

## ON THE LEAST PRIME PRIMITIVE ROOT MODULO A PRIME

A. PASZKIEWICZ AND A. SCHINZEL

ABSTRACT. We derive a conditional formula for the natural density  $E(q)$  of prime numbers  $p$  having its least prime primitive root equal to  $q$ , and compare theoretical results with the numerical evidence.

### 1. THEORETICAL RESULT CONCERNING THE DENSITY OF PRIMES WITH A GIVEN LEAST PRIME PRIMITIVE ROOT

Let us denote, following Elliott and Murata [4], by  $g(p)$  and  $G(p)$  the least primitive and the least prime primitive root mod  $p$ , respectively. The first aim of this paper is to derive from the work of Matthews [5] a conditional (under the generalized Riemann hypothesis) formula for the density of primes  $p$  such that  $G(p) = q$ , where  $q$  is a given prime, and to compare this formula with the numerical evidence. Next we give for each prime  $q \leq 349$  the least prime  $p$  such that  $G(p) = q$ , if such  $p$  exists below  $2^{31}$ , and we compare  $G(p)$  with  $(\log p)(\log \log p)^2$ , which, according to a conjecture of E. Bach [2], is the maximal order of  $G(p)$  (i.e.,  $0 < \limsup \frac{G(p)}{(\log p)(\log \log p)^2} < \infty$ ). We also numerically investigate the average value of the least prime primitive root.

In order to formulate the theorem, we denote by  $p_n$  the  $n$ th prime and, for a given set  $M$ , by  $|M|$  its cardinality. Now we can state

**Theorem.** *Assume that the Riemann hypothesis holds for each of the fields  $Q(\sqrt[k]{1}, \sqrt[k]{p_1}, \dots, \sqrt[k]{p_n})$ , where  $k = \text{l.c.m. } l_i$  is squarefree. Then the set of primes  $p$  such that  $G(p) = p_n$  has a natural density equal to*

$$(1) \quad E(p_n) = \sum_{m=1}^n (-1)^{m-1} \Delta_m \cdot c_{m,n},$$

where

$$\Delta_m = \prod_{i=1}^{\infty} \left( 1 - \frac{1}{p_i - 1} \left( 1 - \left( 1 - \frac{1}{p_i} \right)^m \right) \right),$$

$$(2) \quad c_{m,n} = \frac{1}{2} \sum_{\substack{|M|=m \\ M \subset \{p_1, p_2, \dots, p_n\} \\ (M \ni p_n)}} \left\{ \prod_{p \in M - \{2\}} (1 + d_{m,p}) + \prod_{p \in M - \{2\}} (1 + (-1|p)d_{m,p}) \right\}$$

---

Received by the editor April 27, 1999 and, in revised form, September 7, 2000.

2000 *Mathematics Subject Classification.* Primary 11Y16; Secondary 11A07, 11M26.

*Key words and phrases.* Primes, generators, extended Riemann hypothesis.

and

$$d_{m,p} = \frac{1}{p-1} \left( 1 - \left( 1 - \frac{1}{p} \right)^m \right) \cdot \left( 1 - \frac{1}{p-1} \left( 1 - \left( 1 - \frac{1}{p} \right)^m \right) \right)^{-1}.$$

The above formula for  $c_{m,n}$  is due to the referee, which we gratefully acknowledge. The expression given in (2) can be efficiently evaluated using a generating function approach. Our original formula was less suitable for computation.

The proof is based on two lemmas, in which the letters  $p, q, r$ , are reserved for primes and  $\log_2 x = \log \log x$ .

**Lemma 1.** *Let  $M = \{r_1, \dots, r_m\}$  be a set of primes,*

$$N_M(x) = \{p \leq x : \text{every } r \text{ in } M \text{ is a primitive root mod } p\}.$$

*On the assumption of the Riemann hypothesis for each extension*

$$Q(\sqrt[k]{1}, \sqrt[k]{r_1}, \dots, \sqrt[k]{r_m}),$$

*where  $k = \text{l.c.m.} l_i$  is squarefree we have*

$$|N_M(x)| = A_M \cdot \text{Li } x + O_M(\text{Li } x (\log x)^{-1} (\log_2 x)^{2^{M^1-1}}),$$

*where  $A_M$  is defined as follows.*

*Let  $c(p)$  be the natural density of the set*

$$\{q : q \equiv 1 \pmod{p}, \text{ at least one of } r_1, \dots, r_m \text{ is a } p\text{th power residue mod } r\}$$

*and let  $\bar{c}(p) = 1 - c(p)$ . Also let  $G(r_1, \dots, r_m)$  denote the set of numbers of the form  $a = r_1^{\varepsilon_1} \cdots r_m^{\varepsilon_m} \equiv 1 \pmod{4}$ ,  $\varepsilon_i = 0$  or  $1$ , and finally let*

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

*Then*

$$(3) \quad A_M = \prod_{i=1}^{\infty} \bar{c}(p_i) \sum_{a \in G(r_1, \dots, r_m)} f(a).$$

*Proof.* This is how Theorem 13.2 of Matthews [5] simplifies when his set  $M$  consists of primes.

**Lemma 2.** *In the notation of Lemma 1*

$$c(p) = \frac{1}{p-1} \left( 1 - \left( 1 - \frac{1}{p} \right)^m \right).$$

*Proof.* Let us put in Theorem 7.11\* of [6]  $K = Q(\zeta_p), L = Q(\zeta_p, \sqrt[p]{r_1}, \dots, \sqrt[p]{r_m})$ , where  $\zeta_p$  is a primitive root of unity of order  $p$ . The extension  $L/K$  is Abelian and its Galois group is isomorphic to  $F_p^m$ , a vector  $[a_1, \dots, a_m] \in F_p^m$  acts on  $L$  by the formula

$$\sqrt[p]{r_i} \rightarrow \zeta_p^{a_i} \cdot \sqrt[p]{r_i} \quad (1 \leq i \leq m).$$

Let, for a prime ideal  $\mathfrak{q}$  of  $K$  not dividing  $r_1, \dots, r_m$ ,  $F_{L/K}(\mathfrak{q})$  be the Artin symbol, i.e., a vector  $[a_1, \dots, a_m] \in F_p^m$  such that

$$(4) \quad r_i^{\frac{N_{\mathfrak{q}}-1}{p}} \equiv \zeta_p^{a_i} \pmod{\mathfrak{q}} \quad (1 \leq i \leq m).$$

By Theorem 7.11\* of [6] for each  $[a_1, \dots, a_m] \in F_p^m$ , the number of prime ideals  $\mathfrak{q}$  of  $K$  with norm  $\leq x$  satisfying  $F_{L/K}(\mathfrak{q}) = [a_1, \dots, a_m]$ , hence (4), is  $(\frac{1}{p^m} + o(1)) \cdot \frac{x}{\log x}$ .

If at least one  $r_i$  is a  $p$ th power residue and  $q \equiv 1 \pmod{p}$ ,  $q \nmid r_1, \dots, r_m$ , then for each prime ideal  $\mathfrak{q}$  of  $K$  dividing  $q$  we have in (1) at least one  $a_i = 0$  ( $1 \leq i \leq m$ ). The number of vectors  $[a_1, \dots, a_m]$  in  $F_p^m$  with this property is  $p^m - (p-1)^m$ . To each prime  $q \equiv 1 \pmod{p}$  correspond  $p-1$  ideals  $\mathfrak{q}$  of norm  $q$ . Since the number of prime ideals with norm  $\leq x$  not being a prime is  $o(\frac{x}{\log x})$ , the lemma follows.

*Proof of the Theorem.* By the sieve principle the number  $N(x)$  of primes  $\leq x$  with  $G(p) = p_n$  equals

$$\sum_{\substack{M \subset \{p_1, \dots, p_n\} \\ (M \ni p_n)}} (-1)^{|M|-1} N_M(x)$$

(cf. [4, Lemma 10], for a similar formula concerning  $g(p)$ ); hence by Lemma 1,

$$N(x) = \sum_{\substack{M \subset \{p_1, \dots, p_n\} \\ (M \ni p_n)}} (-1)^{|M|-1} A_M \operatorname{Li} x + O_n(\operatorname{Li} x (\log x)^{-1} (\log_2 x)^{2^n-1})$$

and

$$(5) \quad E(p_n) = \sum_{\substack{M \subset \{p_1, \dots, p_n\} \\ (M \ni p_n)}} (-1)^{|M|-1} A_M.$$

Now if  $M = \{r_1, \dots, r_m\}$ , we have by Lemma 2

$$\begin{aligned} \bar{c}(p_i) &= 1 - \frac{1}{p_i - 1} \left( 1 - \left( 1 - \frac{1}{p_i} \right)^m \right), \\ \frac{c(p)}{1 - c(p)} &= d_{m,p}, \end{aligned}$$

hence

$$(6) \quad \prod_{i=1}^{\infty} \bar{c}(p_i) = \Delta_m.$$

On the other hand if  $M_\varepsilon = \{r : r \equiv \varepsilon \pmod{4}\}$ , the condition  $\prod_{\mu=1}^m r_\mu^{\varepsilon_\mu} \equiv 1 \pmod{4}$  is equivalent to

$$\varepsilon_\mu = 0 \text{ if } r_\mu = 2 \text{ and } \sum_{r_\mu \in M_{-1}} \varepsilon_\mu \equiv 0 \pmod{2}.$$

Hence

$$\begin{aligned} \sum_{a \in G(r_1, \dots, r_m)} f(a) &= \sum_{k=0}^{|M_1|} \sum_{\substack{N \subset M_1 \\ |N|=k}} \prod_{r \in N} d_{m,r} \cdot \sum_{k=0}^{\lfloor \frac{|M_{-1}|}{2} \rfloor} \sum_{\substack{N \subset M_{-1} \\ |N|=2k}} \prod_{r \in N} d_{m,r} \\ (7) \quad &= \prod_{r \in M_1} (1 + d_{m,r}) \cdot \frac{\prod_{r \in M_{-1}} (1 + d_{m,r}) + \prod_{r \in M_{-1}} (1 - d_{m,r})}{2} \\ &= \frac{1}{2} \left\{ \prod_{p \in M - \{2\}} (1 + d_{m,p}) + \prod_{p \in M - \{2\}} (1 + (-1|p)d_{m,p}) \right\}, \end{aligned}$$

and (1) follows from (2), (3), (5), (6) and (7).

## 2. RESULTS OF NUMERICAL INVESTIGATIONS

This section addresses two practical topics:

- It attempts to verify empirically the existence of positive densities  $E(p_n)$  for all primes having their least prime primitive root equal to  $p_n$ . By formulas (1) and (2), values of  $E(p_n)$  for  $n \leq 25$  have been computed. These values were compared with the frequencies calculated empirically on computers.
- It attempts to answer the question of whether the average value of the least prime primitive root tends to a finite limit.

The computation of  $E(p_n)$  was programmed for all  $n \leq 25$  with the aid of an IBM PC (Pentium 100 Mhz) computer using Borland's PASCAL compiler. Table 1 shows the results of the computation of  $E(p_n)$  according to formulas (1) and (2) for initial values of  $n$ . The constants  $\Delta_n$  were computed with high accuracy and are as follows:

|                                 |                                 |                                 |
|---------------------------------|---------------------------------|---------------------------------|
| $\Delta_1 = 0.373955813619,$    | $\Delta_2 = 0.147349400317,$    | $\Delta_3 = 0.060821655315,$    |
| $\Delta_4 = 0.026107446426,$    | $\Delta_5 = 0.011565842109,$    | $\Delta_6 = 0.005251758060,$    |
| $\Delta_7 = 0.002430226781,$    | $\Delta_8 = 0.001140851399,$    | $\Delta_9 = 0.000541435518,$    |
| $\Delta_{10} = 0.000259105371,$ | $\Delta_{11} = 0.000124792269,$ | $\Delta_{12} = 0.000060404308,$ |
| $\Delta_{13} = 0.000029353746,$ | $\Delta_{14} = 0.000014309885,$ | $\Delta_{15} = 0.000006994080,$ |
| $\Delta_{16} = 0.000003425724,$ | $\Delta_{17} = 0.000001680934,$ | $\Delta_{18} = 0.000000826053,$ |
| $\Delta_{19} = 0.000000406471,$ | $\Delta_{20} = 0.000000200235,$ | $\Delta_{21} = 0.000000098737,$ |
| $\Delta_{22} = 0.000000048730,$ | $\Delta_{23} = 0.000000024068,$ | $\Delta_{24} = 0.000000011896,$ |
| $\Delta_{25} = 0.000000005883.$ |                                 |                                 |

The calculation was similar to that of Wrench [9].

One can prove that  $\lim_{n \rightarrow \infty} \frac{\Delta_n}{\Delta_{n+1}} = 2$ .

Note that  $E(2)$  is Artin's constant and that  $E(3) = \Delta_1 - \Delta_2$ . The referee has observed that  $E(p_{n+1})/E(p_n)$  seems to tend to a limit, but we are unable to prove or disprove this.

Additionally the frequencies of least prime primitive roots for prime numbers from the interval [3, 2147483647] were computed. The computations were done on several IBM PC Pentium computers. The program for the computations was optimized for 32-bit arithmetic. Results of computations are gathered in Table 2. The correctness of computations was monitored in several ways.

- The number of generated primes. To verify the number of generated primes that least prime primitive roots were searched for, the algorithm by D. C. Mapes from 1963, for finding isolated values of the  $\pi(x)$  function (the number of primes  $\leq x$ ) was used.
- Verification of the factorization of  $p-1$ , where  $p$  is a randomly selected prime, with the aid of procedures independently implemented by other people.
- Partial verification of computations by existing packages, e.g., GP/PARI, Maple.

Let us denote by  $N(p_n, x)$  the number of least prime primitive roots equal to  $p_n$  for primes not exceeding  $x$  and respectively by  $E(p_n, x)$  the natural density of primes not exceeding  $x$ , having their least primitive roots equal to  $p_n$ .

TABLE 1. Theoretical values of densities  $E(p_n)$  of least prime primitive roots equal to  $p_n$  for  $n \leq 25$ 

| $n$ | $p_n$ | $E_n$      |
|-----|-------|------------|
| 1   | 2     | 0.37395581 |
| 2   | 3     | 0.22660641 |
| 3   | 5     | 0.13906581 |
| 4   | 7     | 0.08639185 |
| 5   | 11    | 0.05640411 |
| 6   | 13    | 0.03669884 |
| 7   | 17    | 0.02468028 |
| 8   | 19    | 0.01691581 |
| 9   | 23    | 0.01159480 |
| 10  | 29    | 0.00799836 |
| 11  | 31    | 0.00561924 |
| 12  | 37    | 0.00394799 |
| 13  | 41    | 0.00280419 |
| 14  | 43    | 0.00200731 |
| 15  | 47    | 0.00144059 |
| 16  | 53    | 0.00103755 |
| 17  | 59    | 0.00075313 |
| 18  | 61    | 0.00054722 |
| 19  | 67    | 0.00040018 |
| 20  | 71    | 0.00029321 |
| 21  | 73    | 0.00021534 |
| 22  | 79    | 0.00015895 |
| 23  | 83    | 0.00011751 |
| 24  | 89    | 0.00008706 |
| 25  | 97    | 0.00006471 |

Graphs of the functions  $E(p_n, x)$  for primes  $p_n < 32$  and  $x < 21 \cdot 10^8$  are given below. Figures 1–11 show us that the behavior of natural densities of primes with a given least primitive root equal to a small prime number is extremely regular. The functions  $E(p_n, x)$  for primes  $p_n < 32$  stabilize very early and at least four decimal digits after the dot are constant.

Let us denote by  $E^*(x)$  the average value of the least prime primitive root of primes not exceeding  $x$ , that is

$$E^*(x) = \frac{1}{\pi(x)} \sum_{p \leq x} G(p),$$

and the above sum is extended for all primes  $p$  less than or equal to  $x$ .

TABLE 2. Frequencies of least prime primitive roots of prime numbers less than or equal to  $x = 2,000,000,000$ .  $N(p_n, x)$  denotes the number of least prime primitive roots equal to  $p_n$  for primes not exceeding  $x$ .

| $p_n$ | $N(p_n, x)$ | $E(p_n, x)$  | $p_n$ | $N(p_n, x)$ | $E(p_n, x)$  |
|-------|-------------|--------------|-------|-------------|--------------|
| 2     | 36730667    | 0.3739545079 | 131   | 787         | 0.0000080124 |
| 3     | 22258719    | 0.2266157680 | 137   | 632         | 0.0000064344 |
| 5     | 3659479     | 0.1390670022 | 139   | 471         | 0.0000047952 |
| 7     | 8486600     | 0.0864019792 | 149   | 362         | 0.0000036855 |
| 11    | 5539490     | 0.0563974854 | 151   | 248         | 0.0000025249 |
| 13    | 3603666     | 0.0366888830 | 157   | 183         | 0.0000018631 |
| 17    | 2424059     | 0.0246793174 | 163   | 139         | 0.0000014152 |
| 19    | 1662660     | 0.0169275228 | 167   | 98          | 0.0000009977 |
| 23    | 1139840     | 0.0116046982 | 173   | 75          | 0.0000007636 |
| 29    | 786125      | 0.0080035298 | 179   | 71          | 0.0000007229 |
| 31    | 551842      | 0.0056182972 | 181   | 53          | 0.0000005396 |
| 37    | 387927      | 0.0039494804 | 191   | 40          | 0.0000004072 |
| 41    | 275476      | 0.0028046181 | 193   | 39          | 0.0000003971 |
| 43    | 197240      | 0.0020080982 | 197   | 21          | 0.0000002138 |
| 47    | 140579      | 0.0014312332 | 199   | 22          | 0.0000002240 |
| 53    | 101667      | 0.0010350706 | 211   | 20          | 0.0000002036 |
| 59    | 73978       | 0.0007531692 | 223   | 8           | 0.0000000814 |
| 61    | 53542       | 0.0005451105 | 227   | 3           | 0.0000000305 |
| 67    | 39135       | 0.0003984330 | 229   | 2           | 0.0000000204 |
| 71    | 28765       | 0.0002928561 | 233   | 6           | 0.0000000611 |
| 73    | 20912       | 0.0002129048 | 239   | 4           | 0.0000000407 |
| 79    | 15548       | 0.0001582940 | 241   | 3           | 0.0000000305 |
| 83    | 11486       | 0.0001169388 | 251   | 3           | 0.0000000305 |
| 89    | 8462        | 0.0000861515 | 257   | 2           | 0.0000000204 |
| 97    | 6217        | 0.0000632952 | 263   | 2           | 0.0000000204 |
| 101   | 4721        | 0.0000480644 | 277   | 1           | 0.0000000102 |
| 103   | 3470        | 0.0000353280 | 283   | 1           | 0.0000000102 |
| 107   | 2498        | 0.0000254321 | 307   | 1           | 0.0000000102 |
| 109   | 1818        | 0.0000185090 | 347   | 1           | 0.0000000102 |
| 113   | 1419        | 0.0000144468 | 349   | 1           | 0.0000000102 |
| 127   | 980         | 0.0000099774 |       |             |              |

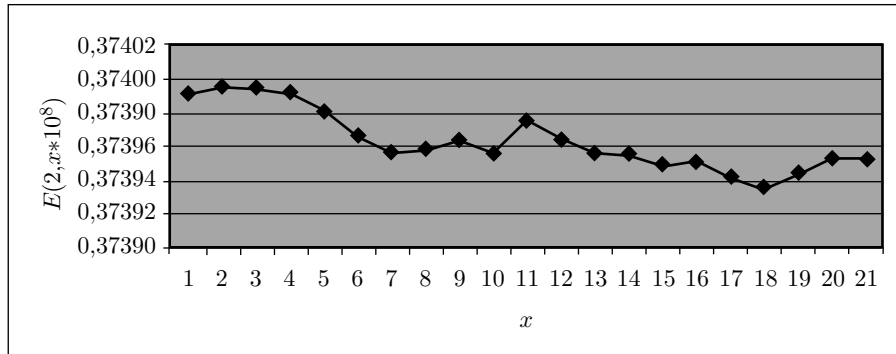


FIGURE 1. The natural density of primes with the least prime primitive root equal to 2

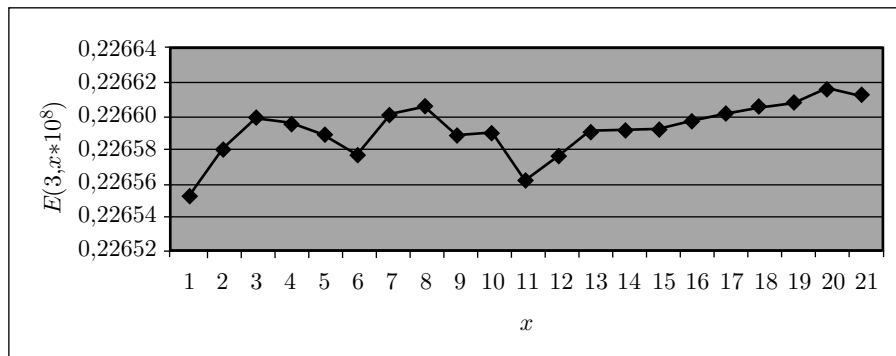


FIGURE 2. The natural density of primes with the least prime primitive root equal to 3

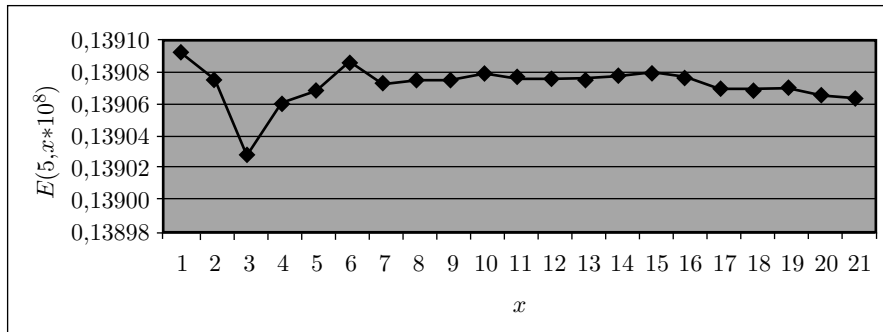


FIGURE 3. The natural density of primes with the least prime primitive root equal to 5

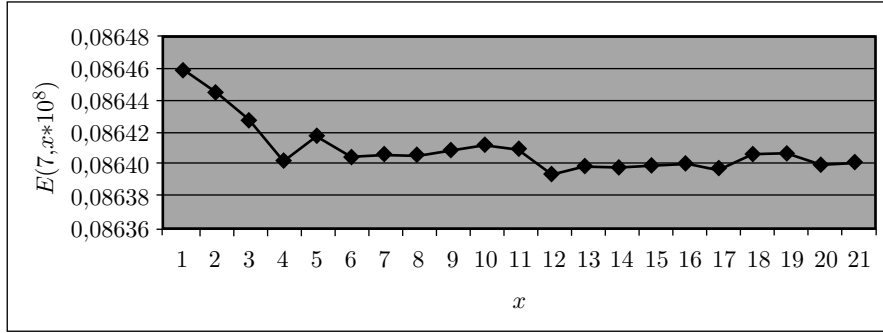


FIGURE 4. The natural density of primes with the least prime primitive root equal to 7

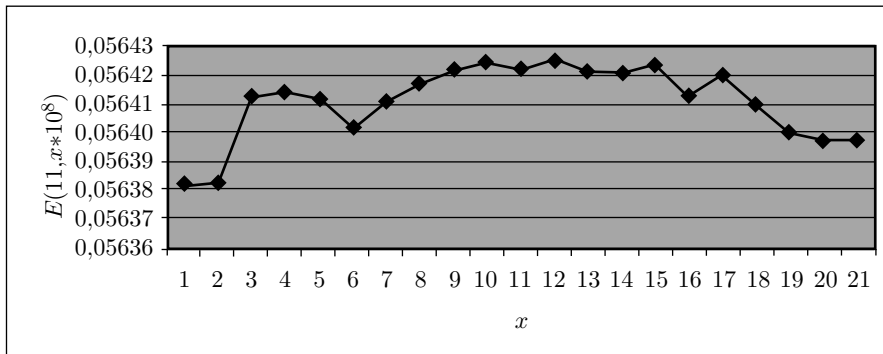


FIGURE 5. The natural density of primes with the least prime primitive root equal to 11

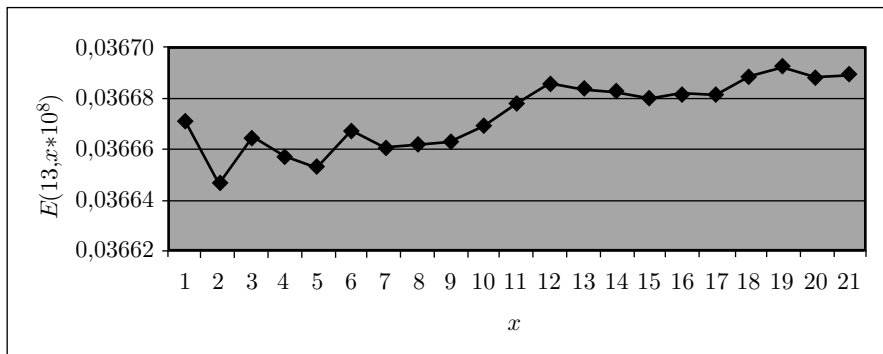


FIGURE 6. The natural density of primes with the least prime primitive root equal to 13

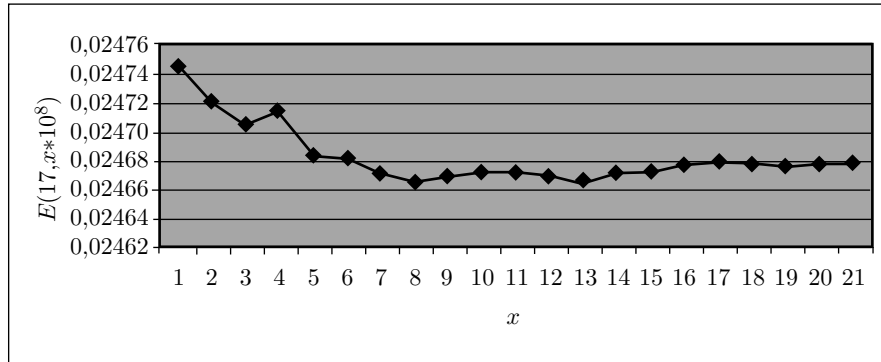


FIGURE 7. The natural density of primes with the least prime primitive root equal to 17

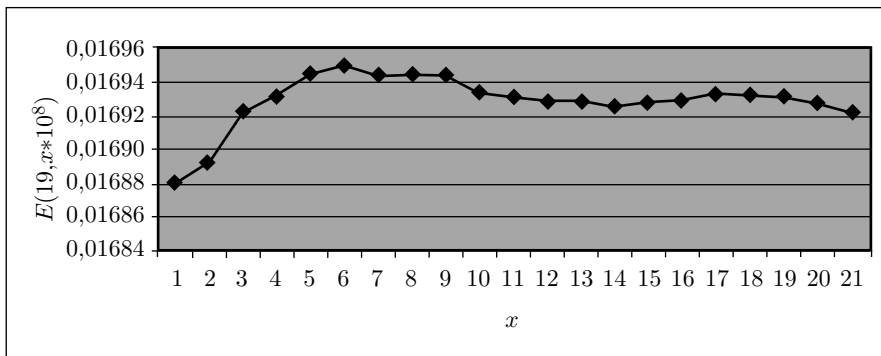


FIGURE 8. The natural density of primes with the least prime primitive root equal to 19

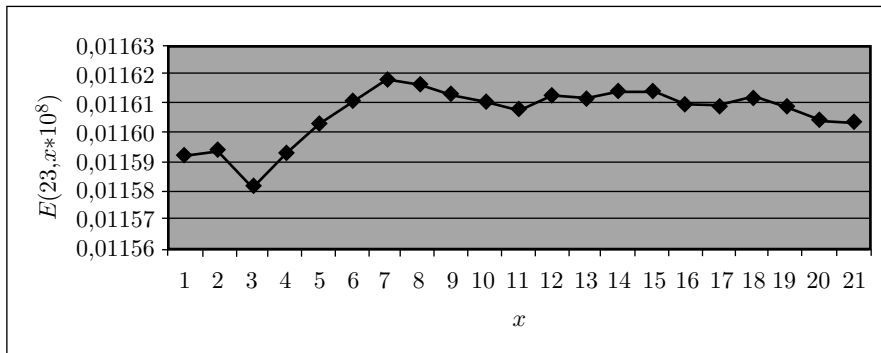


FIGURE 9. The natural density of primes with the least prime primitive root equal to 23

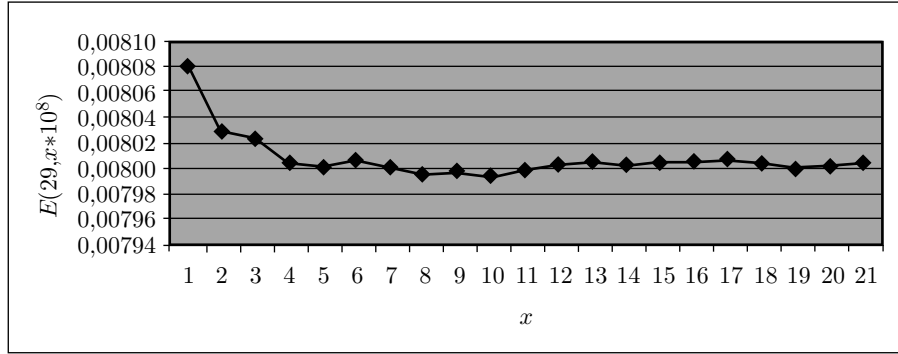


FIGURE 10. The natural density of primes with the least prime primitive root equal to 29

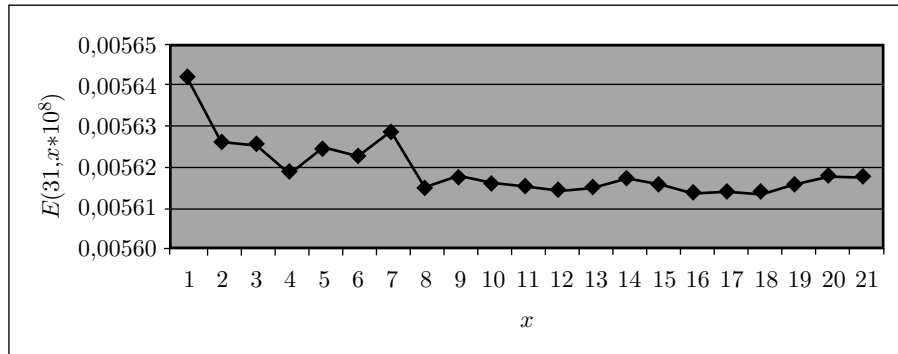


FIGURE 11. The natural density of primes with the least prime primitive root equal to 31

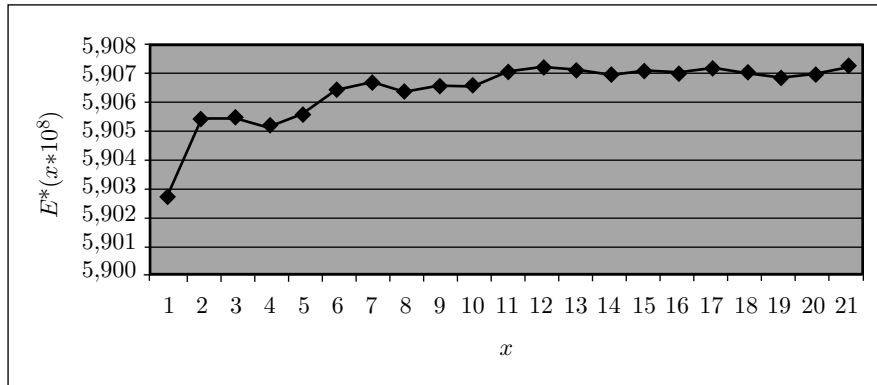


FIGURE 12. The average value  $E^*(x)$  of the least prime primitive root of primes  $\leq x$

TABLE 3. Average values  $E^*$  of least prime primitive roots of prime numbers (primitive roots of prime numbers) not exceeding  $x \cdot 10^8$

| $x$ | $E^*(x \cdot 10^8)$ | $x$ | $E^*(x \cdot 10^8)$ | $x$ | $E^*(x \cdot 10^8)$ |
|-----|---------------------|-----|---------------------|-----|---------------------|
| 1   | 5.9027080833        | 8   | 5.9063536374        | 15  | 5.9070799864        |
| 2   | 5.9054200778        | 9   | 5.9065722812        | 16  | 5.9070094456        |
| 3   | 5.9054950599        | 10  | 5.9066169463        | 17  | 5.9072094835        |
| 4   | 5.9052252014        | 11  | 5.9070787552        | 18  | 5.9071083838        |
| 5   | 5.9056411614        | 12  | 5.9072307772        | 19  | 5.9068949876        |
| 6   | 5.9064682273        | 13  | 5.9071263097        | 20  | 5.9070018498        |
| 7   | 5.9066463619        | 14  | 5.9069476033        | 21  | 5.9072779365        |

TABLE 4. The growth rate of least prime primitive roots

| $G(p)$ | $p$        | $\frac{G(p)}{\log p}$ | $\frac{G(p)}{\log^2 p}$ | $\frac{G(p)}{e^\gamma \log p (\log \log p)^2}$ |
|--------|------------|-----------------------|-------------------------|--|
| 2      | 3          | 1.820478              | 1.657070                | 115.559706                                     |
| 3      | 7          | 1.541695              | 0.792274                | 1.953084                                       |
| 5      | 23         | 1.594644              | 0.508578                | 0.685570                                       |
| 7      | 41         | 1.884977              | 0.507591                | 0.614838                                       |
| 11     | 109        | 2.344741              | 0.499801                | 0.551000                                       |
| 19     | 191        | 3.617481              | 0.688745                | 0.738260                                       |
| 43     | 271        | 7.675667              | 1.370136                | 1.451413                                       |
| 53     | 2791       | 6.679980              | 0.841927                | 0.874297                                       |
| 79     | 11971      | 8.412988              | 0.895928                | 0.941673                                       |
| 107    | 31771      | 10.321899             | 0.995715                | 1.059694                                       |
| 149    | 190321     | 12.256850             | 1.008257                | 1.102962                                       |
| 151    | 2080597    | 10.379315             | 0.713444                | 0.812905                                       |
| 163    | 3545281    | 10.808210             | 0.716671                | 0.824196                                       |
| 211    | 4022911    | 13.874717             | 0.912359                | 1.051558                                       |
| 223    | 73189117   | 12.314619             | 0.680044                | 0.824189                                       |
| 263    | 137568061  | 14.034429             | 0.748917                | 0.917462                                       |
| 277    | 443571241  | 13.912348             | 0.698748                | 0.873004                                       |
| 307    | 565822531  | 15.232866             | 0.755831                | 0.948147                                       |
| 347    | 1160260711 | 16.625214             | 0.796535                | 1.011101                                       |
| 349    | 1622723341 | 16.456541             | 0.775982                | 0.990421                                       |

TABLE 5. The least prime numbers  $p < 2^{31}$  and their least prime primitive roots

| $G(p)$ | $g(p)$ | $p$     | Factorization of $p - 1$    |
|--------|--------|---------|-----------------------------|
| 2      | 2      | 3       | 2                           |
| 3      | 3      | 7       | 2,3                         |
| 5      | 5      | 23      | 2,11                        |
| 7      | 6      | 41      | 2(3), 5                     |
| 11     | 6      | 109     | 2(2), 3(3)                  |
| 13     | 13     | 457     | 2(3), 3, 19                 |
| 17     | 17     | 311     | 2, 5, 31                    |
| 19     | 19     | 191     | 2, 5, 19                    |
| 23     | 10     | 2137    | 2(3), 3, 89                 |
| 29     | 21     | 409     | 2(3), 3, 17                 |
| 31     | 10     | 1021    | 2(2), 3, 5, 17              |
| 37     | 14     | 1031    | 2, 5, 103                   |
| 41     | 6      | 1811    | 2, 5, 181                   |
| 43     | 6      | 271     | 2, 3(3), 5                  |
| 47     | 6      | 14293   | 2(2), 3(2), 397             |
| 53     | 6      | 2791    | 2, 3(2), 5, 31              |
| 59     | 38     | 55441   | 2(4), 3(2), 5, 7, 11        |
| 61     | 12     | 35911   | 2, 3(3), 5, 7, 19           |
| 67     | 6      | 57991   | 2, 3, 5, 1933               |
| 71     | 22     | 221101  | 2(2), 3, 5(2), 11, 67       |
| 73     | 6      | 23911   | 2, 3, 5, 797                |
| 79     | 10     | 11971   | 2, 3(2), 5, 7, 19           |
| 83     | 69     | 110881  | 2(5), 3(2), 5, 7, 11        |
| 89     | 6      | 103091  | 2, 5, 13(2), 61             |
| 97     | 44     | 71761   | 2(4), 3, 5, 13, 23          |
| 101    | 6      | 513991  | 2, 3(2), 5, 5711            |
| 103    | 35     | 290041  | 2(3), 3, 5, 2417            |
| 107    | 10     | 31771   | 2, 3(2), 5, 353             |
| 109    | 14     | 448141  | 2(2), 3, 5, 7, 11, 97       |
| 113    | 33     | 2447761 | 2(4), 3, 5, 7, 31, 47       |
| 127    | 6      | 674701  | 2(2), 3, 5(2), 13, 173      |
| 131    | 10     | 3248701 | 2(2), 3, 5(2), 7(2), 13, 17 |
| 137    | 10     | 2831011 | 2, 3, 5, 7, 13, 17, 61      |
| 139    | 18     | 690541  | 2(2), 3, 5, 17, 677         |

TABLE 5. (continued)

|     |    |            |                               |
|-----|----|------------|-------------------------------|
| 149 | 14 | 190321     | 2(4), 3, 5, 13, 61            |
| 151 | 6  | 2080597    | 2(2), 3, 7, 17, 31, 47        |
| 157 | 33 | 4076641    | 2(5), 3(2), 5, 19, 149        |
| 163 | 14 | 3545281    | 2(6), 3(2), 5, 1231           |
| 167 | 33 | 11643607   | 2, 3(2), 13, 17, 2927         |
| 173 | 18 | 16135981   | 2(2), 3, 5, 7, 103, 373       |
| 179 | 94 | 5109721    | 2(3), 3, 5, 7(2), 11, 79      |
| 181 | 15 | 9633751    | 2, 3, 5(4), 7, 367            |
| 191 | 38 | 25400761   | 2(3), 3, 5, 7, 11, 2749       |
| 193 | 15 | 25738831   | 2, 3(3), 5, 13, 7333          |
| 197 | 22 | 399263281  | 2(4), 3, 5, 13, 73, 1753      |
| 199 | 6  | 37565431   | 2, 3, 5, 7, 41, 4363          |
| 211 | 6  | 4022911    | 2, 3(2), 5, 44699             |
| 223 | 6  | 73189117   | 2(2), 3(3), 7, 11, 13, 677    |
| 227 | 6  | 298155271  | 2, 3, 5, 7, 71, 19997         |
| 229 | 6  | 741488749  | 2(2), 3, 7, 11, 13, 61729     |
| 223 | 6  | 453507991  | 2, 3, 5, 13, 31, 37511        |
| 239 | 12 | 187155691  | 2, 3, 5, 1223, 5101           |
| 241 | 14 | 449032321  | 2(7), 3(2), 5, 11, 19, 373    |
| 251 | 22 | 672618871  | 2, 3(3), 5, 7, 11, 32353      |
| 257 | 10 | 794932741  | 2(2), 3(2), 5, 7, 630899      |
| 263 | 14 | 137568061  | 2(2), 3(2), 5, 7, 23, 47, 101 |
| 277 | 57 | 443571241  | 2(3), 3, 5, 7, 29, 131, 139   |
| 283 | 22 | 1095701881 | 2(3), 3, 5, 7, 13, 19, 5281   |
| 307 | 12 | 565822531  | 2, 3(3), 5, 7, 13, 23029      |
| 347 | 15 | 1160260711 | 2, 3, 5, 7(2), 17, 29, 1601   |
| 349 | 6  | 1622723341 | 2(2), 3, 5, 7, 1151, 2557     |

It is still an open problem whether  $E^*(x)$  tends to a constant value when  $x$  tends to infinity. Table 3 and the graph of the function  $E^*(x)$  for  $x < 2.1 \cdot 10^9$  (Figure 12) allow us to believe that  $E^*(x)$  will really tend to a constant.

With the aid of computer programs, the average values of least prime primitive roots were computed. Table 3 collects these values.

Table 4 registers the very first occurrence of a prime number as a least prime primitive root greater than the previous one. With the aid of the table one can approximate the growth rate of prime primitive roots. It can easily be seen that the growth rate of the least prime primitive root of primes is well approximated by small powers of logarithms of these primes.

E. Bach [2] surmises, giving probabilistic arguments, that

$$\limsup_{p \rightarrow \infty} \frac{G(p)}{\log p (\log \log p)^2} = e^\gamma,$$

where  $\gamma$  in the above formula is equal to the Euler constant  $0.5772\dots$

The validity of the above limit may be of great importance for practical purposes, e.g., for primality testing. The existence a small primitive root of a prime number is the basic assumption in many primality testing strategies.

Table 4 supports the correctness of Bach's computations. In the Table 5 we present minimal prime numbers  $p$  having prescribed least prime primitive roots  $q \leq 349$ , corresponding to  $G(p) = q$ , the least primitive root  $g(p)$ , and the factorization of  $p - 1$ . We see that all primes below 350 with the exception of 311, 313, 317, 331 and 337 occur as the least prime primitive root of a prime less than  $2^{31}$ .

### 3. CONCLUSIONS AND PROPOSALS FOR FUTURE INVESTIGATIONS

We derived a conditional formula for the natural density  $E(p_n)$  of prime numbers  $p$  having its least prime primitive root equal to  $p_n$ . For every prime number from the interval  $[3, 2147483647 (= 2^{31} - 1)]$  the least prime primitive root has been found. Under the generalized Riemann hypothesis, densities  $E(p_n)$  of prime numbers having their least prime primitive root equal to the prime  $p_n$ , where  $p_n < 100$ , were computed (Table 1). These values were compared with empirical values (Table 2). The agreement of both: theoretical and practical results are surprisingly good.

Relying on the computed material, the average value of the least prime primitive root has been found (Table 3).

It seems reasonable (Table 4) to majorize the value of the least prime primitive root of a prime by a constant multiple of the square of the natural logarithm of that prime. It would be useful to find a stronger theoretical estimate than that found by Ankeny [1] on the extended Riemann hypothesis, namely  $G(p) = O(Y^2 \log^2 Y)$ , where  $Y = 2^{\omega(p-1)} \log p$  and  $\omega(n)$  is the number of distinct prime factors of  $n$ . It is highly probable that the estimate can be improved to the form  $G(p) < \log^{1+\varepsilon} p$ , where  $\varepsilon$  can be any positive number as suggested by E. Bach.

We extended the investigations of least (unrestricted) primitive roots to the bound  $3 \cdot 10^{10}$ , but they were stopped because of highly time-consuming computations. The results will be submitted for publication in the near future. It would be very useful to extend the computations of least (prime) primitive roots for all primes  $p < 10^{11}$  or higher, but for this project much more powerful machines should be applied.

## ACKNOWLEDGMENTS

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

We are grateful to the anonymous referee for his valuable suggestions, including the formula for  $c_{m,n}$  and also for indicating papers [3], [7] and [8] which are somewhat related to our work. These references were not quoted in the original text.

## NOTE ADDED IN PROOF

The computation described in the paper has been carried further, up to the limit  $10^{12}$  by A. Paszkiewicz and  $10^{14}$  by Tomas Oliveira e Silva, University of Aveiro, Portugal.

## REFERENCES

1. N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) **55** (1952), 65–72. MR **13**:538c
2. E. Bach, *Comments on search procedures for primitive roots*, Math. Comp. **66** (1997), 1719–1727. MR **98a**:11187
3. L. Cangelmi, E. Pappalardi, *On the  $r$ -rank Artin Conjecture, II*, J. Number Theory **75** (1999), 120–132. MR **2000i**:11149
4. P. D. T. A. Elliott, L. Murata, *On the average of the least primitive root modulo  $p$* , J. London Math. Soc. (2) **56** (1997), 435–445. MR **98m**:11094
5. K. R. Matthews, *A generalisation of Artin's conjecture for primitive roots*, Acta Arith. **29** (1976), 113–146. MR **53**:313
6. W. Narkiewicz, *Elementary and analytic theory of algebraic number fields*, Warszawa, 1974, second ed. Warszawa 1990. MR **91h**:11107
7. F. Pappalardi, *On minimal sets of generators for primitive roots*, Canad. Math. Bull. **38** (1995), 465–468. MR **96k**:11120
8. F. Pappalardi, *On the  $r$ -rank Artin Conjecture*, Math. Comp. **66** (1967), 853–868. MR **97f**:11082
9. J. W. Wrench, Jr., *Evaluation of Artin's constant and the twin-prime constant*, Math. Comp. **5** (1961), 396–398. MR **23**:A1619

WARSAW UNIVERSITY OF TECHNOLOGY, DIVISION OF TELECOM FUNDAMENTALS, 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@plearn.edu.pl`