Journal of Integer Sequences, Vol. 9 (2006),
Article 06.2.8

Asymptotically Exact Heuristics for Prime Divisors of the Sequence $\{a^k + b^k\}_{k=1}^{\infty}$

Pieter Moree[1]
Korteweg-de Vries Instituut
Plantage Muidergracht 24
1018 TV Amsterdam
The Netherlands
moree@science.uva.nl

Abstract

Let $N_{a,b}(x)$ count the number of primes $p \le x$ with p dividing $a^k + b^k$ for some $k \ge 1$. It is known that $N_{a,b}(x) \sim c(a,b)x/\log x$ for some rational number $c(a,b)$ that depends in a rather intricate way on a and b. A simple heuristic formula for $N_{a,b}(x)$ is proposed and it is proved that it is asymptotically exact, i.e., has the same asymptotic behavior as $N_{a,b}(x)$. Connections with Ramanujan sums and character sums are discussed.

1 Introduction

Let p be a prime (indeed, throughout this note the letter p will be used to indicate primes). Let g be a non-zero rational number. By $\nu_p(g)$ we denote the exponent of p in the canonical factorization of g. If $\nu_p(g) = 0$, then by $\mathrm{ord}_g(p)$ we denote the smallest positive integer k such that $g^k \equiv 1 \pmod{p}$. If $k = p - 1$, then g is said to be a *primitive root* mod p. If g is a primitive root mod p, then g^j is a primitive root mod p iff $\gcd(j, p-1) = 1$. There are thus $\varphi(p-1)$ primitive roots mod p in $(\mathbb{Z}/p\mathbb{Z})^*$, where φ denotes Euler's totient function.

Let $\pi(x)$ denote the number of primes $p \le x$ and $\pi_g(x)$ the number of primes $p \le x$ such that g is a primitive root mod p. Artin's celebrated primitive root conjecture (1927) states that if g is an integer with $|g| > 1$ and g is not a square, then for some positive rational number c_g we have $\pi_g(x) \sim c_g A\pi(x)$, as x tends to infinity. Here A denotes *Artin's constant*

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\cdots$$

[1]Author's current address: Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany. E-mail: moree@mpim-bonn.mpg.de .

Hooley [3] established Artin's conjecture and explicitly evaluated c_g, under assumption of the Generalized Riemann Hypothesis (GRH).

It is an old heuristic idea that the behavior of $\pi_g(x)$ should be mimicked by $H_1(x) = \sum_{p\le x} \varphi(p-1)/(p-1)$, the idea being that the 'probability' that g is a primitive root mod p equals $\varphi(p-1)/(p-1)$ (since this is the density of primitive roots in $(\mathbb{Z}/p\mathbb{Z})^*$). Using the Siegel-Walfisz theorem (see Lemma 1 below), it is not difficult to show, unconditionally, that $H_1(x) \sim A\pi(x)$. Although true for many g and also on average, it is however not always true, under GRH, that $\pi_g(x) \sim H_1(x)$, i.e., the heuristic $H_1(x)$ is not always asymptotically exact. Nevertheless, Moree [6] found a modification, $H_2(x)$, of the above heuristic $H_1(x)$ involving the Legendre symbol that is always asymptotically exact (assuming GRH).

A prime p is said to divide a sequence S of integers, if it divides at least one term of the sequence S (see [1] for a nice introduction to this topic). Several authors studied the problem of characterizing (prime) divisors of the sequence $\{a^k + b^k\}_{k=1}^{\infty}$. Hasse [2] seems to have been the first to consider the Dirichlet density of prime divisors of such sequences. Later authors, e.g., Odoni [11] and Wiertelak strengthened the analytic aspects of his work, with the strongest result being due to Wiertelak [14]. In particular, Theorem 2 of Wiertelak [14], in the formulation of [5], yields the following corollary (recall that $\mathrm{Li}(x) = \int_2^x dt/\log t$ is the logarithmic integral):

Theorem 1. *Let a and b be non-zero integers. Let $N_{a,b}(x)$ count the number of primes $p \le x$ that divide some term $a^k + b^k$ in the sequence $\{a^k + b^k\}_{k=1}^{\infty}$. Put $r = a/b$. Assume that $r \neq \pm 1$. Let λ be the largest integer such that $|r| = u^{2^\lambda}$, with u a rational number. Let $\varepsilon = \mathrm{sgn}(r)$ and $L = \mathbb{Q}(\sqrt{u})$. We have*

$$N_{a,b}(x) = \delta(r)\mathrm{Li}(x) + O\left(\frac{x(\log\log x)^4}{\log^3 x}\right),$$

where the implied constant may depend on a and b, and $\delta(r)$ is a positive rational number that is given in Table 1.

L	λ	$\delta(r)$ if $\varepsilon = +1$	$\delta(r)$ if $\varepsilon = -1$
$L \neq \mathbb{Q}(\sqrt{2})$	$\lambda \ge 0$	$2^{1-\lambda}/3$	$1 - 2^{-\lambda}/3$
$L = \mathbb{Q}(\sqrt{2})$	$\lambda = 0$	$17/24$	$17/24$
$L = \mathbb{Q}(\sqrt{2})$	$\lambda = 1$	$5/12$	$2/3$
$L = \mathbb{Q}(\sqrt{2})$	$\lambda \ge 2$	$2^{-\lambda}/3$	$1 - 2^{-1-\lambda}/3$

Table 1: The value of $\delta(r)$

Theorem 1 implies that if a and b are non-zero integers such that $a \neq \pm b$, then asymptotically $N_{a,b}(x) \sim \delta(r)x/\log x$ with $\delta(r) > 0$ (thus the constant $c(a,b)$ mentioned in the introduction equals $\delta(r)$). In particular, the set of prime divisors of the sequence $\{a^k + b^k\}_{k=1}^{\infty}$ has a positive natural density.

A starting point in the proof of Theorem 1 is the observation that $p \nmid 2ab$ divides the sequence $\{a^k + b^k\}_{k=1}^{\infty}$ iff $\mathrm{ord}_r(p)$ is even, where $r = a/b$. The condition that $\mathrm{ord}_r(p)$ be even is weaker than the condition that $\mathrm{ord}_r(p) = p-1$ and now the analytic tools are strong enough to establish an unconditional result.

Note that $\delta(r)$ does not depend on ε in case $\lambda = 0$. For a 'generic' choice of a and b, L will be different from $\mathbb{Q}(\sqrt{2})$ and λ will be zero and hence $\delta(a/b) = 2/3$. It is not difficult to show [9] that the average density of elements of even order in a finite field of prime cardinality also equals $2/3$.

In this note analogs $H^{(1)}_{a,b}(x)$ and $H^{(2)}_{a,b}(x)$ of $H_1(x)$ and $H_2(x)$ will be introduced and it will be shown that $H^{(2)}_{a,b}(x)$ is always asymptotically exact. This leads to the following main result (where $\pi(x;k,l)$ denotes the number of primes $p \le x$ satisfying $p \equiv l \pmod{k}$ and $(*/p)$ denotes the Legendre symbol):

Theorem 2. *Let a and b be non-negative natural numbers. Put $r = a/b$ and $\varepsilon = \mathrm{sgn}(a/b)$. Assume that $r \ne \pm 1$. Let h be the largest integer such that $|r| = r_0^h$ for some $r_0 \in \mathbb{Q}$ and $h \ge 1$. Put $e = \nu_2(h)$. If $\varepsilon = 1$, then*

$$N_{a,b}(x) = \pi(x; 2^{e+1}, 1) - 2^{e+1} \sum_{\substack{p \le x,\ (r_0/p)=1 \\ \nu_2(p-1) > e}} 2^{-\nu_2(p-1)} + O\left(\frac{x(\log\log x)^4}{\log^3 x}\right),$$

and if $\varepsilon = -1$, then

$$N_{a,b}(x) = \pi(x) - \sum_{\substack{p \le x,\ (r_0/p)=-1 \\ \nu_2(p-1) = e+1}} 1 - 2^{e+1} \sum_{\substack{p \le x,\ (r_0/p)=1 \\ \nu_2(p-1) > e+1}} 2^{-\nu_2(p-1)} + O\left(\frac{x(\log\log x)^4}{\log^3 x}\right),$$

where the implied constants depend at most on a and b. In the latter three sums it is required in addition that $p \nmid 2ab$.

Numerical work, cf. Table 2, suggests that the main term in Theorem 2 approximates $N_{a,b}(x)$ better than $\delta(r)\mathrm{Li}(x)$ (or $\delta(r)\pi(x)$ for that matter). It also suggests that the error term $O(x(\log\log x)^4 \log^{-3} x)$ is far from being sharp. Indeed, assuming GRH one can prove a much better result.

Theorem 3. (GRH). *The error term in both Theorem 1 and 2 is of magnitude $\sqrt{x}\log^{\omega(d)+1} x$, where $\omega(d)$ denotes the number of distinct prime divisors of d and the implied constant depends at most on a and b.*

The result that, under GRH, we have

$$N_{a,b}(x) = \delta(r)\mathrm{Li}(x) + O(\sqrt{x}\log^{\omega(d)+1} x), \tag{1}$$

was established by the author in an earlier paper [10].

2 Preliminaries

The proof of Theorem 2 requires a result from analytic number theory: the Siegel-Walfisz theorem, see e.g., [12, Satz 4.8.3]. For notational convenience we write (a,b) instead of $\gcd(a,b)$.

Lemma 1. *Let $C>0$ be arbitrary. There exists $c_1>0$ such that*

$$\pi(x;k,l)=\frac{\mathrm{Li}(x)}{\varphi(k)}+O(xe^{-c_1\sqrt{\log x}}),$$

uniformly for $1\le k\le \log^C x$, $(l,k)=1$, where the implied constant depends at most on C.

We will also make use of the Chebotarev density theorem, which we recall now. Let $L/\mathbb{Q}$ be a finite Galois extension of degree n_L and with discriminant d_L. Let $\pi_1(x;L/\mathbb{Q})$ denote the number of primes $p\le x$ such that p splits completely in $L/\mathbb{Q}$. The Chebotarev density theorem asserts that

$$\pi_1(x;L/\mathbb{Q})\sim\frac{1}{n_L}\frac{x}{\log x}. \tag{2}$$

On GRH this can be made much more precise (see [13, p. 133], cf. [4]):

Lemma 2. *Assuming the RH for the Dedekind zeta function of L one has*

$$\pi_1(x;L/\mathbb{Q})=\frac{\mathrm{Li}(x)}{n_L}+O\left(\frac{\sqrt{x}}{n_L}\log(|d_L|x^{n_L})\right).$$

Note that in case $L=\mathbb{Q}$ Lemma 2 implies that $\pi(x)=\mathrm{Li}(x)+O(\sqrt{x}\log x)$, under RH. This result was first proved in 1901 by H. von Koch.

We will also need an estimate for the discriminant of $K(\zeta_n)$ in terms of n and d_K, the discriminant of K.

Lemma 3. *We have* $\log|d_{K(\zeta_n)}|\le\varphi(k)(n_K\log n+\log|d_K|)$.

Proof. If $L_1/\mathbb{Q}$ and $L_2/\mathbb{Q}$ are two extension fields and L is their compositum, then the associated discriminant (over $\mathbb{Q}$) satisfies $d_L|d_{L_1}^{[L:L_1]}d_{L_2}^{[L:L_2]}$. From this and the obvious estimates $[L:L_1]\le[L_2:\mathbb{Q}]$ and $[L:L_2]\le[L_1:\mathbb{Q}]$, we obtain the estimate $\log|d_L|\le[L_2:\mathbb{Q}]\log|d_{L_1}|+[L_1:\mathbb{Q}]\log|d_{L_2}|$. On using the well-known fact that the discriminant of $\mathbb{Q}(\zeta_n)$ is a divisor of $n^{\varphi(n)}$, the result then follows on taking $L_1=\mathbb{Q}(\zeta_n)$ and $L_2=K$. □

Our two heuristics will be based on the following elementary observation in group theory.

Lemma 4.
1) *Let $h\ge1$ and $w\ge0$ be integers. Let G be a cyclic group of order n. Let $G^h=\{g^h:g\in G\}$ and $G_w^h=\{g^h:\nu_2(\mathrm{ord}(g^h))=w\}$. We have $\#G^h=n/(n,h)$ and $\#G_0^h=2^{-\nu_2(n/(n,h))}n/(n,h)$. Furthermore, for $w\ge1$, we have*

$$\#G_w^h=\begin{cases}2^{w-1-\nu_2(n/(n,h))}n/(n,h), & \text{if } \nu_2(n/(n,h))\ge w;\\ 0, & \text{otherwise.}\end{cases} \tag{3}$$

2) *If $\nu_2(h)\ge\nu_2(n)$, then every element in G^h has odd order. If $\nu_2(h)<\nu_2(n)$, then $G_0^h\subseteq G^{2h}$.*
3) *We have*

$$G_1^h\subseteq\begin{cases}G^h\backslash G^{2h}, & \text{if } \nu_2(n)=\nu_2(h)+1;\\ G^{2h}, & \text{if } \nu_2(n)>\nu_2(h)+1.\end{cases}$$

If $\nu_2(n)\le\nu_2(h)$, then G_1^h is empty.

Proof. 1) Let g_0 be a generator of G. On noting that $g_0^{m_1} = g_0^{m_2}$ iff $m_1 \equiv m_2 \pmod{n}$, the proof becomes a simple exercise in solving linear congruences. In this way one infers that $G^h = \{g_0^{hk} \ : \ 1 \le k \le n/(n,h)\}$ and hence $\#G^h = n/(n,h)$. Note that $\mathrm{ord}(g_0^{hk})$ is the smallest positive integer m such that $n/(n,h)$ divides mk. Thus $\mathrm{ord}(g_0^{hk})$ will be odd iff $\nu_2(k) \ge \nu_2(n/(n,h))$. Using this observation we obtain that

$$G_0^h = \{g_0^{hk} \ : \ 1 \le k \le \frac{n}{(n,h)}, \ \nu_2(k) \ge \nu_2(\frac{n}{(n,h)})\} \tag{4}$$

and hence $\#G_0^h = 2^{-\nu_2(n/(n,h))} n/(n,h)$. Similarly

$$G_w^h = \{g_0^{hk} \ : \ 1 \le k \le \frac{n}{(n,h)}, \ \nu_2(k) = \nu_2(\frac{n}{(n,h)}) - w\}$$

and hence we obtain (3).
2) If $\nu_2(h) \ge \nu_2(n)$, then $\#G_0^h = \#G^h$ by part 1 and hence every element in G^h has odd order. If $\nu_2(h) < \nu_2(n)$, then using (4) we infer that

$$G_0^h \subseteq \{g_0^{hm} : 1 \le m \le \frac{n}{(n,h)}, \ \nu_2(m) \ge 1\} = \{g_0^{2hk} : 1 \le k \le \frac{n}{(n,2h)}\} = G^{2h},$$

where we have written $m = 2k$ and used that $(n,2h) = 2(n,h)$.
3) Similar to that of part 2. □

Remark. Note that G^h and G_0^h with the induced group operation from G are actually subgroups of G.

3 Two heuristic formulae for $N_{a,b}(x)$

In this section we propose two heuristics for $N_{a,b}(x)$; one more refined than the other. The starting point is the observation that a prime $p \nmid 2ab$ divides the sequence $\{a^k + b^k\}_{k=1}^{\infty}$ if and only if $\mathrm{ord}_r(p)$ is even, where $r = a/b$. Let h be the largest integer such that we can write $|r| = r_0^h$ with r_0 a rational number. Let $\varepsilon = \mathrm{sgn}(r)$ and $e = \nu_2(h)$.

We will use Lemma 4 in the case $G = G_p := (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{F}_p^*$. The first heuristic approximation we consider is

$$K_{a,b}^{(1)}(x) = \sum_{p \le x, \ p \nmid 2ab} \frac{\#G_{p,(1-\varepsilon)/2}^h}{\#G_p^h},$$

where $K_{a,b}^{(1)}(x)$ is supposed to be an heuristic for the number of primes $p \le x$ such that $\mathrm{ord}_r(p)$ is odd. From our results below it will follow that $\lim_{x\to\infty} K_{a,b}^{(1)}(x)/\pi(x)$ exists. Note that in case $h = 1$ this limit is the average density of elements of odd order (if $\varepsilon = 1$), respectively of order congruent to 2 (mod 4) (if $\varepsilon = -1$). For a more detailed investigation of the average number of elements having order $\equiv a \pmod{d}$, see [9].

Suppose that $p \nmid 2ab$. By assumption $r \in \varepsilon G_p^h$. In the case $\varepsilon = 1$, the latter set has $\#G_{p,0}^h$ elements having odd order and so, in some sense, $\#G_{p,0}^h/\#G_p^h$ is the probability that $\mathrm{ord}_r(p)$ is odd. This motivates the definition of $K_{a,b}^{(1)}(x)$ in case $\varepsilon = 1$. In case $\varepsilon = -1$

we use the observation that for p is odd, $-r_0^h$ has odd order iff r_0^h has order congruent to 2 (mod 4). Thus the elements in $-G_p^h$ of odd order are precisely the elements having order 2 (mod 4) in G_p^h and hence have cardinality $\#G_{p,1}^h$. On using part 1 of Lemma 4 we infer that $K_{a,b}^{(1)}(x) = \sum_{p\le x,\ p\nmid 2ab} k_{a,b}^{(1)}(p)$ with

$$k_{a,b}^{(1)}(p) = \begin{cases} (1+\varepsilon)/2, & \text{if } \nu_2(p-1) \le e; \\ 2^{e-\nu_2(p-1)}, & \text{if } \nu_2(p-1) > e. \end{cases} \tag{5}$$

An heuristic $H_{a,b}^{(1)}(x)$ for $N_{a,b}(x)$ is now obtained merely by setting

$$H_{a,b}^{(1)}(x) = \pi(x) - K_{a,b}^{(1)}(x).$$

Put $\omega(n) = \sum_{p|n} 1$. On using (5) we then infer that

$$H_{a,b}^{(1)}(x) = \pi(x; 2^{e+1}, 1) - 2^e \sum_{\substack{p\le x \\ \nu_2(p-1)>e}} 2^{-\nu_2(p-1)} + O(\omega(ab)),$$

if $\varepsilon = 1$ and

$$H_{a,b}^{(1)}(x) = \pi(x) - 2^e \sum_{\substack{p\le x \\ \nu_2(p-1)>e}} 2^{-\nu_2(p-1)} + O(\omega(ab)),$$

if $\varepsilon = -1$.

In the context of (near) primitive roots it is known that the analogs of $H_{a,b}^{(1)}(x)$ do not always, assuming GRH, exhibit the correct asymptotic behavior, but that an appropriate 'quadratic' heuristic, i.e., an heuristic taking into account Legendre symbols, always has the correct asymptotic behavior [6, 7, 8] (in [8] the main result of [7] is proved in a different and much shorter way). With this in mind, we propose a second, more refined, heuristic: $H_{a,b}^{(2)}(x)$.

If $\nu_p(r) = 0$ we can consider $|r| = r_0^h$ and r_0 as elements of G_p. We write $(r_0/p) = 1$ if r_0 is a square in G_p and $(r_0/p) = -1$ otherwise.

First consider the case where $\varepsilon = 1$. If $\nu_2(p-1) \le e$, then r has odd order by part 2 of Lemma 4. If $\nu_2(p-1) > \nu_2(h)$ and $(r_0/p) = -1$, then $r \in G_p^h$, but $r \notin G_p^{2h}$ (by part 2 of Lemma 4 again). It then follows that r has even order. On the other hand, if $(r_0/p) = 1$ then $r \in G_p^{2h}$. This suggests to take

$$K_{a,b}^{(2)}(x) = \sum_{p\le x,\ \nu_2(p-1)\le e} 1 + \sum_{\substack{p\le x,\ (r_0/p)=1 \\ \nu_2(p-1)>e}} \frac{\#G_{p,0}^h}{\#G_p^{2h}},$$

where furthermore we require that $p \nmid 2ab$. A similar argument, now using part 3 instead of part 2 of Lemma 4, leads to the choice

$$K_{a,b}^{(2)}(x) = \sum_{\substack{p\le x,\ (r_0/p)=-1 \\ \nu_2(p-1)=e+1}} \frac{\#G_{p,1}^h}{\#G_p^{2h}} + \sum_{\substack{p\le x,\ (r_0/p)=1 \\ \nu_2(p-1)>e+1}} \frac{\#G_{p,1}^h}{\#G_p^{2h}},$$

in case $\varepsilon = -1$, where again we furthermore require that $p \nmid 2ab$. We obtain $K^{(2)}_{a,b}(x) = \sum_{p\le x,\ p\nmid 2ab} k^{(2)}_{a,b}(p)$, with

$$k^{(2)}_{a,b}(p) = \begin{cases} (1+\varepsilon)/2, & \text{if } \nu_2(p-1) \le e; \\ (1+\varepsilon(\frac{r_0}{p}))/2, & \text{if } \nu_2(p-1) = e+1; \\ (1+(\frac{r_0}{p}))2^{e-\nu_2(p-1)}, & \text{if } \nu_2(p-1) > e+1. \end{cases} \tag{6}$$

Now we put $H^{(2)}_{a,b}(x) = \pi(x) - K^{(2)}_{a,b}(x)$ as before. On invoking Lemma 4, $H^{(2)}_{a,b}(x)$ can then be more explicitly written as

$$H^{(2)}_{a,b}(x) = \pi(x; 2^{e+1}, 1) - 2^{e+1} \sum_{\substack{p\le x,\ (r_0/p)=1 \\ \nu_2(p-1)>e}} 2^{-\nu_2(p-1)} + O(\omega(ab)), \tag{7}$$

if $\varepsilon = 1$ and

$$H^{(2)}_{a,b}(x) = \pi(x) - \sum_{\substack{p\le x,\ (r_0/p)=-1 \\ \nu_2(p-1)=e+1}} 1 - 2^{e+1} \sum_{\substack{p\le x,\ (r_0/p)=1 \\ \nu_2(p-1)>e+1}} 2^{-\nu_2(p-1)} + O(\omega(ab)), \tag{8}$$

if $\varepsilon = -1$.

4 Asymptotic analysis of the heuristic formulae

4.1 Unconditional asymptotic analysis

In this section we determine the unconditional asymptotic behavior of $H^{(1)}_{a,b}(x)$ and $H^{(2)}_{a,b}(x)$. We adopt the notation from Theorem 2 and in addition write D for the discriminant of $\mathbb{Q}(\sqrt{r_0})$. Note that $D > 0$.

Theorem 4. *Let $A > 0$ be arbitrary. The implied constants below depend at most on A.*
1) *We have $H^{(1)}_{a,b}(x) = \delta_1(r)\mathrm{Li}(x) + O(x\log^{-A} x) + O(\omega(ab))$, where*

$$\delta_1(r) = \begin{cases} 2^{1-e}/3, & \text{if } \varepsilon = +1; \\ 1 - 2^{-e}/3, & \text{if } \varepsilon = -1. \end{cases}$$

In particular, if $L \neq \mathbb{Q}(\sqrt{2})$, then $H^{(1)}_{a,b}(x)$ is an asymptotically exact heuristic for $N_{a,b}(x)$.
2) *We have $H^{(2)}_{a,b}(x) = \delta(r)\mathrm{Li}(x) + O(D^2 x\log^{-A} x) + O(\omega(ab))$. In particular, $H^{(2)}_{a,b}(x)$ is an asymptotically exact heuristic for $N_{a,b}(x)$.*

The proof of part 2 requires some facts from algebraic number theory, the proof of part 1 does not even require that and is an easier variant of the proof of part 2 (and is left to the interested reader). The proof of part 2 rests on a few lemmas.

Lemma 5. *Let n be a non-zero integer, $\zeta_n = e^{2\pi i/n}$, and $K = \mathbb{Q}(\sqrt{n})$ be a quadratic number field of discriminant Δ. Let $A > 1$ and $C > 0$ be positive real numbers. Then*

$$\sum_{\substack{p\le x,\ (n/p)=1\\ \nu_2(p-1)=k}} 1 = \mathrm{Li}(x)\left(\frac{1}{[K(\zeta_{2^k}):\mathbb{Q}]} - \frac{1}{[K(\zeta_{2^{k+1}}):\mathbb{Q}]}\right) + O\left(\frac{|\Delta|x}{\log^A x}\right),$$

uniformly in k with k satisfying $2^{k+3}|\Delta| \le \log^C x$, where the implied constant depends at most on A and C.

Proof. By quadratic reciprocity a prime p satisfies $(n/p) = 1$ iff p is in a certain set of congruences classes modulo $4|\Delta|$. Thus the primes we are counting in our sum are precisely the primes that belong to certain congruences classes modulo $2^{k+2}|\Delta|$, but do not belong to certain congruence classes modulo $2^{k+3}|\Delta|$. The total number of congruence classes involved is less than $8|\Delta|$. Now apply Lemma 1. This yields the result but with an, as yet, unknown density.

On the other hand, the primes p that are counted are precisely the primes $p \le x$ that split completely in the normal number field $K(\zeta_{2^k})$, but do not split completely in the normal number field $K(\zeta_{2^{k+1}})$. If M is any normal extension then it is a consequence of Chebotarev's density theorem (2) that the set of primes that split completely in M has density $1/[M:\mathbb{Q}]$. On using this, the proof is completed. □

Lemma 6. *Let m be fixed. With the notation as in the previous lemma we have*

$$T_n(m;x) = \mathrm{Li}(x)\sum_{k=m}^{\infty}\frac{1}{2^k}\left(\frac{1}{[K(\zeta_{2^k}):\mathbb{Q}]} - \frac{1}{[K(\zeta_{2^{k+1}}):\mathbb{Q}]}\right) + O\left(\frac{\Delta^2 x}{\log^A x}\right),$$

where the implied constant depends at most on A and

$$T_n(m;x) := \sum_{\substack{p\le x,\ (n/p)=1\\ \nu_2(p-1)\ge m}} 2^{-\nu_2(p-1)}.$$

Proof. We have

$$T_n(m;x) = \sum_{k=m}^{m_1}\sum_{\substack{p\le x,\ (n/p)=1\\ \nu_2(p-1)=k}} 2^{-k} + O(\frac{x}{4^{m_1}}),$$

where we used the trivial bound $\sum_{p\le x,\ \nu_2(p-1)\ge m_1} 2^{-\nu_2(p-1)} = O(x/4^{m_1})$. Choose m_1 to be the largest integer such that $2^{m_1+3}|\Delta| \le \log^C x$. Apply Lemma 5 with any $C > A/2$. It follows that

$$\begin{aligned} T_n(m;x) &= \mathrm{Li}(x)\sum_{k=m}^{m_1}\frac{1}{2^k}\left(\frac{1}{[K(\zeta_{2^k}):\mathbb{Q}]} - \frac{1}{[K(\zeta_{2^{k+1}}):\mathbb{Q}]}\right) + O(\frac{x}{4^{m_1}});\\ &= \mathrm{Li}(x)\sum_{k=m}^{\infty}\frac{1}{2^k}\left(\frac{1}{[K(\zeta_{2^k}):\mathbb{Q}]} - \frac{1}{[K(\zeta_{2^{k+1}}):\mathbb{Q}]}\right) + O(\frac{x}{4^{m_1}}), \end{aligned}$$

where we used that $\varphi(2^k) \le [K(\zeta_{2^k}):\mathbb{Q}] \le 2\varphi(2^k)$. On noting that $O(x/4^{m_1}) = O(\Delta^2 x \log^{-A} x)$, the result follows. □

Lemma 7. *We have* $H^{(2)}_{a,b}(x) = \delta_2(r)\mathrm{Li}(x) + O(D^2 x \log^{-A} x) + O(\omega(ab))$, *where*

$$\delta_2(r) = \frac{1}{2^e} - 2^{e+1}\sum_{k=e+1}^{\infty}\frac{1}{2^k}\left(\frac{1}{[L(\zeta_{2^k}):\mathbb{Q}]} - \frac{1}{[L(\zeta_{2^{k+1}}):\mathbb{Q}]}\right) \tag{9}$$

if $\varepsilon = 1$ *and, in case* $\varepsilon = -1$,

$$\delta_2(r) = 1 - \frac{1}{2^{e+1}} + \frac{1}{[L(\zeta_{2^{e+1}}):\mathbb{Q}]} - \frac{1}{[L(\zeta_{2^{e+2}}):\mathbb{Q}]}$$

$$-2^{e+1}\sum_{k=e+2}^{\infty}\frac{1}{2^k}\left(\frac{1}{[L(\zeta_{2^k}):\mathbb{Q}]} - \frac{1}{[L(\zeta_{2^{k+1}}):\mathbb{Q}]}\right). \tag{10}$$

Proof. This easily follows on combining the previous lemma with equation (7), respectively (8). (Note that $L = \mathbb{Q}(\sqrt{u}) = \mathbb{Q}(\sqrt{r_0})$.) $\square$

Remark. From (9) and (10) we infer that

$$\delta_2(-|r|) - \delta_2(|r|) = 1 - \frac{3}{2^{e+1}} + \frac{2}{[L(\zeta_{2^{e+1}}):\mathbb{Q}]} - \frac{2}{[L(\zeta_{2^{e+2}}):\mathbb{Q}]}.$$

The number $\delta_2(r)$ can be readily evaluated on using the following simple fact from algebraic number theory:

Lemma 8. *Let* K *be a real quadratic field. Let* $k \ge 1$. *Then*

$$[K(\zeta_{2^k}):\mathbb{Q}] = \begin{cases} 2^k, & \text{if } k \le 2 \text{or} K \ne \mathbb{Q}(\sqrt{2}); \\ 2^{k-1}, & \text{if } k \ge 3 \text{and} K = \mathbb{Q}(\sqrt{2}). \end{cases}$$

Proof. If K is a quadratic field other than $\mathbb{Q}(\sqrt{2})$ then there is an odd prime that ramifies in it. This prime, however, does not ramify in $\mathbb{Q}(\zeta_{2^n})$, so in this case K and $\mathbb{Q}(\sqrt{2})$ are linearly disjoint. Note that $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$ and hence $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$. Using the well-known result that $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$, the result is then easily completed. $\square$

The result of this evaluation is stated below.

Lemma 9. *We have* $\delta_2(r) = \delta(r)$.

After all this preliminary work, it is straightforward to prove the two main results of this note:

Proof of Theorem 4. 1) Left to the reader. 2) Combine the latter lemma with Lemma 7. Comparison with Theorem 1 shows that $H^{(2)}_{a,b}(x) \sim N_{a,b}(x)$ as $x \to \infty$ and thus $H^{(2)}_{a,b}(x)$ is an asymptotically exact approximation of $N_{a,b}(x)$. $\square$

Proof of Theorem 2. Combine part 2 of Theorem 4 (with any $A > 3$), Theorem 1 and equations (7) and (8). $\square$

4.2 Conditional asymptotic analysis

In this section we redo the unconditional analysis under the assumption that RH holds for all fields of the form $K(\zeta_{2^n})$ with K quadratic or $K=\mathbb{Q}$. Let us abbreviate this assumption by SRH (with S standing for 'small').

Lemma 10. (SRH). *Let n be a non-zero integer and $K=\mathbb{Q}(\sqrt{n})$ be a quadratic number field of discriminant Δ. Then*

$$\sum_{\substack{p\le x,\ (n/p)=1\\ \nu_2(p-1)=k}} 1 = \mathrm{Li}(x)\left(\frac{1}{[K(\zeta_{2^k}):\mathbb{Q}]}-\frac{1}{[K(\zeta_{2^{k+1}}):\mathbb{Q}]}\right)+O\left(\sqrt{x}[k\log 2+\log(|\Delta|x)]\right).$$

Proof. The proof follows the second part of the proof in Lemma 5, but this time with the Chebotarev density theorem as given by Lemma 2, rather than (2). The terms $\log|d_{K(\zeta_{2^m})}|$ involved (with $m=k$ and $m=k+1$) are estimated using Lemma 3. □

By simply summing the right hand side in Lemma 10 from $k=m$ onwards, one obtains that, on SRH,

$$T_n(m;x)=\mathrm{Li}(x)\sum_{k=m}^{\infty}\frac{1}{2^k}\left(\frac{1}{[K(\zeta_{2^k}):\mathbb{Q}]}-\frac{1}{[K(\zeta_{2^{k+1}}):\mathbb{Q}]}\right)+O\left(\sqrt{x}\log(|\Delta|x)\right).$$

With these ingredients one obtains that on SRH we have that Theorem 4 holds with error term $O(\sqrt{x}\log x)$, respectively $O(\sqrt{x}\log(|D|x))$ in part 1, respectively part 2. On using (1) the proof of Theorem 3 is then easily completed.

5 Two alternative formulations

5.1 An alternative formulation using Ramanujan sums

Recall that the *Ramanujan sum* $c_n(m)$ is defined as $\sum_{1\le k\le n,\ (k,n)=1} e^{2\pi ikm/n}$. Alternatively one can write $c_n(m)=\mathrm{Tr}_n(\zeta_n^m)$, where by Tr_n we denote the trace over the cyclotomic field $\mathbb{Q}(\zeta_n)$. It follows at once from the properties of the trace that $c_n(m)=c_n((n,m))$. Since ζ_n^m is an algebraic integer, it follows that $c_n(m)$ is an integer. The following result is known as *Hölder's identity.*

Lemma 11 (Hölder's identity). *Let μ denote the Möbius function. Then*

$$c_n(m)=\varphi(n)\frac{\mu(\frac{n}{(n,m)})}{\varphi(\frac{n}{(n,m)})}.$$

Proof. Write $v=(n,m)$. Note that $\zeta_n^m=\zeta_{n/v}^{m/v}$ and $(n/v,m/v)=1$. From this we obtain

$$c_n(m)=\mathrm{Tr}_n(\zeta_n^m)=\frac{\varphi(n)}{\varphi(\frac{n}{v})}\mathrm{Tr}_{\frac{n}{v}}(\zeta_{\frac{n}{v}}^{\frac{m}{v}})=\frac{\varphi(n)}{\varphi(\frac{n}{v})}\mathrm{Tr}_{\frac{n}{v}}(\zeta_{\frac{n}{v}}).$$

Note that the result follows if we show that $\mathrm{Tr}_n(\zeta_n) = \mu(n)$. Suppose that v and w are coprime integers. Noting that the set

$$\{\zeta_{vw}^j : 1 \le j \le vw,\ (j, vw) = 1\}$$

equals the set

$$\{\zeta_v^a \zeta_w^b : 1 \le a \le v, 1 \le b \le w, (a, v) = (b, w) = 1\},$$

it is seen that $\mathrm{Tr}_{vw}(\zeta_{vw}) = \mathrm{Tr}_v(\zeta_v)\mathrm{Tr}_w(\zeta_w)$ and that consequently $\mathrm{Tr}_n(\zeta_n)$ is a multiplicative function in n. The minimal polynomial over $\mathbb{Q}$, $m_{p^r}(X)$, of ζ_{p^r} is seen to be $m_{p^r}(X) = (X^{p^r} - 1)/(X^{p^{r-1}} - 1) = \sum_{j=0}^{p-1} X^{p^{r-1}j}$ and hence $\mathrm{Tr}_{p^r}(\zeta_{p^r}) = \mu(p^r)$ and so, indeed, $\mathrm{Tr}_n(\zeta_n) = \mu(n)$. □

For our purposes the following weak version of Hölder's identity will suffice:

$$c_{2^v}(t) = \begin{cases} 0, & \text{if } \nu_2(t) \le v-2; \\ -\varphi(2^v), & \text{if } \nu_2(t) = v-1; \\ \varphi(2^v), & \text{if } \nu_2(t) \ge v. \end{cases} \tag{11}$$

Another elementary property of Ramanujan sums we need is that for arbitrary natural numbers n and m

$$\frac{1}{n}\sum_{d|n} c_d(m) = \begin{cases} 1, & \text{if } n|m; \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

Suppose that $\nu_p(r) = 0$, then $\mathrm{ord}_r(p)[\mathbb{F}_p^* : \langle r\rangle] = p-1$. Note that $\mathrm{ord}_r(p)$ is odd iff $2^{\nu_2(p-1)} | [\mathbb{F}_p^* : \langle r\rangle]$. Using identity (12) it then follows that

$$N_{a,b}(x) = \pi(x) - \sum_{p\le x,\ p\nmid 2ab} 2^{-\nu_2(p-1)} \sum_{v \le \nu_2(p-1)} c_{2^v}([\mathbb{F}_p^* : \langle r\rangle]) + O(\omega(ab)). \tag{13}$$

The following lemma relates Ramanujan sums with our heuristics.

Lemma 12. *Let a, b, ε and e be as in Theorem 2, $k_{a,b}^{(1)}(p)$ and $k_{a,b}^{(2)}(p)$ be as in (5), respectively (6), and let $p \nmid 2ab$.*
1) *We have*

$$2^{-\nu_2(p-1)} \sum_{v \le \min(\nu_2(p-1), e)} c_{2^v}([\mathbb{F}_p^* : \langle r\rangle]) = k_{a,b}^{(1)}(p).$$

2) *We have*

$$2^{-\nu_2(p-1)} \sum_{v \le \min(\nu_2(p-1), e+1)} c_{2^v}([\mathbb{F}_p^* : \langle r\rangle]) = k_{a,b}^{(2)}(p).$$

Corollary 1. *For $1 \le j \le 2$ we have*

$$\sum_{p\le x,\ p\nmid 2ab} 2^{-\nu_2(p-1)} \sum_{v \le \min(\nu_2(p-1), e+j-1)} c_{2^v}([\mathbb{F}_p^* : \langle r\rangle]) = K_{a,b}^{(j)}(x).$$

Proof of Lemma 12. 1) We consider the two cases $\nu_2(p-1) > e$ and $\nu_2(p-1) \leq e$ separately.
- *The case $\nu_2(p-1) > e$.* Note that $(\varepsilon r_0^h)^{\frac{p-1}{2^e}} \equiv 1 \pmod p$ and so $\nu_2([\mathbb{F}_p^* : \langle r\rangle]) \geq e$. Hence the sum in the statement of the lemma reduces to

$$2^{-\nu_2(p-1)} \sum_{v \leq e} \varphi(2^v) = 2^{e-\nu_2(p-1)} = k_{a,b}^{(1)}(p),$$

where (11), (5) and the identity $\sum_{d|n} \varphi(d) = n$ are used.
- *The case $\nu_2(p-1) \leq e$.* Note that

$$\nu_2([\mathbb{F}_p^* : \langle r\rangle]) = \begin{cases} \nu_2(p-1) - 1, & \text{if } \varepsilon = -1; \\ \nu_2(p-1), & \text{if } \varepsilon = 1. \end{cases}$$

If $\epsilon = -1$, the sum under consideration equals

$$2^{-\nu_2(p-1)}[\sum_{v \leq \nu_2(p-1)-1} \varphi(2^v) - \varphi(2^{\nu_2(p-1)})] = 0 = \frac{1+\varepsilon}{2}.$$

If $\epsilon = 1$, the sum under consideration equals

$$2^{-\nu_2(p-1)} \sum_{v \leq \nu_2(p-1)} \varphi(2^v) = 1 = \frac{1+\varepsilon}{2}.$$

We thus infer that the sum under consideration equals $(1+\varepsilon)/2 = k_{a,b}^{(1)}(p)$.
2) We consider the three cases $\nu_2(p-1) \leq e$, $\nu_2(p-1) = e+1$ and $\nu_2(p-1) > e+1$ separately.
- *The case $\nu_2(p-1) \leq e$.* The quantity under consideration agrees with that considered in part 1 of this proof and by (6) we obtain that $k_{a,b}^{(1)}(p) = (1+\varepsilon)/2 = k_{a,b}^{(2)}(p)$.
- *The case $\nu_2(p-1) = e+1$.* Now

$$\varepsilon^{\frac{p-1}{2^{e+1}}} = \varepsilon,\ (r_0^h)^{\frac{p-1}{2^{e+1}}} \equiv (\frac{r_0}{p}) \pmod p \text{ and hence } r^{\frac{p-1}{2^{e+1}}} = (\varepsilon r_0^h)^{\frac{p-1}{2^{e+1}}} \equiv \varepsilon(\frac{r_0}{p}) \pmod p.$$

It follows that $\nu_2([\mathbb{F}_p^* : \langle r\rangle]) \geq e+1$ if $\varepsilon(\frac{r_0}{p}) = 1$ and $\nu_2([\mathbb{F}_p^* : \langle r\rangle]) = e$ if $\varepsilon(\frac{r_0}{p}) = -1$. Using (11) the quantity under consideration is reduced to

$$2^{-\nu_2(p-1)} \left(\sum_{v \leq e} \varphi(2^v) + \varepsilon(\frac{r_0}{p})2^e \right) = \frac{1+\varepsilon(\frac{r_0}{p})}{2}.$$

By (6) this equals $k_{a,b}^{(2)}(p)$.
- *The case $\nu_2(p-1) > e+1$.* Now $r^{(p-1)/2^{1+e}} \equiv (\frac{r_0}{p}) \pmod p$. Proceeding as before the quantity under consideration reduces to

$$2^{-\nu_2(p-1)} \left(\sum_{v \leq e} \varphi(2^v) + (\frac{r_0}{p})2^e \right) = 2^{e-\nu_2(p-1)}(1 + (\frac{r_0}{p})).$$

By (6) this equals $k^{(2)}_{a,b}(p)$. $\square$

Corollary 1 shows that if in the double sum in (13) the summation is restricted to those v satisfying in addition $v \le e$, respectively $v \le e+1$, then $K^{(1)}_{a,b}(x)$, respectively $K^{(2)}_{a,b}(x)$ is obtained. This in combination with Theorems 1, 3 and 4 leads to the following theorem:

Theorem 5. *We have in the notation of Theorem 2,*

$$N_{a,b}(x) = \pi(x) - \sum_{p\le x,\ p\nmid 2ab} 2^{-\nu_2(p-1)} \sum_{2^v|(p-1,2h)} c_{2^\nu}([\mathbb{F}_p^* : \langle r\rangle]) + O\left(\frac{x(\log\log x)^4}{\log^3 x}\right),$$

and

$$\sum_{p\le x,\ p\nmid 2ab} 2^{-\nu_2(p-1)} \sum_{e+2\le v\le \nu_2(p-1)} c_{2^\nu}([\mathbb{F}_p^* : \langle r\rangle]) = O\left(\frac{x(\log\log x)^4}{\log^3 x}\right),$$

where the implied constant depends at most on a and b. Under GRH the above error terms can be replaced by $O(\sqrt{x}\log^{\omega(d)+1} x)$.

Remark. Note that the inequality $v \le \min(\nu_2(p-1), e+1)$ is equivalent to $2^v|(p-1,2h)$.

5.2 An alternative formulation involving character sums

Let G be a cyclic group of order n and g an element in G. It is not difficult to show that, for any $d|n$, $\sum_{\mathrm{ord}(\chi)=d}\chi(g) = c_d([G:\langle g\rangle])$, where the sum is over the characters χ of G of order d. Using this and noting that $\chi(r) = \chi(\varepsilon)\chi^h(r_0)$, equation (13) can be rewritten as

$$N_{a,b}(x) = \pi(x) - \sum_{p\le x,\ p\nmid 2ab} 2^{-\nu_2(p-1)} \sum_{\mathrm{ord}(\chi)|2^{\nu_2(p-1)}} \chi(\varepsilon)\chi^h(r_0) + O(\omega(ab)), \tag{14}$$

where the sum is over all characters of $\mathbb{F}_p^*$ having order dividing $2^{\nu_2(p-1)}$. Note that if χ is of order 2^v, then χ^h is the trivial character if $v \le e$ and a quadratic character if $v = e+1$. If in the main term of (14) only those characters of order dividing h are retained, i.e., those for which χ^h is the trivial character, then $H^{(1)}_{a,b}(x)$ is obtained (this is a reformulation of part 1 of Lemma 12) and hence, by part 1 of Theorem 4, the naïve heuristic. If in (14) only those characters of order dividing $2h$ are retained, i.e., those for which χ^h is the trivial or a quadratic character, then the asymptotically exact heuristic is obtained. The error term assertion in Theorem 5 can be reformulated as:

Proposition 1. *We have*

$$\sum_{p\le x,\ p\nmid 2ab} 2^{-\nu_2(p-1)} \sum_{2^{e+2}|\mathrm{ord}(\chi)|2^{\nu_2(p-1)}} \chi(\varepsilon)\chi^h(r_0) = O\left(\frac{x(\log\log x)^4}{\log^3 x}\right),$$

where the implied constant depends at most on a and b. Under GRH the above error term can be replaced by $O(\sqrt{x}\log^{\omega(d)+1} x)$.

In the setting of near primitive roots it is already known that for the main term of the counting function of (near) primitive roots only the contributions coming from characters that are either trivial or quadratic need to be included [7].

6 Some numerical experiments

Let $N'_{a,b}(x)$ denote the number of odd prime divisors $p \le x$ of the sequence $\{a^k + b^k\}_{k=1}^{\infty}$ and $\pi'(x)$ the number of odd primes not exceeding x. We define

$$\min_{\text{old}} = \min_{x \le 10^6} \{N'_{a,b}(x) - \delta(\frac{a}{b})\pi'(x)\} \text{ and } \max_{\text{old}} = \max_{x \le 10^6} \{N'_{a,b}(x) - \delta(\frac{a}{b})\pi'(x)\}.$$

Similarly we define $\min_{heur}$ and $\max_{heur}$, but with $\delta(a/b)\pi'(x)$ replaced by the main term in Theorem 2.

Numerical work strongly suggests (cf. Table 2) that the main term in Theorem 2 gives a better approximation to $N_{a,b}(x)$ than $\delta(r)\pi(x)$ (which on its turn gives a better approximation that $\delta(r)\mathrm{Li}(x)$).

sequence	$\min_{\text{old}}$	$\max_{\text{old}}$	$\min_{\text{heur}}$	$\max_{\text{heur}}$
$\{2^k+1\}_{k=1}^{\infty}$	$-56.416\cdots$	$46.958\cdots$	$-24.791\cdots$	$22.432\cdots$
$\{4^k+1\}_{k=1}^{\infty}$	$-54.916\cdots$	$45.500\cdots$	$-11.328\cdots$	$38.466\cdots$
$\{16^k+1\}_{k=1}^{\infty}$	$-22.250\cdots$	$35.083\cdots$	$-2.785\cdots$	$44.571\cdots$
$\{9^k+1\}_{k=1}^{\infty}$	$-71.666\cdots$	$32.000\cdots$	$-6.237\cdots$	$41.006\cdots$
$\{(-2)^k+1\}_{k=1}^{\infty}$	$-33.833\cdots$	$32.041\cdots$	$-7.051\cdots$	$29.440\cdots$
$\{(-3)^k+1\}_{k=1}^{\infty}$	$-43.666\cdots$	$44.666\cdots$	$-6.514\cdots$	$39.951\cdots$
$\{(-4)^k+1\}_{k=1}^{\infty}$	$-49.000\cdots$	$45.333\cdots$	$-19.641\cdots$	$30.507\cdots$

Table 2: The old approximation of $N'_{a,b}(x)$ versus the heuristic one

The results in Table 2 were produced using the Maple package.

7 Conclusion

There is a naïve heuristic for $N_{a,b}(x)$ that in many, but not all, cases is asymptotically exact. There is a quadratic modification of this heuristic involving the Legendre symbol that is *always* asymptotically exact. The same phenomenon is observed (assuming GRH) in the setting of Artin's primitive root conjecture. Numerical experiments strongly suggests that the quadratic heuristic better approximates $N_{a,b}(x)$ than the main terms in earlier results.

8 Acknowledgments

I would like to thank Peter Stevenhagen for pointing out that Lemma 11 follows easily using properties of the trace. Since I am not aware of a proof along these lines in the literature, I have included it here.

Thanks are also due to the referee for his/her extensive comments.

References

[1] C. Ballot, Density of prime divisors of linear recurrences, *Mem. Amer. Math. Soc.* **115** (1995), no. 551.

[2] H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod. p ist, *Math. Ann.* **166** (1966), 19–23.

[3] C. Hooley, Artin's conjecture for primitive roots, *J. Reine Angew. Math.* **225** (1967), 209–220.

[4] S. Lang, On the zeta function of number fields, *Invent. Math.* **12** (1971), 337–345.

[5] P. Moree, On the divisors of $a^k + b^k$, *Acta Arith.* **80** (1997), 197–212.

[6] P. Moree, On primes in arithmetic progression having a prescribed primitive root, *J. Number Theory* **78** (1999), 85–98.

[7] P. Moree, Asymptotically exact heuristics for (near) primitive roots, *J. Number Theory* **83** (2000), 155–181.

[8] P. Moree, Asymptotically exact heuristics for (near) primitive roots. II, *Japan. J. Math.* **29** (2003), 143–157.

[9] P. Moree, On the average number of elements in a finite field with order or index in a prescribed residue class, *Finite Fields Appl.* **10** (2004), 438–463.

[10] P. Moree, On primes p for which d divides $\mathrm{ord}_p(g)$, *Funct. Approx. Comment. Math.* **33** (2005), 85–95.

[11] R. W. K. Odoni, A conjecture of Krishnamurthy on decimal periods and some allied problems, *J. Number Theory* **13** (1981), 303–319.

[12] K. Prachar, *Primzahlverteilung*, Springer, New York, 1957.

[13] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401.

[14] K. Wiertelak, On the density of some sets of primes. IV, *Acta Arith.* **43** (1984), 177–190.

2000 *Mathematics Subject Classification*: Primary 11N37; Secondary 11N69, 11R45.
Keywords: primitive root, Chebotarev density theorem, Dirichlet density.

Received February 14 2005; revised version received February 24 2006. Published in *Journal of Integer Sequences*, July 7 2006.

Return to Journal of Integer Sequences home page.