive root problem, and other density question*, Ph.D. Thesis, University of Queensland, Queensland, 1983.
3. P.D.T.A. Elliott, L. Murata, *On the average of the least primitive root modulo p*, J. London Math. Soc. (2) **56** (1997), 435-454. MR **98m:**11094
4. K. R. Matthews, *A generalisation of Artin's conjecture for primitive roots*, Acta Arith. **29** (1976), 113–146. MR **53:**313

Warsaw University of Technology, Institute of Telecommunications, Division of Telecommunications Fundamental, ul. Nowowiejska 15/19, 00-665 Warsaw, Poland
E-mail address: anpa@tele.pw.edu.pl

Institute of Mathematics, Polish Academy of Sciences, ul. Śniadeckich 8, 00-950 Warsaw, Poland
E-mail address: schinzel@impan.gov.pl