MOSCOW MATHEMATICAL JOURNAL
Volume 15, Number 2, April–June 2015, Pages 283–291

A NOTE ON ARTIN'S CONSTANT

IVAN CHEREDNIK

To Borya Feigin with admiration and best wishes on the occasion of his 60th birthday

Abstract. We suggest new heuristic summation formulas for the Artin constant and its analogs in higher ranks, for the density of prime numbers p such that a given set of integers generates the corresponding multiplicative groups modulo powers of p. Depending on the choice of these integers, certain interesting rational corrections emerge, which are calculated in rank one case. The rate of convergence of these sums to the corresponding constants, connected with the generalized Riemann Hypothesis, is analyzed numerically. We also discuss the Stephens constant.

2010 Math. Subj. Class. 11M06, 11N69, 11Z05.

Key words and phrases. Artin constant, Riemann hypothesis.

We suggest a representation of Artin's constant, which conjecturally describes the density of prime p such that "generic" $g \in \mathbb{Z}$ is primitive modulo p. Namely, $A = \lim_{N\to\infty} R_k(N)$ for $R_k(N) = \frac{\sum p^k \phi(p_i-1)}{\sum p^k(p_i-1)}$, where the summation is over first N prime p_i, $k \in \mathbb{Z}_+$. The classical summation formula is as follows: $A = \lim_{N\to\infty} \Sigma(N)$, where $\Sigma(N) = \frac{1}{N}\sum \frac{\phi(p_i-1)}{p_i-1}$. The changes needed for arbitrary g are addressed in Theorem 1, a good exercise in basic analytic and algebraic number theory. The same procedure can be applied to other number-theoretic constants like A (see for example [Ni]). In Theorem 2, we demonstrate how it works for the Stephens constant and for Artin's constants of higher ranks (for the density of prime p such that a given set of "generic" integers generates $\mathbb{Z}_p^*$).

The following three features of this approach vs. the summation formulas are worth noticing.

1) The *restricted summation* suggested by P. Moore to make the Σ-formula matching the right heuristic density for arbitrary $g \in \mathbb{Z}$ gives the desired answer in our approach only when g is not a pure (odd) power in $\mathbb{Z}$. Otherwise, *nontrivial* rational multiplicative corrections occur; they are provided in Theorem 1, (ii).

2) The p^k*-terms* in the denominator and numerator of $R_k(N)$ do not influence the limit, which can be heuristically associated with switching from primitive roots

Supported in part by NSF grant DMS-1101535.

in $\mathbb{Z}_p$ to those in $(\mathbb{Z}/(p^{k+1}))^*$. The extra p^k-factors disappear (cancel) in the corresponding summation formula. When $k=0$, our R-formula for A (without restricting the summation) follows from [Pi].

3) The R-formulas oscillate significantly around A (and the other constants). The magnitude of *oscillations* increases as k grows; see Figure 1. Representing $R_k(N)=\sum_{i=1}^N w_i\frac{\phi(p_i-1)}{p_i-1}$, the weights w_i change from $O\big(\frac{\log N}{N^{k+2}}\big)$ for small i to $O\big(\frac{(\log N)^{k+1}}{N}\big)$ for $i\sim N$. Thus, large p receive greater weights in our approach, especially when k is large, which increases the range of oscillations.

1. Brief history. Artin's primitive root conjecture states that given an integer g, possibly negative but not a perfect square in $\mathbb{Z}$, the number $\mathcal{P}_N(g)$ of prime p among $p_1=2$, $p_2=3$, $\dots$, p_N such that g is primitive modulo p approaches asymptotically $A(g)N$ as $N\to\infty$ for

$$A(g)=A_h\,A_d, \tag{1}$$

$$A_d=\Big(1-\mu(|d|)\prod_{p|d,\,p|h}\frac{1}{p-2}\prod_{p|d,\,p\nmid h}\frac{1}{p^2-p-1}\Big),$$

$$A_h=\prod_{p|h}\Big(1-\frac{1}{p-1}\Big)\prod_{p\nmid h}\Big(1-\frac{1}{p(p-1)}\Big),$$

where $d=$ Discriminant $(\mathbb{Q}[\sqrt{g}])$, $g=g_o^h$ for $g_o\in\mathbb{Z}$ and maximal $h\in\mathbb{N}$.

Note that $\mu(|d|)=0$ and, respectively, $A(g)=A_h$ if and only if the discriminant d is not from $1+4\mathbb{Z}$. If $h=1$ for such g, then $A(g)$ equals

$$\text{Artin's constant}=A=\prod_{\text{prime }p}\Big(1-\frac{1}{p(p-1)}\Big). \tag{2}$$

According to [St], Artin's conjecture was finalized around 1965. In 1967, it was deduced by Hooley [Ho] from the generalized Riemann hypothesis for the fields $K_m=\mathbb{Q}[\zeta_m,\,g^{1/m}]$ for squarefree m. See [Mo1] for a comprehensive introduction (including some recent developments). See also [Mu], [Le].

Artin's heuristic approach to this conjecture was based on the expectation that events "*prime p does not split completely in K_q for prime q*" are independent (subject to later qualitative and quantitative corrections). For instance, one can expect that A equals $\lim_{N\to\infty}\mathcal{P}_N(g)/N$ if g is *generic* as far as primitive roots modulo prime p are concerned. It leads to the following heuristic summation formula for Artin's constant:

$$A=\lim_{N\to\infty}\Sigma(N),\quad \Sigma(N)=\frac{1}{N}\sum_{i=1}^{N}\frac{\phi(p_i-1)}{p_i-1}, \tag{3}$$

which can be checked unconditionally, without any reference to Artin's conjecture. See [LL], [Mo1]. P. Moore extended it to arbitrary $A(g)$ by switching to p in this summation such that g is a quadratic nonresidue modulo p and $(p-1,\,h)=1$ (heuristically, it makes sense); see below.

As Lehmers wrote, the convergence in (3) is "discouragingly slow" (they considered prime numbers $p<1500000$). It remains very slow when prime numbers

in much greater ranges are considered, generally, no better than the (conjectural) convergence of $\mathcal{P}_N(2)/N$ to $A = A(2)$; cf. Table "Artin's constant estimates" from [Si] ($p < 10^{14}$).

2. Main Theorem. A refined version of this heuristic approach is from [Mo1] (for any integer g):

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \varphi_g(p_i) = A(g) \quad (\overset{\text{RH}}{=} \lim_{N\to\infty} \mathcal{P}_N(g)/N), \tag{4}$$

where

$$\varphi_g(p) \overset{\text{def}}{=} 2\,\frac{\phi(p-1)}{p-1} \quad \text{for } \left(\frac{g}{p}\right) = -1 \text{ and } (p-1,\, h) = 1,$$

$$\varphi_g(p) \overset{\text{def}}{=} 0 \quad \text{otherwise.}$$

Heuristically, it is equally reasonable to expect that

$$A = \lim_{N\to\infty} \frac{\sum_{i=1}^{N} \phi(p_i - 1)}{\sum_{i=1}^{N} (p_i - 1)} \tag{5}$$

for sufficiently general g. Switching here to the restricted summation from (4), we come to the following theorem.

Theorem 1. (i) *For arbitrary integers $k \geqslant 0$ and g (possibly, negative),*

$$A(g) = \lim_{N\to\infty} \frac{\sum_{i=1}^{\prime N} p_i^k \phi(p_i - 1)}{\sum_{i=1}^{\prime N} p_i^k (p_i - 1)}, \tag{6}$$

provided that $h = 1$, where the summation Σ' is over prime p_i such that $\left(\frac{g}{p_i}\right) = -1$ and $(p_i - 1,\, h) = 1$.

(ii) *If $h > 1$, then the limit in the r.h.s. of (6) equals*

$$\widetilde{A}(g) = \widetilde{A}_h\, \widetilde{A}_d, \tag{7}$$

where

$$\widetilde{A}_h = \prod_{p \nmid h} \Big(1 - \frac{1}{p(p-1)}\Big), \quad \widetilde{A}_d = 1 \text{ if } d \mid h \text{ and } \widetilde{A}_d = A_d \text{ otherwise.}$$

Sketch of proof. We follow [LL], [Mo1], restricting ourselves with (5); see also [Pi]. Coupling the generalized Landau formula from [ŚZ]

$$\sum_{p \leqslant x} p^m = \frac{(1 + o(1))\, x^{m+1}}{(1+m)\log x}, \quad m \geqslant 0, \tag{8}$$

with the classical estimate

$$\frac{\pi(x,\, d,\, 1)}{\pi(x)} = \frac{1 + O(1/\log x)}{\phi(d)}, \tag{9}$$

where $\pi(x,\, d,\, 1)$ is the number of prime numbers $p \leqslant x$ in $1 + d\mathbb{N}$ ($\pi(x) = \pi(x,\, 1,\, 1)$), one arrives at:

$$\frac{\pi^{(m)}(x,\, d,\, 1)}{\pi^{(m)}(x)} = \frac{1 + O(x^m/\log x)}{\phi(d)}, \tag{10}$$

where $\pi^{(m)}(x,\,d,\,1)=\sum_{p\leqslant x}p^m$ over prime $p\in 1+d\,\mathbb{N}$. Then,

$$\sum_{p\leqslant x}\phi(p-1)=\sum_{p\leqslant x}\sum_{d|p-1}(p-1)\frac{\mu(d)}{d}$$
$$=\sum_{d|p-1}\frac{\mu(d)}{d}\sum_{p\leqslant x}(p-1)=\sum_{d\leqslant x}\frac{\mu(d)}{d}(\pi^{(1)}(x,\,d,\,1)-\pi(x,\,d,\,1)).$$

Finally,

$$\frac{\sum_{p\leqslant x}\phi(p-1)}{\sum_{p\leqslant x}(p-1)}\sim\sum_{d\leqslant x}\frac{\mu(d)}{d\phi(d)}\xrightarrow{x\to\infty}A.$$

We will omit the arguments (from the basic algebraic number theory) that give the rational corrections for arbitrary g. □

In (5), (6), only the leading powers of p_i matter; for instance, one can take here the ratio $\sum_p\phi(\phi(p^{k+1}))/\sum_p\phi(p^{k+1})$, the heuristic probability for g being a primitive root modulo p^{k+1} over all prime p, which leads to the same Artin constant.

3. Further examples. Let us apply the same procedure to Stephens' constant $S(a,\,b)$ and the higher rank Artin constants. The former is defined for a given pair $a,\,b\in\mathbb{Q}^*$ such that $a^rb^s=1\Rightarrow r=0,\,s=0$ for $r,\,s\in\mathbb{Z}$; it describes the density of primes p such that $b=a^m \mod p$ for some $m\in\mathbb{Z}$. Modulo the generalized Riemann hypothesis, it equals

$$C_{ab}\,S\quad\text{for}\quad S\stackrel{\text{def}}{=}\prod_{i=1}^{\infty}\Big(1-\frac{p_i}{p_i^3-1}\Big),$$

where the factors C_{ab} are rational [S], [MS]. These factors were calculated explicitly in [MS] under the condition that the group $\mathbb{Q}^*/\langle a,\,b,\,-1\rangle$ is torsion free. Assuming that $a,\,b$ are "random", the heuristic probability $PS(p)$ that $b=a^m \mod p$ for some m can be readily calculated:

$$PS(p)=\mathcal{S}(p)/(p-1)^2,\tag{11}$$

where

$$\mathcal{S}(p)\stackrel{\text{def}}{=}\sum_{d|p-1}d\phi(d)=\prod_{j=1}^{m}\frac{q_j^{2k_j+1}+1}{q_j+1}\text{ for prime factorization }p-1=\prod_{j=1}^{m}q_j^{k_j}.$$

We naturally omit the prime numbers that divide the numerators or denominators of $a,\,b$.

The rank r Artin constant $A_r(g_1,\,\dots,\,g_r)$ describes the heuristic density of primes p such that a given set of nonzero integers $\{g_1,\,\dots,\,g_r\}$ (or rationals) generates $\mathbb{Z}_p^*$. See [CP]. Its "generic" value (modulo the generalized Riemann hypothesis) is as follows:

$$A_r\stackrel{\text{def}}{=}\prod_{i=1}^{\infty}\Big(1-\frac{1}{p_i^r(p_i-1)}\Big).\tag{12}$$

The corresponding probability at p for "random" $g_1, \ldots, g_r$ equals

$$PA_r(p) = \mathcal{A}_r(p)/(p-1)^r \quad \text{for} \quad \mathcal{A}_r(p) \stackrel{\text{def}}{=} \prod_{j=1}^{m} (q_j^{rk_j} - q_j^{r(k_j-1)}) \tag{13}$$

in terms of the prime factorization $p-1 = \prod_{j=1}^{m} q_j^{k_j}$.

The summation (unconditional) limiting formulas are as follows:

$$S = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} PS(p_i), \qquad A_r = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} PA_r(p_i). \tag{14}$$

The proof of the following theorem is similar to that of Theorem 1.

Theorem 2. *For an arbitrary integer $k \geqslant 0$,*

$$S = \lim_{N\to\infty} \frac{\sum_{i=1}^{N} p_i^k \, \mathcal{S}(p_i)}{\sum_{i=1}^{N} p_i^k \, (p_i-1)^2}, \tag{15}$$

$$A_r = \lim_{N\to\infty} \frac{\sum_{i=1}^{N} p_i^k \, \mathcal{A}_r(p_i)}{\sum_{i=1}^{N} p_i^k \, (p_i-1)^r}, \tag{16}$$

where the summation is over consecutive prime numbers p_i. □

4. Numerical aspects. For the constants C considered above, we plot $\frac{\Sigma(N)}{C} - 1$, shown thin, for the classical summation $\Sigma(N)$ and $\frac{R(N)}{C} - 1$, which are thick, for our ratio approximations $R(N)$; for instance, $\Sigma(N)$ is from (3) for Artin's A. The range is $N \leqslant 1000\text{M}$.

Figure 1 compares the stabilization of (3), thin, to the Artin constant and the stabilization of (5), thick, as $k = 0, 1$. The function $\Sigma(N) - A$ remains positive in the range $N \leqslant 1000\text{M}$; $R_k(N)$ oscillate around Artin's constant $A \approx 0.37395581361920228805$ (the zero level of this graph). The amplitude of oscillations become larger for $R_{k=1}$ vs. $R_{k=0}$, however the graphs are very much similar.

We note that the best way to calculate A and similar constants is based on the known product formulas in terms of $\zeta(n)$ for integers $n > 1$.

Figure 2 shows the convergence of (4) and (6) to $A(g=5)$ for $k=0$; notice that the thin curve remains beyond the thick one in this range.

The last two plots show the graphs for the Stephen constant

$$S \approx 0.57595996889294543964 \quad \text{(Figure 3)},$$

and the rank 3 Artin constant

$$A_3 \approx 0.85654044485354217443 \quad \text{(Figure 4)};$$

here $k = 0$. The convergence rate and other features of these four graphs are similar to those for A and $A(5)$. There is striking (qualitative) similarity of these two figures, including the oscillations, although the convergence rate in Figure 4 (for A_3) is significantly (almost 10 times) greater than in Figure 3.

Qualitatively, the behavior of $R(N)$ for large N can be evaluated following [Pi]. For instance, the functions $|R(N)/A - 1|$ in Figure 1 must be no greater than $C_m(\log N)^{-m}$ for *any* fixed $m > 0$ and proper constant C_m (depending on k) as

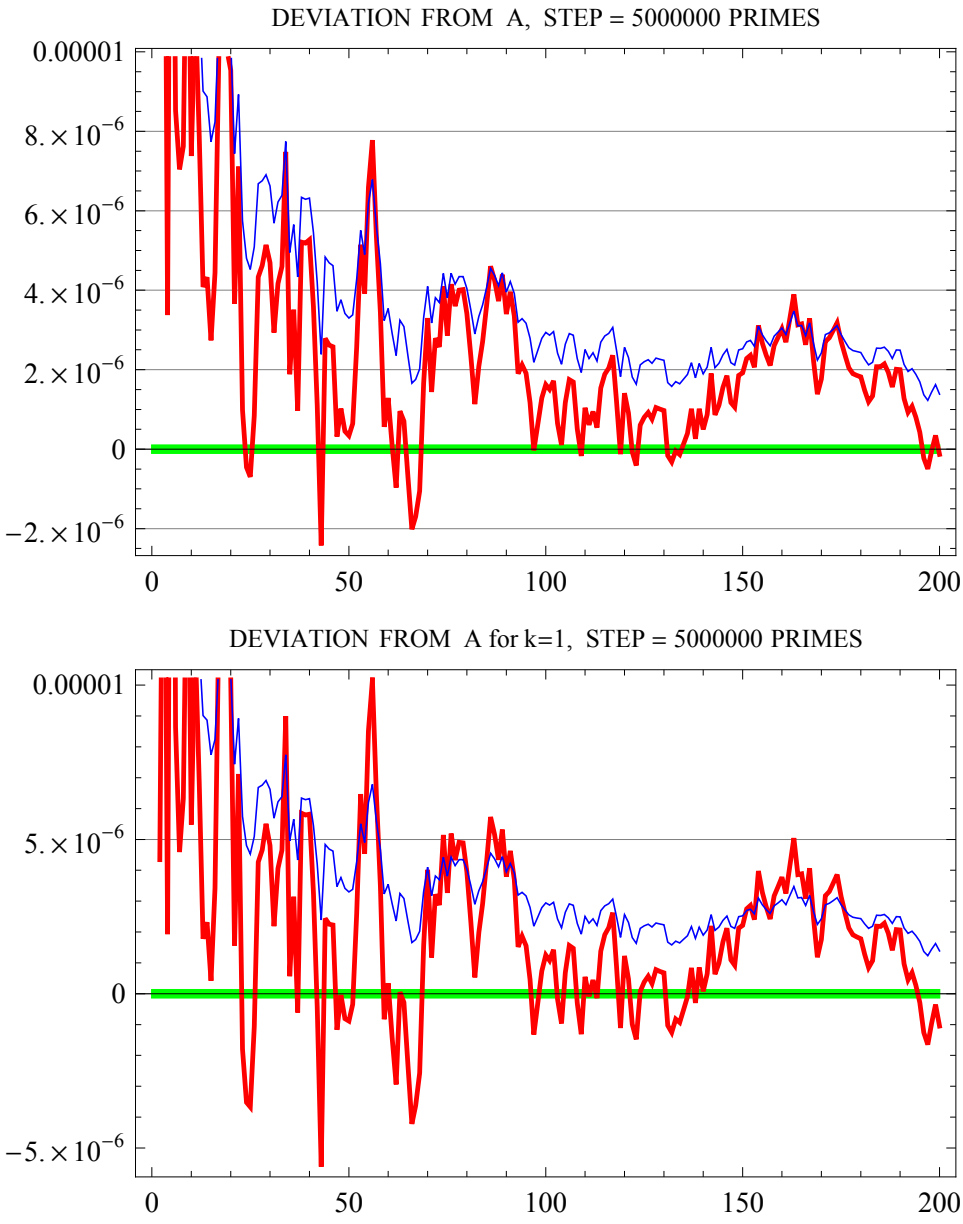

FIGURE 1. Deviation from A as $k = 0, 1$ for 1000M primes

$N \gg 0$. Generally speaking, C_m can be estimated in terms of (the order of) N, but we will not discuss it. Indeed, the graphs of $R(N)/A - 1$, thick from Figure 1, look like $O((\log N)^{-4})$ in the range $N < 1000$M.

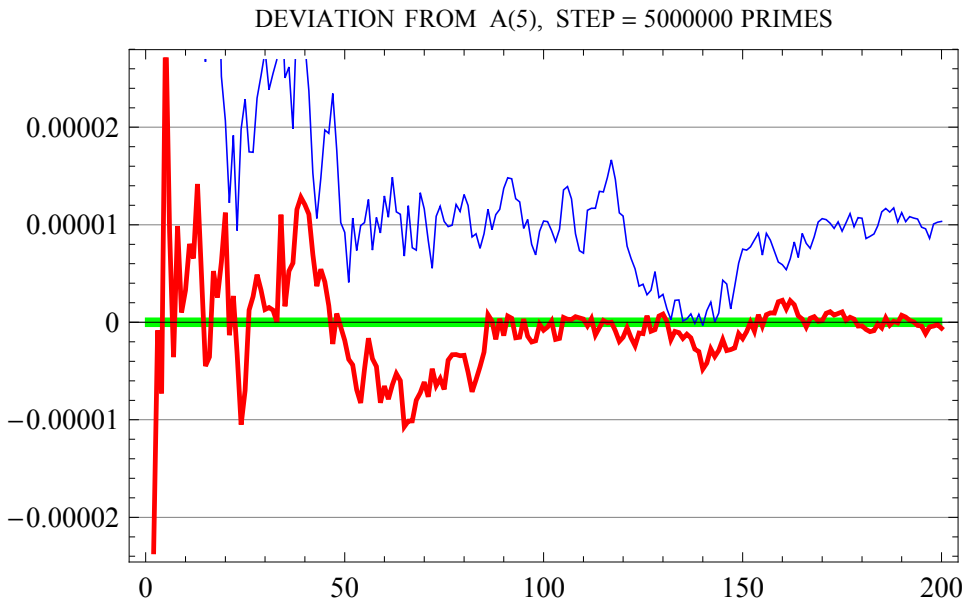

FIGURE 2. Deviation from $A(5)$ for 1000M primes

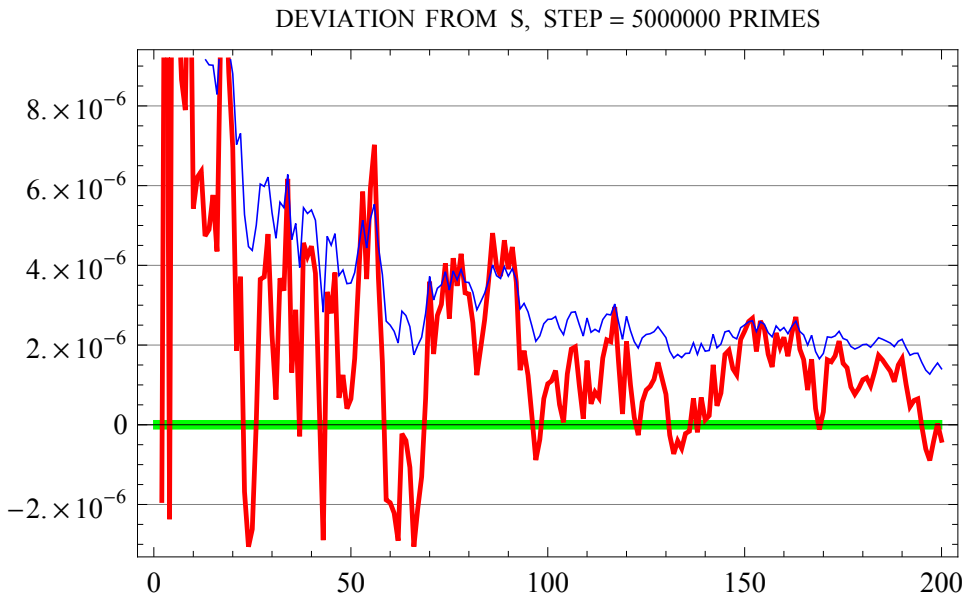

FIGURE 3. Deviation from S for 1000M primes

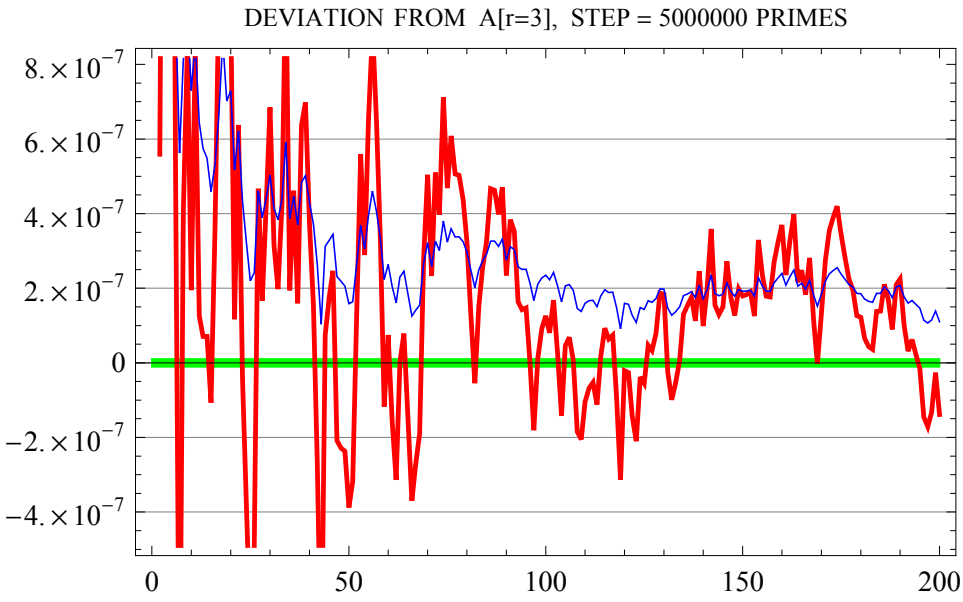

FIGURE 4. Deviation from A_3 (rank $= 3$) for 1000M primes

The nature of oscillations of the functions $R(N)$ around the corresponding constants remains unclear.

Acknowledgements. I am grateful to Zeev Rudnik for valuable comments. I am very thankful to Pieter Moree for reading the note, suggesting interesting questions toward comparing our approach with the results from [Mo2], [Mo3] and for the reference to [Pi].

REFERENCES

[CP] L. Cangelmi and F. Pappalardi, *On the r-rank Artin conjecture. II*, J. Number Theory **75** (1999), no. 1, 120–132. MR 1677559

[Ho] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR 0207630

[LL] D. H. Lehmer and E. Lehmer, *Heuristics, anyone?*, Studies in mathematical analysis and related topics, Stanford Univ. Press, Stanford, Calif., 1962, pp. 202–210. MR 0144868

[Le] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224. MR 0480413

[Mo1] P. Moree, *Artin's primitive root conjecture — a survey*, preprint arXiv:math/0412262 [math.NT].

[Mo2] P. Moree, *Asymptotically exact heuristics for (near) primitive roots*, J. Number Theory **83** (2000), no. 1, 155–181. MR 1767657

[Mo3] P. Moree, *Asymptotically exact heuristics for (near) primitive roots. II*, Japan. J. Math. (N.S.) **29** (2003), no. 2, 143–157. MR 2035537

[MS] P. Moree and P. Stevenhagen, *A two-variable Artin conjecture*, J. Number Theory **85** (2000), no. 2, 291–304. MR 1802718

[Mu] M. R. Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), no. 4, 59–67. MR 966133

[Ni] G. Niklasch, *Some number-theoretical constants arising as products of rational functions of p over primes*, Preprint http://www.gn-50uma.de/alula/essays/Moree/Moree.en.shtml, 2002.

[Pi] S. S. Pillai, *On the sum function connected with primitive roots*, Proc. Indian Acad. Sci., Sect. A. **13** (1941), 526–529. MR 0004834

[Si] T. Oliveira e Silva, *Least primitive root of prime numbers*, preprint http://www.ieeta.pt/~tos/p-roots.html, 2004.

[ŠZ] T. Šalát and Š. Znám, *On sums of the prime powers*, Acta Fac. Rerum Natur. Univ. Comenian. Math. **21** (1968), 21–24 (1969). MR 0266888

[S] P. J. Stephens, *Prime divisors of second-order linear recurrences*, J. Number Theory **8** (1976), no. 3, 313–345. MR 0417081, MR 0417082

[St] P. Stevenhagen, *The correction factor in Artin's primitive root conjecture*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 383–391. MR 2019022. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

Department of Mathematics, UNC Chapel Hill, North Carolina 27599, USA
E-mail address: chered@email.unc.edu