Max-Planck-Institut für Mathematik Bonn

Prime divisors of ℓ-Genocchi numbers and the ubiquity of Ramanujan-style congruences of level ℓ

by

Pieter Moree
Pietro Sgobba

Max-Planck-Institut für Mathematik
Preprint Series 2022 (75)

Date of submission: December 5, 2022

Prime divisors of ℓ-Genocchi numbers and the ubiquity of Ramanujan-style congruences of level ℓ

by

Pieter Moree
Pietro Sgobba

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

University of Luxembourg
Department of Mathematics
6 Avenue de la Fonte
4364 Esch-sur-Alzette
Luxembourg

MPIM 22-75

PRIME DIVISORS OF ℓ-GENOCCHI NUMBERS AND THE UBIQUITY OF RAMANUJAN-STYLE CONGRUENCES OF LEVEL ℓ

PIETER MOREE AND PIETRO SGOBBA

Abstract. Let ℓ be any fixed prime number. We define the ℓ-Genocchi numbers by $G_n := \ell(1-\ell^n)B_n$, with B_n the n-th Bernoulli number. They are integers. We introduce and study a variant of Kummer's notion of regularity of primes. We say that an odd prime p is ℓ-Genocchi irregular if it divides at least one of the ℓ-Genocchi numbers $G_2, G_4, \ldots, G_{p-3}$, and ℓ-regular otherwise. With the help of techniques used in the study of Artin's primitive root conjecture, we give asymptotic estimates for the number of ℓ-Genocchi irregular primes in a prescribed arithmetic progression in case ℓ is odd. The case $\ell = 2$ was already dealt with by Hu, Kim, Moree and Sha (2019).

Using similar methods we study the prime factors of $(1-\ell^n)B_{2n}/2n$ and $(1+\ell^n)B_{2n}/2n$. This allows us to estimate the number of primes $p \leq x$ for which there exist modulo p Ramanujan-style congruences between the Fourier coefficients of an Eisenstein series and some cusp form of prime level ℓ.

1. Introduction

Recall that the n-th Bernoulli number B_n is implicitly defined as the coefficient of t^n in the generating function

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}. \tag{1}$$

The Bernoulli numbers are rational. It is easy to see that $B_0 = 1, B_1 = -1/2$ and $B_{2n+1} = 0$ for $n \geq 1$. By the *von Staudt-Clausen theorem* (see for example [2, Chp. 3]) the remaining Bernoulli numbers satisfy

$$B_{2n} + \sum_{p-1|2n} \frac{1}{p} \in \mathbb{Z}, \tag{2}$$

where the sum is over the primes p for which $p-1$ divides $2n$, and thus their denominators are well understood. However, their numerators are far less so. We say that an odd prime p is *B-irregular* if p divides the numerator of at least one of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$, and *$B$-regular* otherwise. This notion has an important application in algebraic number theory. Let $\mathbb{Q}(\zeta_p)$ with $\zeta_p = e^{2\pi i/p}$ be the p-th cyclotomic field, and h_p its class number.

Theorem 1 (Kummer). *Let p be an odd prime. If $p \nmid h_p$, then the Fermat equation $x^p + y^p = z^p$ does not have a solution in positive integers x, y, z with p coprime to xyz. An odd prime p is B-regular if and only if $p \nmid h_p$.*

This result of Kummer is considered to be one of the highlights of 19th century number theory. In the process of proving it, Kummer developed a lot of algebraic number theory including the notion of ideals. For a more modern proof of Theorem 1 using p-adic methods, see the book by Borevich and Shafarevich [4].

1991 *Mathematics Subject Classification.* Primary 11A07, 11B68; secondary 11F33.

Key words and phrases. ℓ-Genocchi numbers, ℓ-regularity, Ramanujan type congruences, Artin's primitive root conjecture.

In 1915, Jensen (as a student!) proved that there are infinitely many irregular primes (see, e.g., [4, p. 381] or [28, p. 20]). Unfortunately the same is not known for regular primes, although numerical evidence indicates that about 61% of all primes are regular. This number is easily explained using an heuristical argument due to Siegel [32]. Assuming that the divisor structure of Bernoulli denominators is random, we expect that $p \nmid B_k$ with probability $1 - 1/p$. We thus might expect that p is regular with probability $(1 - 1/p)^{(p-3)/2}$, which as p gets large tends to $e^{-1/2} = 0.60653\ldots$.

Conjecture 1 (Siegel)**.** *The number of B-regular primes up to x is given asymptotically by*

$$\frac{x}{\sqrt{e}\log x}.$$

In this paper we study the divisibility of some sequences related to Bernoulli numbers. As usual $\nu_p(a)$ denotes the exponent of p in the prime factorization of the rational number a.

Definition 1 (Divisibility of a sequence)**.** Let $A = \{a_n\}_{n=1}^{\infty}$ be a sequence of rational numbers. We say that a prime p divides the sequence A if there exists $n \geq 1$ such that $a_n \neq 0$ and $\nu_p(a_n) \geq 1$. The set of prime divisors of A we denote by $\mathcal{Q}_A$.

Throughout, if $\mathcal{S}$ is a set of prime numbers, then we denote $\#\{p \leq x : p \in \mathcal{S}\}$ by $\mathcal{S}(x)$.

It is a consequence of (2) and the Kummer congruences, that a prime p divides the sequence of Bernoulli numbers if and only if it is B-irregular. Recall that the *Kummer congruence* (cf. Murty [28, pp. 18-19]) implies that

$$\frac{B_j}{j} \equiv \frac{B_k}{k} \pmod{p}, \quad \text{with } j \equiv k \not\equiv 0 \pmod{p-1}. \tag{3}$$

The aim of this paper is to study the prime divisors of the sequences $\{H_{2n}\}_{n=1}^{\infty}$, $\{H_{2n}^{-}\}_{n=1}^{\infty}$ and $\{H_{2n}^{+}\}_{n=1}^{\infty}$ with

$$H_{2n} := (1 - \ell^{2n})\frac{B_{2n}}{2n}, \qquad H_{2n}^{-} := (1 - \ell^{n})\frac{B_{2n}}{2n}, \qquad H_{2n}^{+} := (1 + \ell^{n})\frac{B_{2n}}{2n}. \tag{4}$$

In this context the notion of irregularity will play an important role.

Definition 2 ((Ir)regularity)**.** Given a sequence of rational numbers $\{A_k\}_{k=1}^{\infty}$, we say that $p > 3$ is A-regular if all of $\nu_p(A_2), \ldots, \nu_p(A_{p-3})$ are non-positive, and A-irregular otherwise. The prime 3 is defined to be A-regular. The set of A-irregular primes is denoted by $\mathcal{P}_A$.

Sometimes we use H_{2n}^{-1} and H_{2n}^{1} instead of H_{2n}^{-}, respectively H_{2n}^{+}. Thus the final two entries in (4) can be more compactly written as

$$H_{2n}^{\varepsilon} := (1 + \varepsilon\ell^{n})\frac{B_{2n}}{2n}, \qquad \varepsilon \in \{-1, 1\}.$$

The number $-H_k^{\varepsilon}/2$ occurs for even k as constant term in the Fourier expansion of a generalization $E_{k,\ell}^{\varepsilon}(z)$ (given by (6)) of the classical weight k Eisenstein series $E_k(z)$ to the prime level ℓ setting. In case modulo a prime p this constant is zero, the Eisenstein series $E_{k,\ell}^{\varepsilon}(z)$ is possibly coefficient wise congruent to a cusp form leading to a congruence of Ramanujan type (such as (5)). In Sect. 4 we consider, given ℓ and ε, for how many primes $p \leq x$ there exists at least one Eisenstein series $E_{k,\ell}^{\varepsilon}(z)$ such that modulo p its constant term $-H_k^{\varepsilon}/2$ is zero. In the next section we discuss this modular form connection in more detail.

1.1. **Ramanujan style congruences for prime level ℓ.** Let E_k be the Eisenstein series of even weight $k \geq 2$ for the group $SL_2(\mathbb{Z})$, normalized so that its Fourier series expansion is

$$E_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2\pi i n z},$$

where $\sigma_r(n) = \sum_{d|n} d^r$ is the r-th sum of divisors function. The prototype of a Ramanujan congruence goes back to 1916 and asserts that

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}, \tag{5}$$

for every positive integer n. This can be viewed as a (coefficient-wise) congruence between the unique cusp form $\Delta(z) = \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n z}$ of weight 12 and the Eisenstein series $E_{12}(z)$, namely $\Delta \equiv E_{12} \pmod{691}$. Note that 691 divides B_{12}. There are several well-known ways to prove, interpret, and generalize this. Here we will only focus on a generalization to prime level ℓ, where the associated Eisenstein series, for $\varepsilon \in \{\pm 1\}$, even weight $k \geq 2$ and prime level ℓ, is

$$E^{\varepsilon}_{k,\ell}(z) = E_k(z) + \varepsilon \ell^{k/2} E_k(\ell z). \tag{6}$$

Notice that the constant term in the Fourier series of $E^{\varepsilon}_{k,\ell}(z)$ equals $-H^{\varepsilon}_k/2$. Kumar et al. [16] recently established the following result. Throughout this article, given a rational number a, by $p \mid a$, we mean that the prime number p divides the reduced numerator of a, that is $\nu_p(a) \geq 1$.

Theorem 2. *Let k be an even natural integer, ℓ and p be primes. Let $S^{\varepsilon}_k(\ell)$ denote the ε-eigenspace of the Atkin-Lehner operator W_p inside $S_k(\ell)$, the space of modular cusp forms of weight k for the group $\Gamma_0(\ell)$.*
i) *Suppose that $p \geq 5$ divides H_k for some even integer $k \geq 4$. Then there exists $\varepsilon \in \{\pm 1\}$ and a normalized eigenfunction $f \in S^{\varepsilon}_k(\ell)$ for all Hecke operators T_q with $q \neq \ell$ a prime, and a prime ideal $\mathfrak{p}$ over p in the coefficient field of f such that*

$$f \equiv E^{\varepsilon}_{k,\ell} \pmod{\mathfrak{p}}. \tag{7}$$

ii) *Let $\varepsilon \in \{\pm 1\}$ be fixed. Suppose that $p \geq 5$ divides H^{ε}_k for some even integer $k \geq 4$. Then there exists a normalized eigenfunction $f \in S^{\varepsilon}_k(\ell)$ for all Hecke operators T_q with $q \neq \ell$ a prime, and a prime ideal $\mathfrak{p}$ over p in the coefficient field of f such that* (7) *holds.*

If we fix a prime ℓ, we can wonder about the ubiquity of the primes p for which a Ramanujan-congruence (7) for some even integer $k \geq 4$ exists. This amounts to estimating the number of prime divisors $p \leq x$ as x gets large of the sequences $\{H_{2n}\}_{n=1}^{\infty}$ and $\{H^{\varepsilon}_{2n}\}_{n=1}^{\infty}$[1].

It is not so difficult to show (see Lemma 4) that a prime p divides the H-sequence if and only if it is H-irregular or is in the Wieferich set

$$\mathcal{W}_{\ell} = \{p > 2 : \ell^{p-1} \equiv 1 \bmod p^2\}. \tag{8}$$

Likewise, p divides the H^{ε}-sequence if and only if it is H^{ε}-irregular or is in the Wieferich set $\mathcal{W}_{\ell}$ (if $\varepsilon = -1$) or $\mathcal{W}^{+}_{\ell}$ (if $\varepsilon = 1$), where

$$\mathcal{W}^{\varepsilon}_{\ell} = \{p > 2 : \ell^{(p-1)/2} \equiv -\varepsilon \bmod p^2\}, \quad \varepsilon \in \{-1, 1\}. \tag{9}$$

Note that $\mathcal{W}_{\ell} = \mathcal{W}^{-}_{\ell} + \mathcal{W}^{+}_{\ell}$. The Wieferich sets are believed to be very sparse and thus the congruence ubiquity problem in essence amounts to estimating $\mathcal{P}_{H^{\varepsilon}}(x)$, the number of H^{ε}-irregular primes up to x. The results (too lengthy to be stated here) are presented in Sect. 4. We show that

$$\mathcal{P}_{H^{\varepsilon}}(x) > \delta_1 \frac{x}{\log x}, \quad \delta_1 > 0, \quad x \to \infty, \tag{10}$$

[1]For various reasons we included the terms with $n = 1$ as well. It is a consequence of the Kummer congruences that these sequences have the same prime divisors as the ones with the term $n = 1$ left out.

and making heuristical assumptions similar to that of Siegel, we conjecture that

$$\mathcal{P}_{H^\varepsilon}(x) \sim \delta_2 \frac{x}{\log x}, \quad \delta_2 > 0, \quad x \to \infty,$$

with δ_1 and $\delta_2 > \delta_1$ explicit constants. Our constants δ_2 are consistent with numerical data, see Table 2. The inequality (10) can be compared to the best-known result for Bernoulli numbers. Namely, Luca, Pizarro-Madariaga, and Pomerance [19] showed that the number $\mathcal{P}_B(x)$ of irregular primes up to x satisfies

$$\mathcal{P}_B(x) \geq (1 + o(1)) \frac{\log \log x}{\log \log \log x}.$$

In Sec. 7 we extend the above results by restricting to primes in a prescribed arithmetic progression. Given $1 \leq a < d$ coprime integers and a prime ℓ, we define

$$\mathcal{P}_{H^\varepsilon}(d, a) := \{p : p \equiv a \bmod d \text{ and } p \text{ is } H^\varepsilon\text{-irregular}\},\ \varepsilon \in \{-1, 1\}.$$

In order to study the primes in these sets we consider the following related sets:

$$\mathcal{A}_{d,a} = \{p \equiv a \bmod d : \mathrm{ord}_p(\ell) = p - 1\},\ \mathcal{A}^-_{d,a} := \{p \equiv a \bmod d : \mathrm{ord}_p(\ell) = (p-1)/2\}.$$

To these sets we associate infinite sums $\alpha_{d,a}$ and $\alpha^-_{d,a}$ given by (16), respectively (41). Under GRH it follows from general results of Lenstra [18] that these are the respective relative (inside the set of primes $p \equiv a \bmod d$) densities of the sets. The infinite sums $\alpha_{d,a}$ and $\alpha^-_{d,a}$ are given in Euler product form in Theorem 5 (well-known), respectively Theorem 7 (new). Both are rational multiples of the *Artin constant*

$$A = \prod_{\text{prime } p} \Big(1 - \frac{1}{p(p-1)}\Big) = 0.3739558136192022880547280543464\ldots, \tag{11}$$

The set $\mathcal{A}_{d,a}$ has been well-studied, but not so $\mathcal{A}^-_{d,a}$, although some special cases occur in various number theoretical problems, see, e.g., [5, 7, 27].

Theorem 3. *Let ℓ be an odd prime. For $\epsilon > 0$ arbitrary and $\varepsilon \in \{-1, 1\}$ we have*

$$\mathcal{P}_{H^\varepsilon}(d, a)(x) \geq (1 - \delta^\varepsilon_{d,a} - \epsilon) \frac{x}{\varphi(d) \log x},$$

where $\delta^-_{d,a} = \alpha_{d,a} + \alpha^-_{d,a}$. We have $\delta^+_{d,a} = \alpha_{d,a} + \rho_{\ell,1}(a, d)$, where $\rho_{\ell,1}(a, d)$ is the density of prime divisors $p \equiv a \bmod d$ of the sequence $\{\ell^n + 1\}^\infty_{n \geq 1}$. This is always a rational number and is explicitly determined in Moree and Sury [26].

The proof is a quite immediate consequence of the results proved in Section 7 and similar to that of Theorem 4 given in Section 6.1.4. The details are left to the interested reader.

1.2. **Counting ℓ-Genocchi irregular primes.** We let $G = \{G_{2n}\}_{n \geq 1}$ with $G_{2n} := 2\ell n H_{2n} = \ell(1 - \ell^{2n}) B_{2n}$ be the sequence of *ℓ-Genocchi numbers.* The inclusion of the factor ℓ ensures that they are integers. In case $\ell = 2$ we speak about *Genocchi numbers.* These show up in a result similar to Kummer's Theorem 1, see Hu and Kim [13], and it might thus be reasonable to consider them also for arbitrary ℓ. An odd prime p is said to be *ℓ-Genocchi (ir)regular* if and only if it is G-(ir)regular. The first twenty 2-Genocchi irregular primes are

$$17, 31, \mathbf{37}, 41, 43, \mathbf{59}, \mathbf{67}, 73, 89, 97, \mathbf{101}, \mathbf{103}, 109, 113, 127, \mathbf{131}, 137, \mathbf{149}, 151, \mathbf{157},$$

where those that are also B-irregular are put in boldface. There is a considerable literature on the classical Genocchi numbers (Sect. 8.1), but little seems to have been done in the general case (Sect. 8.2). The ℓ-Genocchi irregular primes show up in the study of the prime divisors of H. Namely, a prime p divides the H-sequence if and only if it is ℓ-Genocchi irregular or in the Wieferich set $\mathcal{W}_\ell$ (Proposition 3). As the Wieferich set is believed to be sparse, the study of the prime divisors of H is in essence that of ℓ-Genocchi irregular primes.

Very little is known about the distribution of irregular primes in a prescribed arithmetic progression. We will show that for the ℓ-Genocchi irregular primes the situation is rather different. This is a consequence of the divisor structure of $\ell^{2n}-1$ being much better understood than that of the Bernoulli numerators.

Given $1 \le a < d$ coprime integers and a prime ℓ, we define

$$\mathcal{P}_G(d,a) := \{p : p \equiv a \bmod d \text{ and } p \text{ is } \ell\text{-Genocchi irregular}\}.$$

We are interested in the behavior of $\mathcal{P}_G(d,a)(x)$ as x gets large as compared to that of $\pi(x;d,a) := \#\{p \le x : p \equiv a \bmod d\}$, which is known to behave asymptotically as $x/(\varphi(d)\log x)$. The latter function appears in Theorem 4 and Conjecture 2 and can thus be replaced by $\pi(x;d,a)$. By $\left(\frac{*}{*}\right)$ we denote the Jacobi symbol.

Theorem 4. *Let ℓ be an odd prime. For $\epsilon > 0$ arbitrary we have*

$$\mathcal{P}_G(d,a)(x) \ge (1-\delta_{d,a}-\epsilon)\frac{x}{\varphi(d)\log x},$$

where $\delta_{d,a}$ is given by (30) *and worked out in Euler product form in Theorem 6. We have $1-\delta_{d,a} > 0$. Moreover, either $1-\delta_{d,a} \ge 1/4$, or $4 \mid d$ and $a \equiv 3 \bmod 4$, or $\ell \mid d$ and $\left(\frac{a}{\ell}\right) = -1$.*

A similar result for $\ell = 2$ can be found in Hu et al. [14]. The relative density $1-\delta_{d,a}$ can be arbitrarily close to 0, respectively 1. For particulars see Sect. 6.1.3.

Regarding the true behavior of $\mathcal{P}_G(d,a)(x)$ we make the following conjecture (consistent with numerical data, see Table 3).

Conjecture 2. *Let ℓ be an odd prime. Asymptotically one has*

$$\mathcal{P}_G(d,a)(x) \sim \left(1-\frac{\delta_{d,a}}{\sqrt{e}}\right)\frac{x}{\varphi(d)\log x},$$

where $\delta_{d,a}$ is given by (30) *and worked out in Euler product form in Theorem 6.*

A similar conjecture can be formulated for $\mathcal{P}_{H^\varepsilon}(d,a)(x)$, where one merely replaces $\delta_{d,a}$ by $\delta^\varepsilon_{d,a}$.

By Theorem 6 we have for any odd prime ℓ that $\delta_{d,a} = 0$ if and only if 4ℓ divides d, $\left(\frac{a}{\ell}\right) = 1$ and $a \equiv 1 \bmod 4$. Thus Conjecture 2 leads to the following weaker conjecture.

Conjecture 3. *Let ℓ be an odd prime. The set of ℓ-Genocchi regular primes in the primitive residue class $a \bmod d$ has a positive density, provided we are not in the case where 4ℓ divides d, $\left(\frac{a}{\ell}\right) = 1$ and $a \equiv 1 \bmod 4$. If $\ell = 2$ the density is positive provided we are not in the case where 8 divides d and $a \equiv 1 \bmod 8$.*

The case $\ell = 2$ is not covered by our argumentation, but is Conjecture 1.16 of Hu et al. [14].

2. Preliminaries

2.1. **Basic properties of the numbers H_n.** From (2) we infer that G_{2n} is an integer and H_n an ℓ-integer (that is satisfies $\nu_p(H_{2n}) \ge 0$ for every prime $p \ne \ell$). Put $\zeta_\ell = e^{2\pi i/\ell}$. Using (1) we see that

$$t\sum_{a=1}^{\ell-1}\frac{\zeta_\ell^a}{\zeta_\ell^a - e^t} = \frac{t}{e^t-1} - \frac{\ell t}{e^{\ell t}-1} = \sum_{n=1}^{\infty}\frac{H_n t^n}{(n-1)!}, \tag{12}$$

where the first identity follows on noting that, as formal series,

$$\sum_{a=1}^{\ell-1}\frac{\zeta_\ell^a}{\zeta_\ell^a-e^t}=\sum_{n=0}^{\infty}\left(\sum_{a=1}^{\ell-1}\zeta_\ell^{-an}\right)e^{tn}=-\sum_{\substack{n\ge 0\\ \ell\nmid n}}e^{tn}+(\ell-1)\sum_{\substack{n\ge 0\\ \ell\mid n}}e^{tn}$$

$$=-\sum_{n=0}^{\infty}e^{tn}+\ell\sum_{n=0}^{\infty}e^{\ell tn}=\frac{1}{e^t-1}-\frac{\ell}{e^{\ell t}-1}.$$

If $p-1\nmid 2n$, then Voronoi's congruence (see, for example, Murty [28, Chp. 1]) gives

$$H_{2n}\equiv-\ell^{2n-1}\sum_{j=1}^{p-1}j^{2n-1}\big[\frac{j\ell}{p}\big]\ (\mathrm{mod}\ p),\tag{13}$$

where $[y]$ denotes the greatest integer function.

2.2. **Divisibility of H, H^-, H^+ and the ℓ-Genocchi numbers: elementary observations.** The following trivial result will play an important role. By $\mathrm{ord}_p(\ell)$ we denote the multiplicative order of ℓ modulo p.

Lemma 1. *Let p and ℓ be distinct primes.*
1) *The prime p divides ℓ^n+1 for some integer $n\ge 1$ if and only if $\mathrm{ord}_p(\ell)$ is even.*
2) *The prime p divides ℓ^n+1 for some $1\le n\le (p-3)/2$ if and only if $\mathrm{ord}_p(\ell)$ is even and not equal to $p-1$.*
3) *The prime p divides ℓ^n+1 for some $1\le n\le p-2$ with $n\ne (p-1)/2$ if and only if $\mathrm{ord}_p(\ell)$ is even and not equal to $p-1$.*
4) *The prime p divides ℓ^n-1 for some $1\le n\le (p-3)/2$ if and only if $\mathrm{ord}_p(\ell)<(p-1)/2$.*
5) *The prime p divides ℓ^n-1 for some $1\le n\le p-2$ with $n\ne (p-1)/2$ if and only if $\mathrm{ord}_p(\ell)<(p-1)/2$.*
6) *The prime p divides $\ell^{2n}-1$ for some $1\le n\le (p-3)/2$ if and only if $\mathrm{ord}_p(\ell^2)<(p-1)/2$.*

Proof. Left to the reader (cf. Moree [21, Prop. 2]). □

Remark 1. We will use various times the trivial observation that

$$\mathrm{ord}_p(\ell^2)=\begin{cases}\mathrm{ord}_p(\ell) & \text{if } 2\nmid \mathrm{ord}_p(\ell);\\ \mathrm{ord}_p(\ell)/2 & \text{otherwise.}\end{cases}\tag{14}$$

2.2.1. **The H-sequences.** With the help of Lemma 1 we will now characterize H-, H^-- and H^+-irregular primes.

Lemma 2. *Let $p\ne\ell$ be an odd prime.*
1) *It is H-irregular if and only if it is B-irregular or $\mathrm{ord}_p(\ell^2)<(p-1)/2$.*
2) *It is H^--irregular if and only if it is B-irregular or $\mathrm{ord}_p(\ell)<(p-1)/2$.*
3) *It is H^+-irregular if and only if it is B-irregular or $\mathrm{ord}_p(\ell)$ is even and not equal to $p-1$.*
4) *It is H-irregular if and only if it is either H^-- or H^+-irregular.*
5) *It is both H^-- and H^+-regular if it is B-regular and satisfies $p\equiv 3 \bmod 4$ and $\mathrm{ord}_p(\ell)=(p-1)/2$.*

Proof. The claims are clearly true for $p=3$, and so we may assumue $p>3$. It follows from (2) that the prime factors of the denominator of B_{2n} are precisely those primes p such that $p-1$ divides $2n$. Therefore,

$$\nu_p(B_{2n})=\nu_p(B_{2n}/2n),\quad 1\le n\le (p-3)/2.\tag{15}$$

Suppose that p is H-irregular, i.e. $\nu_p(H_{2n})\ge 1$ for some $1\le n\le (p-3)/2$. By (15) and Lemma 1.6 this is equivalent with p being B-irregular or $\mathrm{ord}_p(\ell^2)<(p-1)/2$.

The proofs of 2) and 3) are analogous, and follow by a similar argument involving Lemma 1. Part 4) is a consequence of the observation that $p \mid \ell^{2n}-1$ if and only if $p \mid \ell^n - 1$ or $p \mid \ell^n+1$. Finally, part 5) follows from parts 2) and 3) on taking into account the identity (14). $\square$

Lemma 3. *Let p be an odd prime and n a positive integer such that $p-1$ divides $2n$. Then we have*

$$\nu_p(H_{2n}) = \nu_p(\ell^{p-1}-1) - 1.$$

Further,

$$\nu_p(H^-_{2n}) = \begin{cases} \nu_p(\ell^{p-1}-1)-1 & \text{if } (p-1) \mid n; \\ \nu_p(\ell^{(p-1)/2}-1)-1 & \text{if } (p-1) \nmid n \text{ and } (\frac{\ell}{p}) = 1; \\ -1-\nu_p(n) & \text{if } (p-1) \nmid n \text{ and } (\frac{\ell}{p}) = -1. \end{cases}$$

Also,

$$\nu_p(H^+_{2n}) = \begin{cases} \nu_p(\ell^{(p-1)/2}+1)-1 & (p-1) \nmid n \text{ and } (\frac{\ell}{p}) = -1; \\ -1-\nu_p(n) & \text{otherwise.} \end{cases}$$

Proof. Write $2n = (p-1)p^e m$, with $p \nmid m$. Then, using (2) and the elementary observation that if $a \equiv 1 \bmod p$ and $a \neq 1$, then $\nu_p(a^j-1) = \nu_p(a-1) + \nu_p(j)$ (cf. Beyl [3]), we find that

$$\nu_p(H_{2n}) = \nu_p(\ell^{2n}-1) + \nu_p(B_{2n}) - \nu_p(2n) = \nu_p(\ell^{p-1}-1) + e - 1 - e = \nu_p(\ell^{p-1}-1) - 1.$$

The two remaining statements are proved similarly, with the difference that whereas $\nu_p(\ell^{2n}-1) > 1$, it can happen that $\nu_p(\ell^n+\varepsilon) = 0$. For the final claim we use that if $a \equiv -1 \bmod p$ and $a \neq -1$ and j is even, then $\nu_p(a^j-1) = \nu_p(a+1) + \nu_p(j)$. $\square$

Recall the definitions (8) and (9) of the Wieferich sets.

Lemma 4. *Let ℓ and $p > 2$ be distinct primes. Then*
1) *p divides the H-sequence if and only if it is H-irregular or is in the Wieferich set $\mathcal{W}_\ell$;*
2) *p divides the H^--sequence if and only if it is H^--irregular or is in the Wieferich set $\mathcal{W}_\ell$;*
3) *p divides the H^+-sequence if and only if it is H^+-irregular or is in the Wieferich set $\mathcal{W}^+_\ell$.*

Proof. We will only deal with cases 2) and 3), since case 1) is similar and easier. It is not difficult to see that only finitely many terms of the H^ε-sequence have to be considered in order to decide whether p divides the sequence or not. Indeed, the Kummer congruence (3) implies that if $p-1 \nmid 2n$, then

$$\frac{B_{2n+r(p-1)}}{2n+r(p-1)}\Big(1+\varepsilon\ell^{n+r(p-1)/2}\Big) \equiv \frac{B_{2n}}{2n}\Big(1+\varepsilon(\frac{\ell}{p})^r\ell^n\Big) \pmod{p}.$$

Thus we have periodicity modulo $p-1$ if $\left(\frac{\ell}{p}\right) = 1$ and modulo $2(p-1)$ otherwise. In particular, if $(p-1) \nmid 2n$ it is enough to consider the p-divisibility of

$$H^\varepsilon_2, H^\varepsilon_4 \ldots, H^\varepsilon_{p-3}, H^\varepsilon_{p+1}, H^\varepsilon_{p+3}, \ldots, H^\varepsilon_{2p-4}$$

The case $p-1 \mid 2n$ is not covered, but for this we invoke Lemma 3, which shows that in this case p divides the H^--sequence if and only p is in $\mathcal{W}_\ell$ and divides the H^+-sequence if and only p is in $\mathcal{W}^+_\ell$. So we restrict now to the case $p-1 \nmid 2n$.

2) Now $\varepsilon = -1$. By Lemma 1.5 the prime p is a divisor if and only if it is B-irregular or $\mathrm{ord}_p(\ell) < (p-1)/2$. By Lemma 2.2 this is equivalent with p being H^--irregular.

3) Now $\varepsilon = 1$. By Lemma 1.3 the prime p is a divisor if and only if it is B-irregular or $\mathrm{ord}_p(\ell)$ is even and not equal to $p-1$. By Lemma 2.3 this is equivalent with p being H^+-irregular. $\square$

2.2.2. **The ℓ-Genocchi numbers.** Since $H_n = G_n/\ell n$, it is natural to wonder how H-(ir)regular and ℓ-Genocchi (ir)regular primes are related.

Proposition 1. *An odd prime $p \neq \ell$ is H-irregular if and only if p is ℓ-Genocchi irregular. If $\ell > 3$, then ℓ is ℓ-Genocchi irregular, and ℓ is H-irregular if and only if it is B-irregular.*

Proof. If $p \neq \ell$, then for every $n = 1, 2, \dots, (p-3)/2$, since p and $p-1$ do not divide $2n$, we have that $\nu_p(H_{2n}) = \nu_p(G_{2n})$. If $\ell > 3$, then for every $n = 1, 2, \dots, (\ell-3)/2$, since ℓ and $\ell - 1$ do not divide $2n$, we have that $\nu_\ell(\ell(1-\ell^{2n})B_{2n}) \geq 1$, and $\nu_\ell((1-\ell^{2n})B_{2n}/2n) = \nu_\ell(B_{2n})$. □

In contrast, the prime divisor structure of G- and H-sequences are rather different.

Proposition 2. *Let ℓ be a fixed prime. Given any prime p (for $\ell \leq 3$ we suppose $p \neq \ell$), there exists an integer n such that $v_p(G_{2n}) \geq 1$. If $\ell \leq 3$, then $v_\ell(G_{2n}) = 0$ for all n.*

Proof. If $p \neq \ell$, we take $2n = p(p-1)$. Then $\ell^{2n} \equiv 1 \bmod p^2$ and $\nu_p(B_{2n}) = -1$, so that $\nu_p(G_{2n}) \geq 1$. If $p = \ell$ (and $\ell > 3$), then we take $n = (\ell-3)/2$ and find that $\nu_\ell(G_{2n}) \geq 1$. If $\ell \leq 3$, then $\ell - 1 \mid 2n$ and hence $\nu_\ell(B_{2n}) = -1$, so that $\nu_\ell(G_{2n}) = 0$. □

Proposition 3. *A prime p divides the H-sequence if and only if it is ℓ-Genocchi irregular or in the Wieferich set $\mathcal{W}_\ell$.*

Proof. This follows on combining Lemma 4.1 and Proposition 1. □

Proposition 4. *Let ℓ be a prime. An odd prime p, with $p \neq \ell$, is ℓ-Genocchi regular if and only if it is B-regular and* $\mathrm{ord}_p(\ell^2) = (p-1)/2$.

Proof. For $\ell = 2$ it was shown by Hu et al. [14, Theorem 1.8]. For the remaining ℓ it follows from Proposition 1 and Lemma 2.1. □

Corollary 1. *Let ℓ be a prime. If* $p \equiv 1 \bmod 4$ *and* $\left(\frac{\ell}{p}\right) = 1$, *then p is ℓ-Genocchi irregular.*

Proof. By contradiction. Suppose that $\mathrm{ord}_p(\ell^2) = (p-1)/2$. The assumption $p \equiv 1 \bmod 4$ ensures that $\mathrm{ord}_p(\ell) = p - 1$, contradicting the assumption that $\left(\frac{\ell}{p}\right) = 1$. □

Proposition 5. *Let ℓ be a prime. If p is congruent to an odd square modulo 4ℓ, then p is ℓ-Genocchi irregular.*

For $\ell = 2$ one verifies this directly. For odd ℓ it follows from Corollary 1 on making use of an alternate form of the law of quadratic reciprocity, initially conjectured by Euler, cf. Cox [6, p. 15].

Lemma 5. *If p and q are distinct odd primes, then $\left(\frac{q}{p}\right) = 1$ if and only if* $p \equiv \pm\beta^2 \bmod 4q$ *for some odd integer β.*

3. Further preliminaries

We recall some relevant results and conjectures from the literature.

3.1. **Primitive roots in arithmetic progression.** Put

$$\mathcal{A}_{d,a} = \{p : p \equiv a \bmod d,\ \mathrm{ord}_p(\ell) = p - 1\}.$$

Under GRH the natural density of this set is given by

$$\alpha_{d,a} = \sum_{n=1}^{\infty} \frac{\varphi(d)\mu(n)c_a(n)}{[\mathbb{Q}(\zeta_{[d,n]}, \ell^{1/n}) : \mathbb{Q}]}, \tag{16}$$

where $c_a(n) = 1$ if the automorphism σ_a of $\mathbb{Q}(\zeta_d)$ determined by $\sigma_a(\zeta_d) = \zeta_d^a$ is the identity on the field $\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_n, \ell^{1/n})$, and $c_a(n) = 0$ otherwise. Its Euler product form was first evaluated by Moree [22] for arbitrary ℓ. In the relevant case for us where ℓ is an odd prime, this result takes on a rather simpler form.

Theorem 5. *Let a and d be coprime integers and ℓ be an odd prime. Put*
$$\alpha_{d,a} = A\, c_1(d,a)\, R(d,a),$$
with
$$R(d,a) = \prod_{p\mid(a-1,d)}\left(1-\frac{1}{p}\right)\prod_{p\mid d}\left(1+\frac{1}{p^2-p-1}\right) \tag{17}$$
and
$$c_1(d,a) = \begin{cases} 1-\left(\frac{\ell}{a}\right) & \text{if } \ell\equiv 1 \bmod 4, \ell\mid d;\\ 1+\frac{1}{\ell^2-\ell-1} & \text{if } \ell\equiv 1 \bmod 4, \ell\nmid d;\\ 1-\left(\frac{\ell}{a}\right) & \text{if } \ell\equiv 3 \bmod 4, 4\mid d, \ell\mid d;\\ 1+\left(\frac{-1}{a}\right)\frac{1}{\ell^2-\ell-1} & \text{if } \ell\equiv 3 \bmod 4, 4\mid d, \ell\nmid d;\\ 1 & \text{if } \ell\equiv 3 \bmod 4, 4\nmid d.\end{cases}$$
Let $\epsilon > 0$ be any fixed real number. Then, for every x sufficiently large,
$$\mathcal{A}_{d,a}(x) \le (\alpha_{d,a}+\epsilon)\frac{x}{\varphi(d)\log x}. \tag{18}$$
Assuming GRH, we have
$$\mathcal{A}_{d,a}(x) = \frac{\alpha_{d,a}}{\varphi(d)}\frac{x}{\log x} + O_d\left(\frac{x\log\log x}{\log^2 x}\right).$$

The unconditional upper bound (18) is not given by Moree in either [22] or [23], but is totally standard and for a related problem worked out in detail in Hu et al. [14].

We note for future use that if d is odd, then
$$R(d,a) = \begin{cases} R(2d,a) & \text{if } 2\nmid a;\\ R(2d,a+d) & \text{otherwise.}\end{cases} \tag{19}$$

Remark 2. Let Δ denote the discriminant of $\mathbb{Q}(\sqrt{\ell})$. In case $\Delta \mid d$ and $\left(\frac{\ell}{a}\right) = 1$, then using quadratic reciprocity it is easy to see that $\mathcal{A}_{d,a}$ is empty and so unconditionally $\alpha_{d,a} = 0$. By Theorem 5, under GRH, $\alpha_{d,a} = 0$ if and only if $\Delta \mid d$ and $\left(\frac{\ell}{a}\right) = 1$.

3.2. **Near-primitive roots.** Given integers $t \ge 1$ and g, we set
$$\mathcal{P}(g,t) := \{p : p \equiv 1 \bmod t, \quad \mathrm{ord}_p(g) = (p-1)/t\}.$$
The primes in $\mathcal{P}(g,t)$ are called *near-primitive roots*. Let $\epsilon > 0$ be fixed. By [14, Theorem 3.1] we have
$$\mathcal{P}(g,t)(x) \le (\delta(g,t)+\epsilon)\frac{x}{\log x}, \tag{20}$$
for every x sufficiently large, where
$$\delta(g,t) = \sum_{n=1}^{\infty}\frac{\mu(n)}{[\mathbb{Q}(\zeta_{nt}, g^{1/nt}) : \mathbb{Q}]}.$$
Assuming the Riemann Hypothesis for all number fields $\mathbb{Q}(\zeta_{nt}, g^{1/nt})$ with n squarefree, we have the sharper estimate
$$\mathcal{P}(g,t)(x) = \delta(g,t)\frac{x}{\log x} + O_{g,t}\left(\frac{x\log\log x}{\log^2 x}\right). \tag{21}$$
Thus, conditionally, the set of primes $\mathcal{P}(g,t)$ has natural density $\delta(g,t)$. This quantity was explicitly computed for $t = 1$ by Hooley [12] and for general t by Moree [25]. It always equals a rational number times the Artin constant, where the rational number may depend on both g and t.

3.3. **Divisors of second order recurrences.** Let α and β be integers. The set of prime divisors $\mathcal{Q}_{\alpha,\beta}$ of the sequence $\{\alpha^n+\beta^n\}_{n=1}^{\infty}$ has been well studied. A prime $p\nmid\alpha\beta$ divides it if and only if $\mathrm{ord}_p(\alpha/\beta)$ is even (Moree [21, Prop. 2]). Let $\mathcal{Q}_{\alpha,\beta}(a,d)$ be the set of primes $p\equiv a \bmod d$ in $\mathcal{Q}_{\alpha,\beta}$. Moree and Sury [26] showed that in case $\alpha/\beta>0$, asymptotically,

$$\mathcal{Q}_{\alpha,\beta}(a,d)(x)=\rho_{\alpha,\beta}(a,d)\frac{x}{\log x}+O\Big(\frac{x\log\log x}{\log^{7/6}x}\Big),\quad x\to\infty, \tag{22}$$

where $\rho_{\alpha,\beta}(c,d)$ is an explicitly computable rational number. For an informal proof in case $a=d=1$ and other references see [24, Sect. 9.2].

3.4. **Wieferich sets.** Recall the definitions (8) and (9) of the Wieferich sets. The first case of Fermat's Last Theorem (FLTI) is the statement that, for any odd prime p, the equation $x^p+y^p=z^p$ does not have positive integer solutions where none of x,y,z is divisible by p. The *generalized Wieferich criterion* (for given q) is the statement that if FLTI fails for some prime p, then $p\in\mathcal{W}_q$. This criterion has been proved by Granville and Monagan [10] for all $q\in\{2,3,5,7,\ldots,89\}$, the first 24 primes, continuing work by a great number of mathematicians, starting with Wieferich ($q=2$) and Mirimanoff ($q=3$). For $q=2$ the only Wieferich numbers known below 10^{17} are 1093 and 3511. For more information see `https://en.wikipedia.org/wiki/Wieferich_prime`. It is believed that $\mathcal{W}_\ell(x)=O(\log\log x)$, but it is not even known whether $\mathcal{W}_\ell(x)=o(x/\log x)$ or not. The same is expected for $\mathcal{W}_\ell^{\varepsilon}(x)$.

4. Counting H^-- and H^+-irregular primes

In Section 7 we will count H^-- and H^+-irregular primes in prescribed arithmetic progression, here as a warm-up we consider the problem of counting *all* such primes.

Denote by $\mathcal{P}_{H^\varepsilon}$ the set of H^ε-irregular primes. By Lemma 2, (20) and (22), we obtain unconditionally

$$\mathcal{P}_{H^-}(x)\ge(1-\delta(\ell,1)-\delta(\ell,2)-\epsilon)\frac{x}{\log x} \tag{23}$$

and

$$\mathcal{P}_{H^+}(x)\ge(\rho_{\ell,1}(1,1)-\delta(\ell,1)-\epsilon)\frac{x}{\log x}, \tag{24}$$

where $\epsilon>0$ is arbitrary.

Conjecture 4. *If we require the primes counted by $\mathcal{P}(g,t)$ and $\mathcal{Q}_{\alpha,\beta}$ to be also B-regular, then the estimates* (21) *and* (22) *hold with $\delta(g,t)$ and $\rho_{\alpha,\beta}(a,d)$ replaced by $\delta(g,t)/\sqrt{e}$, respectively $\rho_{\alpha,\beta}(a,d)/\sqrt{e}$.*

This conjecture leads to the conjectures that

$$\mathcal{P}_{H^-}(x)\sim\Big(1-\frac{1}{\sqrt{e}}(\delta(\ell,1)+\delta(\ell,2)\Big)\frac{x}{\log x} \tag{25}$$

and

$$\mathcal{P}_{H^+}(x)\sim\Big(1-\frac{1}{\sqrt{e}}(1-\rho_{\ell,1}(1,1)+\delta(\ell,1)\Big)\frac{x}{\log x}. \tag{26}$$

For reasons of space we abstain from writing out (23), (24), (25), and (26) explicitly, but this can be done easily using the following lemma.

Lemma 6. *Let A be the Artin constant defined in* (11)*. If $\ell=2$, then $\delta(2,1)=A$ and $\delta(2,2)=3A/4$. If $\ell\equiv 1 \bmod 4$, then*

$$\delta(\ell,1)=A\left(1+\frac{1}{\ell^2-\ell-1}\right)\qquad\textit{and}\qquad\delta(\ell,2)=\frac{3A}{4}\left(1-\frac{1}{\ell^2-\ell-1}\right).$$

If $\ell \equiv 3 \bmod 4$, *then*

$$\delta(\ell,1) = A \qquad \textit{and} \qquad \delta(\ell,2) = \frac{3A}{4}\left(1 + \frac{1}{3(\ell^2-\ell-1)}\right).$$

We have $\rho_{2,1}(1,1) = 17/24$ *and* $\rho_{\ell,1}(1,1) = 2/3$ *for every odd prime* ℓ.

The quantities $\delta(\ell,1)$ and $\delta(\ell,2)$ are, for example, computed in Moree [25]. The results for $\rho_{\ell,1}(1,1)$ were proved by Hasse [11] for Dirichlet density and by Odoni [29] for natural density (which is what we use here).

5. Counting ℓ-Genocchi irregular primes

Recall that by Proposition 1, counting ℓ-Genocchi irregular primes is, except possibly for $p = \ell$, the same as counting H-irregular primes. Corollary 1 implies that

$$\mathcal{P}_G(x) \geq \left(\frac{1}{4} - \epsilon\right)\frac{x}{\log x}.$$

By Proposition 4, given $\epsilon > 0$ arbitrary and fixed, we have for every x sufficiently large

$$\mathcal{P}_G(x) \geq \left(1 - \delta(\ell^2,2) - \epsilon\right)\frac{x}{\log x},$$

Assuming Siegel's heuristic we conjecture that

$$\mathcal{P}_G(x) \sim \left(1 - \frac{\delta(\ell^2,2)}{\sqrt{e}}\right)\frac{x}{\log x}. \tag{27}$$

By [14, Theorem 1.10] for $\ell = 2$, and the results of [25] for ℓ odd, we obtain

$$\mathcal{P}_G(x) \geq \left(1 - \frac{3}{2}A - \epsilon\right)\frac{x}{\log x} \quad \text{and} \quad \mathcal{P}_G(x) \geq \left(1 - \frac{3A}{2}\left(1 + \frac{1}{3(\ell^2-\ell-1)}\right) - \epsilon\right)\frac{x}{\log x}, \tag{28}$$

respectively, where $\epsilon > 0$ is arbitrary and fixed and x sufficiently large. For ϵ small enough, the constants involved are in the interval $(0.4, 0.44)$. We conjecture that

$$\mathcal{P}_G(x) \sim \left(1 - \frac{3A}{2\sqrt{e}}\right)\frac{x}{\log x}\ (\ell = 2) \ \text{ and } \ \mathcal{P}_G(x) \sim \left(1 - \frac{3A}{2\sqrt{e}}\left(1 + \frac{1}{3(\ell^2-\ell-1)}\right)\right)\frac{x}{\log x}\ (\ell > 2),$$

with now the constants involved being in $(0.637, 0.66)$. See Table 1 for some numerical examples supporting these conjectures.

6. Irregular primes in arithmetic progression

The goal of this section is proving the main result of this paper, namely Theorem 4. For $\ell = 2$ this was already considered in [14, Sect. 1.3.1]. Further, we study the extremal behavior of $\delta_{d,a}$.

6.1. **The ℓ-Genocchi case.** Let ℓ be an odd prime number and $1 \leq a < d$ be coprime integers. In this section we consider the set of rational (odd) primes

$$\mathcal{P}_{d,a} := \{p \equiv a \bmod d : \mathrm{ord}_p(\ell^2) = (p-1)/2\}. \tag{29}$$

By Proposition 4 the primes in $\mathcal{P}_{d,a}$ are irregular. Under GRH we have (see [14, Theorem 3.1])

$$\lim_{x\to\infty} \frac{\mathcal{P}_{d,a}(x)}{\pi(x;d,a)} = \delta_{d,a},$$

with

$$\delta_{d,a} = \sum_{n=1}^{\infty} \frac{\varphi(d)\mu(n)c_a(n)}{[\mathbb{Q}(\zeta_{[d,2n]}, \ell^{1/n}) : \mathbb{Q}]}, \tag{30}$$

where $c_a(n) = 1$ if the automorphism σ_a of $\mathbb{Q}(\zeta_d)$ determined by $\sigma_a(\zeta_d) = \zeta_d^a$ is the identity on the field $\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{2n}, \ell^{1/n})$, and $c_a(n) = 0$ otherwise.

We will now express $\delta_{d,a}$ as an Euler product in two different ways: one more starting from first principles and another shorter one relying more heavily on existing results.

Theorem 6. *Let a and d be coprime integers, $\mathcal{P}_{d,a}$ and $\delta_{d,a}$ as in (29), respectively (30), and $\epsilon > 0$ be arbitrary and fixed. Then for every x sufficiently large we have*

$$\mathcal{P}_{d,a}(x) \leq (\delta_{d,a} + \epsilon)\frac{x}{\varphi(d)\log x}, \tag{31}$$

where

$$\delta_{d,a} = A\, c(d,a)\, R(d,a),$$

with $R(d,a)$ as in (17) and

$$c(d,a) = \begin{cases} \frac{1}{2}\left(3 + \frac{1}{\ell^2-\ell-1}\right) & \text{if } \ell \nmid d, 4 \nmid d; \\ 1 + \frac{1}{\ell^2-\ell-1} & \text{if } \ell \nmid d, 4 \mid d, a \equiv 1 \bmod 4; \\ 1 & \text{if } \ell \mid d, 4 \nmid d, \left(\frac{a}{\ell}\right) = 1; \\ 2 & \text{if } 4 \mid d \text{ and } a \equiv 3 \bmod 4, \text{ or } \ell \mid d \text{ and } \left(\frac{a}{\ell}\right) = -1; \\ 0 & \text{if } 4\ell \mid d, \left(\frac{a}{\ell}\right) = 1, a \equiv 1 \bmod 4. \end{cases}$$

Assuming GRH we have

$$\mathcal{P}_{d,a}(x) = \frac{\delta_{d,a}}{\varphi(d)}\frac{x}{\log x} + O_d\left(\frac{x \log\log x}{\log^2 x}\right).$$

Remark 3. Note that alternatively we can write

$$c(d,a) = \begin{cases} \frac{1}{2}\left(3 + \frac{1}{\ell^2-\ell-1}\right) & \text{if } 4 \nmid d, \ell \nmid d; \\ \frac{1}{2}(3 - (\frac{a}{\ell})) & \text{if } 4 \nmid d, \ell \mid d; \\ 1 + \frac{1}{\ell^2-\ell-1} & \text{if } 4 \mid d, a \equiv 1 \bmod 4, \ell \nmid d; \\ 1 - (\frac{a}{\ell}) & \text{if } 4 \mid d, a \equiv 1 \bmod 4, \ell \mid d; \\ 2 & \text{if } 4 \mid d \text{ and } a \equiv 3 \bmod 4. \end{cases}$$

Remark 4. From Theorem 6 we infer that the analogue of identity (19) holds for $\delta_{d,a}$ as well, which is consistent with the fact that the analogue of this identity also holds for $\mathcal{P}_{d,a}$.

6.1.1. **The proof of Theorem 6.** The proof requires a few preliminary lemmas. The first is merely a special case of Lemma 3.1 of [23].

Lemma 7. *Put*

$$\omega_d(n) := \frac{n\varphi([d,n])}{\varphi(d)}.$$

It is a multiplicative function in n. For $m \geq 1$, let

$$S(m) = \sum_{\substack{n\geq 1,\ m\mid n \\ a\equiv 1 \bmod (d,n)}} \frac{\mu(n)}{\omega_d(n)}, \qquad S_2(m) = \sum_{\substack{n\geq 1,\ [2,m]\mid n \\ a\equiv 1 \bmod (d,n)}} \frac{\mu(n)}{\omega_d(n)}.$$

We have $S_2(m) = -S(m)$. Further, $S(1) = AR(d,a)$ and

$$S(\ell) = \begin{cases} -\frac{A}{\ell^2-\ell-1}R(d,a) & \text{if } \ell \nmid d; \\ -\frac{A}{\ell-1}R(d,a) & \text{if } \ell \mid d, \end{cases}$$

where ℓ is an odd prime.

We recall the law of quadratic reciprocity for the Jacobi symbol: if j and k are odd coprime positive integers, then

$$(\frac{j}{k})(\frac{k}{j}) = (-1)^{(j-1)(k-1)/4}. \tag{32}$$

In the following we set $\ell^* = (-1)^{(\ell-1)/2}\ell$.

Lemma 8. *Let σ_a be the automorphism of $\mathbb{Q}(\zeta_d)$ uniquely determined by $\sigma_a(\zeta_d) = \zeta_d^a$ with a a positive integer coprime to d. If $4\ell \mid d$, then $\sigma_a(\sqrt{\ell}) = \left(\frac{\ell}{a}\right)\sqrt{\ell}$. If $\ell \mid d$, then $\sigma_a(\sqrt{\ell^*}) = \left(\frac{a}{\ell}\right)\sqrt{\ell^*}$.*

Proof. The quadratic Gauss sum expresses $\sqrt{\ell^*}$ as an element in $\mathbb{Q}(\zeta_d)$, which allows one to determine $\sigma_a(\sqrt{\ell^*})$ and from this, using $\sigma_a(i) = i^a$, also $\sigma_a(\sqrt{\ell})$. Invoking (32) we can formulate the outcome in a more compact way. □

Remark 5. This can also be proved using that $\sigma_a(\sqrt{\ell})/\sqrt{\ell}$ is a character, see [23, Lemma 2.1].

Lemma 9. *Let n be a squarefree integer. If n is odd, or $\ell \mid n$, or n is even and $\ell \nmid nd$, then we have: $c_a(n) = 1$ if and only if $a \equiv 1 \bmod (d, 2n)$. If n is even, $\ell \nmid n$ and $\ell \mid d$, then we have: $c_a(n) = 1$ if and only if $a \equiv 1 \bmod (d, 2n)$ and $\left(\frac{a}{\ell}\right) = 1$.*

Proof. Let us set $I := \mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{2n}, \ell^{1/n})$. By Kummer theory we may argue that, since $\mathbb{Q}(\zeta_\infty) \cap \mathbb{Q}(\zeta_{2n}, \ell^{1/n})$ is a finite abelian extension of $\mathbb{Q}(\zeta_{2n})$, it is of the form $\mathbb{Q}(\zeta_{2n}, \ell^{e/n})$ for some $e \geq 0$, and hence by Schinzel's Theorem [31, Theorem 2] it is either $\mathbb{Q}(\zeta_{2n})$ if n is odd, or $\mathbb{Q}(\zeta_{2n}, \sqrt{\ell})$ if n is even. The latter extension equals $\mathbb{Q}(\zeta_{2n})$ if $\ell \mid n$ (as $\mathbb{Q}(\sqrt{\ell}) \subseteq \mathbb{Q}(\zeta_{4\ell})$ and we already have that n is even).

Thus, if n is odd or $\ell \mid n$, we deduce that $I = \mathbb{Q}(\zeta_{(d,2n)})$. For n even with $\ell \nmid n$, it suffices to notice that $\mathbb{Q}(\sqrt{\ell^*})$ is contained in $\mathbb{Q}(\zeta_d)$ if and only if $\ell \mid d$. If $\ell \nmid d$, then we have $I = \mathbb{Q}(\zeta_{(d,2n)})$. If $\ell \mid d$, then noticing that $\mathbb{Q}(\zeta_{(d,2n)}) \subseteq I \subseteq \mathbb{Q}(\zeta_{(d,2n)}, \zeta_\ell)$, we deduce that $I = \mathbb{Q}(\zeta_{(d,2n)}, \sqrt{\ell^*})$ (where $\mathbb{Q}(\sqrt{\ell^*})$ is not contained in $\mathbb{Q}(\zeta_{(d,2n)})$).

If $I = \mathbb{Q}(\zeta_{(d,2n)})$, then the automorphism σ_a fixes I if and only if $a \equiv 1 \bmod (d, 2n)$. Suppose now that $I = \mathbb{Q}(\zeta_{(d,2n)}, \sqrt{\ell^*})$ and $\mathbb{Q}(\sqrt{\ell^*}) \not\subseteq \mathbb{Q}(\zeta_{(d,2n)})$. By Lemma 8 the automorphism σ_a fixes $\mathbb{Q}(\sqrt{\ell^*}) \subseteq \mathbb{Q}(\zeta_\ell)$ if and only if a is a square modulo ℓ, i.e. $\left(\frac{a}{\ell}\right) = 1$. □

Remark 6. Let n be a squarefree number. We collect here some technical details on the numbers $(d, 2n)$ and $[d, 2n]$, and on the condition $a \equiv 1 \bmod (d, 2n)$.

- If d is odd, or $4 \nmid d$ and n is even, then $(d, 2n) = (d, n)$ and $[d, 2n] = 2[d, n]$.
- If d is even and n is odd, or $4 \mid d$, then $(d, 2n) = 2(d, n)$ and $[d, 2n] = [d, n]$.

If d is even and n is odd, then we have $a \equiv 1 \bmod 2(d, n)$ if and only if $a \equiv 1 \bmod (d, n)$, because a must be odd. If $4 \mid d$ and n is even, then $a \equiv 1 \bmod 2(d, n)$ holds only if $a \equiv 1 \bmod 4$, and in this case $a \equiv 1 \bmod 2(d, n)$ is equivalent to $a \equiv 1 \bmod (d, n)$.

Proof of Theorem 6. Recall that the degree $[\mathbb{Q}(\zeta_{[d,2n]}, \ell^{1/n}) : \mathbb{Q}]$ equals $\varphi([d, 2n])n/2$ if n is even and $\ell \mid [d, n]$, and it equals $\varphi([d, 2n])n$ otherwise. For the computation of the density $\delta_{d,a}$ we distinguish the cases $\ell \nmid d$ and $\ell \mid d$.

Case 1: $\ell \nmid d$. Using Lemma 9 we see that the expression (30) simplifies to

$$\delta_{d,a} = \sum_{\substack{n \geq 1 \\ a \equiv 1 \bmod (d,2n)}} \frac{\varphi(d)\mu(n)}{[\mathbb{Q}(\zeta_{[d,2n]}, \ell^{1/n}) : \mathbb{Q}]}.$$

In view of the degree formulas, we obtain

$$\delta_{d,a} = \Bigg(\sum_{\substack{n\geq 1 \\ a\equiv 1 \bmod (d,2n)}} + \sum_{\substack{2\ell \mid n \\ a\equiv 1 \bmod (d,2n)}} \Bigg) \frac{\mu(n)}{\omega_d(n)}, \tag{33}$$

with $\omega_d(n)$ as in Lemma 7.

Case 1.1: $4 \nmid d$. By Remark 6, from (33) we have

$$\begin{aligned}\delta_{d,a} &= \Bigg(\sum_{\substack{2\nmid n \\ a\equiv 1 \bmod (d,n)}} + \frac{1}{2} \sum_{\substack{2\mid n \\ a\equiv 1 \bmod (d,n)}} + \frac{1}{2} \sum_{\substack{2\ell\mid n \\ a\equiv 1 \bmod (d,n)}} \Bigg) \frac{\mu(n)}{\omega_d(n)} \\ &= \Bigg(\sum_{\substack{n\geq 1 \\ a\equiv 1 \bmod (d,n)}} - \frac{1}{2} \sum_{\substack{2\mid n \\ a\equiv 1 \bmod (d,n)}} + \frac{1}{2} \sum_{\substack{2\ell\mid n \\ a\equiv 1 \bmod (d,n)}} \Bigg) \frac{\mu(n)}{\omega_d(n)}.\end{aligned}$$

Then using Lemma 7 we obtain

$$\delta_{d,a} = S(1) - \frac{1}{2}S_2(1) + \frac{1}{2}S_2(\ell) = \frac{1}{2}\left(3S(1) - S(\ell)\right) = \frac{A}{2}\left(3 + \frac{1}{\ell^2 - \ell - 1}\right) R(d,a).$$

Case 1.2: $4 \mid d$. In view of Remark 6, if $a \equiv 1 \bmod 4$, then (33) becomes

$$\delta_{d,a} = \Bigg(\sum_{\substack{n\geq 1 \\ a\equiv 1 \bmod (d,n)}} + \sum_{\substack{2\ell\mid n \\ a\equiv 1 \bmod (d,n)}} \Bigg) \frac{\mu(n)}{\omega_d(n)} = S(1) + S_2(\ell) = A\left(1 + \frac{1}{\ell^2 - \ell - 1}\right) R(d,a).$$

If $a \equiv 3 \bmod 4$, then from (33) we are left with

$$\delta_{d,a} = \sum_{\substack{2\nmid n \\ a\equiv 1 \bmod (d,2n)}} \frac{\mu(n)}{\omega_d(n)} = 2S(1) = 2AR(d,a). \tag{34}$$

Case 2: $\ell \mid d$. We distinguish the two cases: a is a square modulo ℓ or not.

Case 2.1: $\left(\frac{a}{\ell}\right) = -1$. Notice that the condition $a \equiv 1 \bmod (d, 2n)$ implies in particular that $\ell \nmid n$, otherwise we would have $a \equiv 1 \bmod \ell$ and hence a contradiction with the assumption. Thus, by Lemma 9 and Remark 6 we have

$$\delta_{d,a} = \sum_{\substack{2\nmid n \\ a\equiv 1 \bmod (d,n)}} \frac{\mu(n)}{\omega_d(n)} = S(1) - S_2(1) = 2AR(d,a).$$

Case 2.2: $\left(\frac{a}{\ell}\right) = 1$. By Lemma 9 we obtain

$$\delta_{d,a} = \sum_{\substack{n\geq 1 \\ a\equiv 1 \bmod (d,2n)}} \frac{\varphi(d)\mu(n)}{[\mathbb{Q}(\zeta_{[d,2n]}, \ell^{1/n}) : \mathbb{Q}]} = \Bigg(\sum_{\substack{2\nmid n \\ a\equiv 1 \bmod (d,2n)}} + 2 \sum_{\substack{2\mid n \\ a\equiv 1 \bmod (d,2n)}} \Bigg) \frac{\mu(n)}{\omega_d(n)}.$$

In the following we take Remark 6 into account. If $4 \nmid d$, then

$$\delta_{d,a} = S(1) = AR(d,a).$$

If $4 \mid d$ and $a \equiv 1 \bmod 4$, then

$$\delta_{d,a} = S(1) + S_2(1) = 0.$$

If $4 \mid d$ and $a \equiv 3 \bmod 4$, then

$$\delta_{d,a} = S(1) - S_2(1) = 2AR(d,a). \qquad \square$$

6.1.2. **Alternative proof of Theorem 6.**

Proof of Theorem 6. We start by noting, cf. (14), that

$$\mathcal{P}_{d,a} = \{p : p \equiv a \bmod d,\ \mathrm{ord}_p(\ell) = p-1 \text{ or } p \equiv 3 \bmod 4 \text{ and } \mathrm{ord}_p(\ell) = (p-1)/2\}. \tag{35}$$

Without loss of generalization we may assume that 4 divides d: if $4 \nmid d$ we split the progression into two, according to whether $a \equiv 1 \bmod 4$ or $a \equiv 3 \bmod 4$, and add the results. Thus, if $a \equiv 1 \bmod 4$, then we just have

$$\mathcal{P}_{d,a} = \{p : p \equiv a \bmod d,\ \mathrm{ord}_p(\ell) = p-1\}.$$

Using Theorem 5 and the law of quadratic reciprocity we conclude that

$$\delta_{d,a} = AR(d,a)c(d,a) \text{ with } c(d,a) = \begin{cases} 1-\left(\frac{a}{\ell}\right) & \text{if } a \equiv 1 \bmod 4,\ \ell \mid d; \\ 1+\frac{1}{\ell^2-\ell-1} & \text{if } a \equiv 1 \bmod 4,\ \ell \nmid d. \end{cases} \tag{36}$$

If $a \equiv 3 \bmod 4$, then by (34) we arrive at

$$\delta_{d,a} = AR(d,a)c(d,a), \text{ with } c(d,a) = 2.$$

Now let us suppose that $4 \nmid d$. We put $d_1 = \mathrm{lcm}(4,d)$. We let a_1 and a_3 be integers such that $a_j \equiv a \bmod d$ and $a_j \equiv j \bmod 4$. Noting that $R(d_1,a_j) = R(d,a)$ and $\varphi(d_1) = 2\varphi(d)$, we conclude that

$$\delta_{d,a} = \frac{\delta_{d_1,a_1} + \delta_{d_1,a_3}}{2} = \frac{A}{2}(c(d_1,a_1) + c(d_1,a_3))R(d,a).$$

We find that $c(d_1,a_3) = 2$ and noticing that if $\ell \mid d$, then we have $\left(\frac{a_1}{\ell}\right) = \left(\frac{a}{\ell}\right)$, we obtain from (36) that

$$c(d_1,a_1) = \begin{cases} 1-\left(\frac{a}{\ell}\right) & \text{if } \ell \mid d; \\ 1+\frac{1}{\ell^2-\ell-1} & \text{if } \ell \nmid d. \end{cases}$$

The proof (with the reformulation of $c(d,a)$ as given in Remark 3) is now easily completed. □

Example 1. Take $d = 4$ and $\ell = 3$. Moree and Zumalacárregui [27] crucially made use of the sets $\mathcal{P}_{4,1}$ and $\mathcal{P}_{4,3}$ in their solution of a conjecture of Salajan. By a simple direct computation they showed that $\delta_{4,1} = 6A/5$ and $\delta_{4,3} = 2A$ [27, Appendix A], in agreement with our results. These sets play also an important role in the resolution of Browkin's generalization of the Salajan conjecture by Ciolan and Moree [5].

6.1.3. **The extremal behavior of $\delta_{d,a}$.** Theorem 4 gives a lower bound for $\mathcal{P}_G(d,a)(x)$. In this section we will study how small and large this lower bound can be. For $\ell = 2$ this was done in [14, Sect. 2.2]. This amounts to bounding $\delta_{d,a}$, which a priori satisfies $0 \le \delta_{d,a} \le 1$, as it is a relative density.

Small $\delta_{d,a}$. We put

$$G(d) = A\prod_{p \mid d}\left(1 + \frac{1}{p^2-p-1}\right).$$

Note that

$$G(d) = \prod_{p \nmid d}\left(1 - \frac{1}{p(p-1)}\right) < 1.$$

Recall that

$$AR(d,a) = G(d)\prod_{p \mid (a-1,d)}\left(1 - \frac{1}{p}\right).$$

If d is even, then $(a-1,d)$ is even and we infer that $AR(d,a)<1/2$. If d is odd, then $G(d)<1/2$ and again $AR(d,a)<1/2$. As $c(d,a)\le 2$, we infer that

$$\delta_{d,a}=AR(d,a)c(d,a)<1.$$

Clearly

$$AR(d,a)\ge AR(d,1)=\frac{\varphi(d)}{d}G(d).$$

The ratio $\varphi(d)/d$ takes on local minima on products of consecutive primes. For these products we see that $G(d)$ tends to 1, on noting that

$$\prod_{p\ge q}\Big(1-\frac{1}{q(q-1)}\Big)=1+O\Big(\frac{1}{q}\Big). \tag{37}$$

Using this and Mertens' theorem (see [1, Theorem 13.13]), with γ Euler's constant,

$$\prod_{p\le x}\Big(1-\frac{1}{p}\Big)\sim\frac{e^{-\gamma}}{\log x}, \tag{38}$$

we can then infer that

$$\liminf_{d\to\infty}AR(d,1)\log\log d=e^{-\gamma}. \tag{39}$$

The argument is similar to that of the proof of the classical result (see, for instance, [1, Theorem 13.14])

$$\liminf_{d\to\infty}\frac{\varphi(d)}{d}\log\log d=e^{-\gamma}.$$

Proposition 6. *Let ℓ be a prime. We have*

$$\liminf_{d\to\infty}\min_{\substack{1\le a<d\\(a,d)=1\\\delta_{d,a}>0}}\delta_{d,a}\log\log d=e^{-\gamma}.$$

Proof. For $\ell=2$ this result is Proposition 2.3 of [14]. Our proof for odd ℓ is in the same spirit.

If $\delta_{d,a}>0$, then $c(d,a)\ge 1$. Hence $\delta_{d,a}\log\log d\ge AR(d,a)\log\log d\ge AR(d,1)\log\log d$. It now follows from (39) that the limes inferior is $\ge e^{-\gamma}$. In order to show that this bound is actually sharp we will show that $\lim_{n\to\infty}\delta_{d_n,1}=e^{-\gamma}$, where $d_n=\prod_{3\le p\le n}p$.

Let $n\ge\ell$ be arbitrary. We have $c(d_n,1)=1$ and

$$\delta_{d_n,1}=\Big(1+O\Big(\frac{1}{n}\Big)\Big)\prod_{2\le p\le n}\Big(1-\frac{1}{p}\Big),$$

where we used that

$$\prod_{p\nmid d_n}\Big(1-\frac{1}{p(p-1)}\Big)=\frac{1}{2}\prod_{p>n}\Big(1-\frac{1}{p(p-1)}\Big)=\frac{1}{2}+O\Big(\frac{1}{n}\Big),$$

with the last equality following from (37). Using Mertens' theorem (38) and the prime number theorem in the form $\log d_n\sim n$, we deduce that, as n tends to infinity,

$$\delta_{d_n,1}\sim\frac{e^{-\gamma}}{\log n}\sim\frac{e^{-\gamma}}{\log\log d_n},$$

completing the proof. $\square$

Large $\delta_{d,a}$. Proposition 7 gives information on how large $\delta_{d,a}$ can be. In its proof we make use of the elementary concepts of a- and d-sequence, which we now introduce. Let $q_1, q_2, \ldots$ be a, possibly finite, sequence of pairwise coprime integers and $\alpha_1, \alpha_2, \ldots$ any integer sequence of equal length. Put $d_k = \prod_{j=1}^{k} q_j$. By the Chinese remainder theorem the system of congruences

$$x \equiv \alpha_1 \bmod q_1,\ x \equiv \alpha_2 \bmod q_2, \ldots,\ x \equiv \alpha_k \bmod q_k, \tag{40}$$

is equivalent with

$$x \equiv a_k \bmod d_k, \quad 0 \le a_k < d_k,$$

with a_k unique (which is a consequence of the Chinese remainder theorem). Thus to the system (40) we can associate the (a,d)-sequence $(a_1, d_1), (a_2, d_2), \ldots$. For example, the system of congruences $x \equiv 3 \bmod 4$ and $x \equiv 2 \bmod p_i$, with p_i running through the consecutive odd primes, leads to the a-sequence $\{3, 11, 47, 107, 3467, 45047, \ldots\}$.

Proposition 7. *Let ℓ be an odd prime. We have*

$$\delta_{d,a} < \begin{cases} \frac{1}{4}\Big(3 - \frac{2}{\ell(\ell-1)}\Big) & \text{if } \ell \nmid d, 4 \nmid d; \\ \frac{1}{2} & \text{if } \ell \nmid d, 4 \mid d, a \equiv 1 \bmod 4; \\ \frac{1}{3} & \text{if } 3 \mid d, \ell = 3, 4 \nmid d, a \equiv 1 \bmod 3; \\ \frac{1}{2} & \text{if } \ell \mid d, \ell > 3, 4 \nmid d, \left(\frac{a}{\ell}\right) = 1; \\ 1 & \text{if } 4 \mid d \text{ and } a \equiv 3 \bmod 4; \\ 1 & \text{if } \ell \mid d \text{ and } \left(\frac{a}{\ell}\right) = -1, \end{cases}$$

and $\delta_{d,a} = 0$ in the remaining cases. All of the upper bounds are sharp in the sense that they do not always hold if an arbitrary $\epsilon > 0$ is subtracted from them.

Proof. Starting point is the formula

$$\delta_{d,a} = c(d,a) \prod_{p \mid (a-1,d)} \Big(1 - \frac{1}{p}\Big) \prod_{p \nmid d} \Big(1 - \frac{1}{p(p-1)}\Big) = c(d,a)\, \Pi_1\, \Pi_2,$$

say. The six subcases we denote by respectively a,b,c,d,e and f. For each of them the conditions imposed on a and d ensure that $(a-1,d)$ has certain prime factors, e.g., if $4 \mid d$, then $2 \mid (a-1,d)$. These factors are indicated in the Π_1 column of Table 1. Likewise certain factors have to appear in the Π_2 column. An entry e in the Π_1 column leads to a factor $1 - \frac{1}{e}$ in $\delta_{d,a}$, in the Π_2 column e leads to $1 - \frac{1}{e(e-1)}$. Further, in absence of an entry, we put a 1 as factor. Clearly multiplying everything and also multiplying by $c(d,a)$ (which has a fixed value in each subcase), leads to an upper bound for $\delta_{d,a}$. For example, in subcase a we obtain

$$\frac{1}{2}\Big(3 + \frac{1}{\ell^2 - \ell - 1}\Big) \cdot 1 \cdot \frac{1}{2}\Big(1 - \frac{1}{\ell(\ell-1)}\Big) = \frac{1}{4}\Big(3 - \frac{2}{\ell(\ell-1)}\Big),$$

with the factor before the dot being $c(d,a)$, 1 being the contribution to Π_1 and the rest being the contribution to Π_2. This explains the upper bound for $\delta_{d,a}$ in subcase a, and the other upper bounds are read off similarly from Table 1.

It remains to establish the sharpness of the upper bounds. We do this by indicating six families (a_j, d_j) such that δ_{d_j,a_j} tends to the indicated upper bound. The a_j are solutions of a certain system of congruences, the default system being

$$x \equiv 2 \bmod 3,\ x \equiv 2 \bmod 5,\ x \equiv 2 \bmod 7, \ldots,\ x \equiv 2 \bmod 11, \ldots$$

where the moduli run over the consecutive odd primes. In each of the six cases we make some small modifications to the default system involves at most the moduli 3 and ℓ, and we possibly add a congruence modulo 4.

Construction of the (a,d)-sequences
a) We remove the congruence $x \equiv 2 \bmod \ell$. Trivially now the a-sequence is $2, 2, 2, 2, \ldots$.
b) We start with the congruence $x \equiv 1 \bmod 4$ and remove the congruence $x \equiv 2 \bmod \ell$. Thus for $\ell = 5$ we find, for example, the a-sequence $1, 5, 65, 233, 3005, 51053, \ldots$.
c) We start with $x \equiv 1 \bmod 3$ and obtain the a-sequence $1, 7, 37, 772, 10012, 85087 \ldots$.
d) Here we need $\ell > 3$. The congruence $x \equiv 2 \bmod \ell$ is changed to $x \equiv 4 \bmod \ell$. Thus for $\ell = 5$ we find, for example, the a-sequence $2, 14, 44, 464, 12014, 102104, \ldots$.
e) We start with the congruence $x \equiv 3 \bmod 4$, leading to an a-sequence $3, 11, 47, 107, 3467, 45047, \ldots$
f) We change $x \equiv 2 \bmod \ell$ to $x \equiv n_0 \bmod \ell$, with n_0 the smallest non-residue modulo ℓ. For $\ell = 7$ we obtain a-sequence $2, 2, 17, 332, 10727, 145862, \ldots$. (Note that we get the default congruence system if and only if $\ell \equiv \pm 3 \bmod 8$.)

Let $k \geq 2$. In each of the above subcases the constructed (a,d)-sequence has the property that $(a_k, d_k) = 1$ and in addition $p \mid (a_k - 1, d_k)$ if and only if p is in the Π_1 column. If k is large enough, the primes that appear in the Π_2 column are precisely those indicated in that column, with in addition all prime $p \geq p_0$ for some p_0 tending to infinity with k. We conclude that, as k gets larger,

$$\delta_{a_k,d_k} = (\text{upper bound}) \prod_{p \geq p_0} \left(1 - \frac{1}{p(p-1)}\right) \to \text{upper bound},$$

concluding the proof. □

Table 1

subcase	$c(d,a)$	Π_1	Π_2
a	$\frac{1}{2}(3 + \frac{1}{\ell^2-\ell-1})$		$2, \ell$
b	$1 + \frac{1}{\ell^2-\ell-1}$	2	ℓ
c	1	3	2
d	1		2
e	2	2	
f	2	2 if $2 \mid d$	2 if $2 \nmid d$

Remark 7. Our choice of the six sequences (a_k, d_k) was very canonical, but in fact given d_k many choices of a_k are allowed. E.g., in subcase c there are $\varphi(d_k) \prod_{3 \leq p \leq p_k} (p-2)/(p-1)$ choices allowed, with p_k the kth odd prime. This number is asymptotically equal to $c_1 \varphi(d_k)/\log\log d_k$, for some positive constant c_1. The same conclusion, with possibly different c_1, is valid for the other five sequences.

It remains to deal with the case $\ell = 2$. Proceeding as above one deduces from Proposition 1.12 of [14] the following result.

Proposition 8. *Let $\ell = 2$. We have*

$$\delta_{d,a} = \begin{cases} \frac{3}{4} & \textit{if } 4 \nmid d; \\ \frac{1}{2} & \textit{if } 4 \mid d, 8 \nmid d, \ a \equiv 1 \pmod 4; \\ 1 & \textit{if } 4 \mid d, 8 \nmid d, \ a \equiv 3 \pmod 4; \\ 1 & \textit{if } 8 \mid d, \ a \not\equiv 1 \pmod 8; \end{cases}$$

and $\delta_{d,a} = 0$ in the remaining cases. All of the upper bounds are sharp in the sense that they do not always hold if an arbitrary $\epsilon > 0$ is subtracted from them.

6.1.4. **The proof of Theorem 4.**

Proof. Let $\epsilon > 0$ be arbitrary. Recalling the definition (29) of $\mathcal{P}_{d,a}$, we find that, for all x sufficiently large,

$$\mathcal{P}_G(d,a)(x) \geq \pi(x;d,a) - \mathcal{P}_{d,a}(x) + O(1) \geq (1-\delta_{d,a}-\epsilon)\frac{x}{\varphi(d)\log x},$$

where we used the upper bound (31) for $\mathcal{P}_{d,a}(x)$, and the well-known asymptotic $\pi(x;d,a) \sim x/(\varphi(d)\log x)$. The claims regarding $1-\delta_{d,a}$ are an immediate consequence of Proposition 7. $\square$

Example 2. Setting $a = d = 1$ we have $\mathcal{P}_G(1,1)(x) = \mathcal{P}_G(x)$ in our earlier notation. Theorem 4 then yields the second inequality in (28).

7. Prime divisors of the H^{ε}-sequences

7.1. **The H^--sequence.** In this section we obtain the results on the growth behavior of $\mathcal{P}_{H^{\varepsilon}}(d,a)(x)$ that are needed in order to prove Theorem 3.

7.1.1. **Statement of results.** Let ℓ be an odd prime number and $1 \leq a < d$ be coprime integers. In this section we consider the set of rational (odd) primes

$$\mathcal{P}^-_{d,a} := \{p \equiv a \bmod d : \mathrm{ord}_p(\ell) = (p-1)/2 \text{ or } \mathrm{ord}_p(\ell) = p-1\}.$$

As Theorem 5 provides all the information we need on the set $\{p \equiv a \bmod d : \mathrm{ord}_p(\ell) = p-1\}$, it suffices to consider the set

$$\mathcal{A}^-_{d,a} := \{p \equiv a \bmod d : \mathrm{ord}_p(\ell) = (p-1)/2\},$$

which, under GRH, has density

$$\alpha^-_{d,a} = \sum_{n=1}^{\infty} \frac{\varphi(d)\mu(n)c^-_a(n)}{[\mathbb{Q}(\zeta_{[d,2n]},\ell^{1/2n}):\mathbb{Q}]}, \tag{41}$$

where $c^-_a(n) = 1$ if the automorphism σ_a of $\mathbb{Q}(\zeta_d)$ determined by $\sigma_a(\zeta_d) = \zeta_d^a$ is the identity on the field $\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{2n},\ell^{1/2n})$, and $c^-_a(n) = 0$ otherwise.

Theorem 7. *Let ℓ be an odd prime, a and d coprime positive integers, $\delta^-_{d,a}$ as in (41) and ϵ be arbitrary and fixed. Then for every x sufficiently large we have*

$$\mathcal{A}^-_{d,a}(x) \leq (\alpha^-_{d,a} + \epsilon)\frac{x}{\varphi(d)\log x},$$

where

$$\alpha^-_{d,a} = A\,c^-(d,a)\,R(d,a),$$

with $R(d,a)$ as in (17). If $4 \mid d$, then

$$c^-(d,a) = \begin{cases} \frac{1}{2}\left(1 - \frac{1}{\ell^2-\ell-1}\right) & \text{if } \ell \nmid d, a \equiv 1 \bmod 4; \\ 1 - \left(\frac{-1}{\ell}\right)\frac{1}{\ell^2-\ell-1} & \text{if } \ell \nmid d, a \equiv 3 \bmod 4; \\ 0 & \text{if } \ell \mid d, \left(\frac{\ell}{a}\right) = -1; \\ \frac{1}{2}\left(3 - \left(\frac{-1}{a}\right)\right) & \text{if } \ell \mid d, \left(\frac{\ell}{a}\right) = 1. \end{cases} \tag{42}$$

If $4 \nmid d$, then

$$c^-(d,a) = \begin{cases} \frac{3}{4}\left(1 - \frac{1}{\ell^2-\ell-1}\right) & \text{if } \ell \nmid d, \ell \equiv 1 \bmod 4; \\ \frac{1}{4}\left(3 + \frac{1}{\ell^2-\ell-1}\right) & \text{if } \ell \nmid d, \ell \equiv 3 \bmod 4; \\ \frac{3}{4}\left(1 + \left(\frac{a}{\ell}\right)\right) & \text{if } \ell \mid d, \ell \equiv 1 \bmod 4; \\ \frac{1}{8}\left(5 + \left(\frac{a}{\ell}\right)\right) & \text{if } \ell \mid d, \ell \equiv 3 \bmod 4. \end{cases}$$

Assuming GRH, we have

$$\mathcal{A}^-_{d,a}(x) = \frac{\alpha^-_{d,a}}{\varphi(d)} \frac{x}{\log x} + O_d\left(\frac{x \log\log x}{\log^2 x}\right).$$

Remark 8. If $4\ell \mid d$ and $\left(\frac{\ell}{a}\right) = -1$, then $\alpha^-_{d,a} = 0$ for trivial reasons and even $\mathcal{A}^-(d,a)$ is empty. Namely, if $p \in \mathcal{A}^-(d,a)$, then $p \equiv a \bmod \ell$ and $\mathrm{ord}_p(\ell) = (p-1)/2$. It follows that $\left(\frac{\ell}{p}\right) = 1$ and hence $\left(\frac{\ell}{a}\right) = 1$.

Remark 9. Note that $\mathcal{P}_{d,a} \subseteq \mathcal{P}^-_{d,a}$. Comparison with (35) shows that $\mathcal{P}^-_{d,a} = \mathcal{P}_{d,a}$ if $4 \mid d$ and $a \equiv 3 \bmod 4$. Hence in this case, under GRH, we have $c^-(d,a) = c(d,a) - c_1(d,a)$, with $c(d,a)$ and $c_1(d,a)$ explicitly given in Theorem 6, respectively Theorem 5. By definition, we have $\mathcal{P}^-_{d,a} = \mathcal{P}_{d,a}$ if and only if the density of primes p such that $p \equiv a \bmod d$, $p \equiv 1 \bmod 4$ and $\mathrm{ord}_p(\ell) = (p-1)/2$ is zero. This happens trivially if the two modular congruences are not compatible, namely when $4 \mid d$ and $a \not\equiv 1 \bmod 4$. If they are compatible, then by Theorem 7 under GRH the considered density is zero if and only if one of the following two conditions holds:

- $4\ell \mid d$, $a \equiv 1 \bmod 4$ and $\left(\frac{\ell}{a}\right) = -1$;
- $4 \nmid d$, $\ell \mid d$, $\ell = 1 \bmod 4$ and $\left(\frac{a}{\ell}\right) = -1$.

Combination of Theorem 7 and Theorem 5 yields the following result.

Theorem 8. *We have*

$$\mathcal{P}^-_{d,a}(x) \leq (\delta^-_{d,a} + \epsilon)\frac{x}{\varphi(d)\log x},$$

where $\delta^-_{d,a} = \alpha^-_{d,a} + \alpha_{d,a} = AR(d,a)c_2(d,a)$ *with*

$$c_2(d,a) = c^-(d,a) + c_1(d,a) = \begin{cases} \frac{1}{2}\left(3 + \frac{1}{\ell^2-\ell-1}\right) & \text{if } \ell \nmid d, \ell \equiv 1 \bmod 4; \\ 2 & \text{if } \ell \nmid d, \ell \equiv 3 \bmod 4; \\ 2 & \text{if } \ell \mid d, \ell \equiv 1 \bmod 4; \\ \frac{1}{2}\left(3 - \left(\frac{-1}{a}\right)\right) & \text{if } \ell \mid d, \ell \equiv 3 \bmod 4, 4 \mid d; \\ \frac{3}{2} & \text{if } \ell \mid d, \ell \equiv 3 \bmod 4, 4 \nmid d. \end{cases}$$

Assuming GRH we have

$$\mathcal{P}^-_{d,a}(x) = \frac{\delta^-_{d,a}}{\varphi(d)} \frac{x}{\log x} + O_d\left(\frac{x \log\log x}{\log^2 x}\right).$$

7.1.2. **Proofs.** We start by determining the coefficients $c^-_a(n)$ that occur in the infinite sum (41).

Lemma 10. *Let ℓ be an odd prime, n a squarefree integer, and d a natural number such that $4 \mid d$. Let Δ be the discriminant of $\mathbb{Q}(\sqrt{\ell})$. We have*

$$\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{2n}, \ell^{1/2n}) = \mathbb{Q}(\zeta_{(d,2n)}, \alpha)$$

with

$$\alpha = \begin{cases} \sqrt{\ell} & \text{if } \ell \mid d, \Delta \nmid 2n; \\ i & \text{if } \ell \nmid d, \ell \mid n, 2 \nmid n, \ell \equiv 3 \bmod 4; \\ 1 & \text{otherwise.} \end{cases}$$

In the first two cases $\mathbb{Q}(\zeta_{(d,2n)}, \alpha)$ is a quadratic extension of $\mathbb{Q}(\zeta_{(d,2n)})$.

Proof. Let us set $I := \mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{2n}, \ell^{1/2n})$. By Kummer theory we may argue that, since $\mathbb{Q}(\zeta_\infty) \cap \mathbb{Q}(\zeta_{2n}, \ell^{1/2n})$ is a finite abelian extension of $\mathbb{Q}(\zeta_{2n})$, it is of the form $\mathbb{Q}(\zeta_{2n}, \ell^{e/2n})$ for some

$e \geq 0$, and hence by Schinzel's theorem [31, Theorem 2] it is $\mathbb{Q}(\zeta_{2n}, \sqrt{\ell})$. The latter extension equals $\mathbb{Q}(\zeta_{2n})$ if $\Delta \mid 2n$.

Therefore, if $\ell \nmid dn$ or $\Delta \mid 2n$, then $I = \mathbb{Q}(\zeta_{(d,2n)})$. If $\Delta \nmid 2n$ and $\ell \mid d$, then noticing that $\mathbb{Q}(\zeta_{(d,2n)}) \subseteq I \subseteq \mathbb{Q}(\zeta_{(d,2n)}, \zeta_{4\ell})$ and $\mathbb{Q}(\zeta_{4\ell}) \subseteq \mathbb{Q}(\zeta_d)$, we deduce that $I = \mathbb{Q}(\zeta_{(d,2n)}, \sqrt{\ell})$. If $\ell \mid n$, n is odd, $\ell \equiv 3 \bmod 4$ and $\ell \nmid d$, then we have $\mathbb{Q}(\zeta_{(d,2n)}) \subseteq I \subseteq \mathbb{Q}(\zeta_{(d,4n)})$, yielding $I = \mathbb{Q}(\zeta_{4(d,n)})$ as $\zeta_4 \in I$ but $\zeta_4 \notin \mathbb{Q}(\zeta_{(d,2n)})$. □

Corollary 2. *Let ℓ be an odd prime, n a squarefree integer, and a, d natural numbers such that $4 \mid d$ and $(a, d) = 1$. If $a \not\equiv 1 \bmod (d, 2n)$, then $c_a^-(n) = 0$. If $a \equiv 1 \bmod (d, 2n)$, then*

$$c_a^-(n) = \begin{cases} \frac{1}{2}\left(1 + \left(\frac{\ell}{a}\right)\right) & \text{if } \ell \mid d, \Delta \nmid n; \\ \frac{1}{2}\left(1 + \left(\frac{-1}{a}\right)\right) & \text{if } \ell \nmid d, \ell \mid n, 2 \nmid n, \ell \equiv 3 \bmod 4; \\ 1 & \text{otherwise.} \end{cases}$$

Proof. An immediate consequence of Lemma 10 on noting that $\sigma_a(\zeta_{(d,2n)}) = \zeta_{(d,2n)}^a$, $\sigma_a(i) = i^a = \left(\frac{-1}{a}\right)i$, and, if $\ell \mid d$, then $\sigma_a(\sqrt{\ell}) = \left(\frac{\ell}{a}\right)\sqrt{\ell}$ (by Lemma 8). □

Remark 10. A different proof of Lemma 10 is obtained on using that if $K/\mathbb{Q}$ is Galois, then

$$I := [K \cap L : \mathbb{Q}] = \frac{[K : \mathbb{Q}][L : \mathbb{Q}]}{[K \cdot L : \mathbb{Q}]}.$$

Applying this equality with $K = \mathbb{Q}(\zeta_d)$ and $L = \mathbb{Q}(\zeta_{2n}, \ell^{1/2n})$, computing all the degree occurring, and using that $\varphi((d, 2n))\varphi([d, 2n]) = \varphi(d)\varphi(2n)$, then shows that in the first two cases I is a quadratic extension of $\mathbb{Q}(\zeta_{(d,2n)})$ and $I = \mathbb{Q}(\zeta_{(d,2n)})$ otherwise. The proof is then easily completed.

Proof of Theorem 7. Our starting point for is formula (41), which expresses $\alpha_{d,a}^-$ as an infinite sum, which we will rewrite as an Euler product using Lemma 7 (the notation of which we will use). Throughout n will be a squarefree integer. We first assume $4 \mid d$, and so $[d, 2n] = [d, n]$. Recall that the degree $[\mathbb{Q}(\zeta_{[d,2n]}, \ell^{1/2n}) : \mathbb{Q}]$ equals $\varphi([d, n])n$ if $\ell \mid [d, n]$ and $\varphi([d, n])2n$ otherwise. We put

$$\Sigma_1 = \sum_{a \equiv 1 \bmod (d,2n)} \frac{\varphi(d)\mu(n)}{[\mathbb{Q}(\zeta_{[d,2n]}, \ell^{1/2n}) : \mathbb{Q}]}, \quad \Sigma_2 = \sum_{\substack{a \equiv 1 \bmod (d,2n) \\ \ell \mid d,\ \Delta \nmid n}} \frac{\varphi(d)\mu(n)}{[\mathbb{Q}(\zeta_{[d,2n]}, \ell^{1/2n}) : \mathbb{Q}]},$$

and

$$\Sigma_3 = \sum_{\substack{a \equiv 1 \bmod (d,2n) \\ \ell \nmid d,\ \ell \mid n,\ 2 \nmid n,\ \ell \equiv 3 \bmod 4}} \frac{\varphi(d)\mu(n)}{[\mathbb{Q}(\zeta_{[d,2n]}, \ell^{1/2n}) : \mathbb{Q}]}.$$

Notice that the three sums Σ_2, Σ_3 and Σ_1 (respectively) reflect the three cases distinguished in Corollary 2. Making the values of $c_a^-(n)$ in (41) explicit using Corollary 2 we obtain

$$\alpha_{d,a}^- = \Sigma_1 + \frac{1}{2}\Big((\frac{\ell}{a}) - 1\Big)\Sigma_2 + \frac{1}{2}\Big((\frac{-1}{a}) - 1\Big)\Sigma_3.$$

Case 1: $\ell \mid d$. Now $\Sigma_3 = 0$ and so

$$\alpha_{d,a}^- = \Sigma_1 + \frac{1}{2}\Big((\frac{\ell}{a}) - 1\Big)\Sigma_2.$$

We have

$$\Sigma_1 = \sum_{a \equiv 1 \bmod (d,2n)} \frac{\mu(n)}{\omega_d(n)},$$

which equals $S(1) = AR(d, a)$ for $a \equiv 1 \bmod 4$, and equals $S(1) - S_2(1) = 2S(1) = 2AR(d, a)$ if $a \equiv 3 \bmod 4$.

Subcase 1.1: $\left(\frac{\ell}{a}\right)=1$. Then $\alpha^-_{d,a}=\Sigma_1$ and we find $c^-(d,a)=\frac{1}{2}(3-\left(\frac{-1}{a}\right))$.

Subcase 1.2: $\left(\frac{\ell}{a}\right)=-1$. Suppose $\ell\equiv 1 \bmod 4$. Then by quadratic reciprocity we have $\left(\frac{a}{\ell}\right)=-1$ and so all n that contribute to Σ_1 satisfy $\ell\nmid n$. As $\Delta=\ell$ we infer that $\Sigma_1=\Sigma_2$ and hence $\alpha^-_{d,a}=\Sigma_1-\Sigma_2=0$. If $\ell\equiv 3 \bmod 4$, the condition $\Delta\nmid n$ is automatically satisfied and we obtain $\Sigma_2=\Sigma_1$, and hence again $\alpha^-_{d,a}=0$. (For a different argument why $\alpha^-_{d,a}=0$ see Remark 8.) We conclude that $c^-(d,a)=0$.

Case 2: $\ell\nmid d$. Now

$$\alpha^-_{d,a}=\Sigma_1+\frac{1}{2}\Big(\big(\frac{-1}{a}\big)-1\Big)\Sigma_3.$$

We have

$$\Sigma_1=\Bigg(\sum_{\substack{\ell\mid n\\ a\equiv 1 \bmod (d,2n)}}+\frac{1}{2}\sum_{\substack{\ell\nmid n\\ a\equiv 1 \bmod (d,2n)}}\Bigg)\frac{\mu(n)}{\omega_d(n)}.$$

If $a\equiv 1 \bmod 4$, then

$$\Sigma_1=\frac{1}{2}\Bigg(\sum_{\substack{n\geq 1\\ a\equiv 1 \bmod (d,n)}}+\sum_{\substack{\ell\mid n\\ a\equiv 1 \bmod (d,n)}}\Bigg)\frac{\mu(n)}{\omega_d(n)}=\frac{1}{2}(S(1)+S(\ell))=\frac{A}{2}\left(1-\frac{1}{\ell^2-\ell-1}\right)R(d,a),$$

and hence $c^-(d,a)=\frac{1}{2}(1-\frac{1}{\ell^2-\ell-1})$.

Next suppose $a\equiv 3 \bmod 4$. In this case in the density sums we can restrict to odd n.

Subcase 2.1: $\ell\equiv 3 \bmod 4$. Now

$$\alpha^-_{d,a}=\Sigma_1-\Sigma_3=\frac{1}{2}\sum_{\substack{\ell\nmid n,\ 2\nmid n\\ a\equiv 1 \bmod (d,n)}}\frac{\mu(n)}{\omega_d(n)},$$

which is easily seen to equal

$$\frac{1}{2}(S(1)-S_2(1)-S(\ell)+S_2(\ell))=S(1)-S(\ell)=A\left(1+\frac{1}{\ell^2-\ell-1}\right)R(d,a).$$

Subcase 2.2: $\ell\equiv 1 \bmod 4$. Now $\Sigma_3=0$ and

$$\alpha^-_{d,a}=\Sigma_1=\Bigg(\sum_{\substack{\ell\mid n,\ 2\nmid n\\ a\equiv 1 \bmod (d,n)}}+\frac{1}{2}\sum_{\substack{\ell\nmid n,\ 2\nmid n\\ a\equiv 1 \bmod (d,n)}}\Bigg)\frac{\mu(n)}{\omega_d(n)},$$

which equals

$$(S(\ell)-S_2(\ell))+(S(1)-S(\ell))=S(1)+S(\ell)=A\left(1-\frac{1}{\ell^2-\ell-1}\right)R(d,a).$$

We conclude that $c^-(d,a)=1-\left(\frac{-1}{\ell}\right)\frac{1}{\ell^2-\ell-1}$.

This completes the proof in the case $4\mid d$. Suppose now that $4\nmid d$. We may argue as in Sect. 6.1.2 and, keeping the notation d,a_1,a_3 as there, we obtain

$$\alpha^-_{d,a}=\frac{\alpha^-_{d_1,a_1}+\alpha^-_{d_1,a_3}}{2}=\frac{A}{2}(c^-(d_1,a_1)+c^-(d_1,a_3))R(d,a),$$

and hence

$$c^-(d,a)=\frac{c^-(d_1,a_1)+c^-(d_1,a_3)}{2}.$$

Since $\left(\frac{a}{\ell}\right)=\left(\frac{a_1}{\ell}\right)=\left(\frac{a_3}{\ell}\right)$, the idea is to rewrite (42) using quadratic reciprocity in terms of $\left(\frac{a}{\ell}\right)$. This gives rise to more cases, but makes it easy to determine $c^-(d,a)$. For example, if $\ell\mid d$, $\left(\frac{\ell}{a}\right)=1$, and $\ell \equiv 1 \bmod 4$, then $c^-(d_1, a_1) = 1$ and $c^-(d_1, a_3) = 2$, and thus $c^-(d, a) = \frac{3}{2}$ if $\ell \mid d$, $\left(\frac{a}{\ell}\right) = 1$, and $\ell \equiv 1 \bmod 4$. □

7.2. **The H^+-sequence.** Let ℓ be an odd prime number and $1 \le a < d$ be coprime integers. In this section we consider the set of rational (odd) primes

$$\mathcal{P}^+_{d,a} := \{p \equiv a \bmod d : \mathrm{ord}_p(\ell) = p-1 \text{ or } \mathrm{ord}_p(\ell) \text{ is odd}\}.$$

This set can be written as a disjoint union of two sets:

$$\mathcal{P}^+_{d,a} = \mathcal{A}_{d,a} \cup \{p \equiv a \bmod d : \mathrm{ord}_p(\ell) \text{ is odd}\}.$$

Under GRH the density of $\mathcal{A}_{d,a}$ is given in Theorem 5. The density of the second set has been unconditionally determined in case ℓ is a positive rational number by Moree and Sury [26]. Unfortunately, even in the case where ℓ is an odd prime, there are many cases and for this reason we will not write the details out here. However, under this restriction on ℓ the density is always positive (this follows from [26, Theorem 5]). If the discriminant of $\mathbb{Q}(\sqrt{\ell})$ divides d and $\left(\frac{\ell}{a}\right) = 1$, then the set $\mathcal{A}_{d,a}$ is empty (see Remark 2) and we obtain an unconditional asymptotic for $\mathcal{P}^+_{d,a}(x)$. A particular easy case arises for $\ell = 3, a = 11$ and $d = 12$. Then we have $\mathcal{P}^+_{12,11} = \{p : p \equiv 11 \bmod 12\}$. This basically is a claim Fermat made in 1641! He made some similar, but unfortunately wrong ones, for the details see [26].

7.3. **Counting prime divisors of the H-, H^-- and H^+-sequences.** Denote the sets of prime divisors in the section header by, respectively, $\mathcal{Q}_H$, $\mathcal{Q}_{H^-}$ and $\mathcal{Q}_{H^+}$. By Proposition 3 and Lemma 4 these sets are very closely related to $\mathcal{P}_G$, $\mathcal{P}_{H^-}$ and $\mathcal{P}_{H^+}$, respectively. Assuming that the associated Wieferich sets are $o(x/\log x)$ (see Sect. 3.4), we arrive at the following conjecture.

Conjecture 5. *Asymptotically we have $\mathcal{Q}_H(x) \sim \mathcal{P}_G(x)$, $\mathcal{Q}_{H^-}(x) \sim \mathcal{P}_{H^-}(x)$ and $\mathcal{Q}_{H^+}(x) \sim \mathcal{P}_{H^+}(x)$, where the asymptotic behavior of $\mathcal{P}_G(x), \mathcal{P}_{H^-}(x), \mathcal{P}_{H^+}(x)$ is given by* (27), (25), *respectively* (26).

8. Earlier work on the Genocchi ℓ-integers

We recapitulate some earlier work on ℓ-Genocchi integers. None of it is directly relevant for the proofs presented in this paper, and so it can be regarded as background reading.

8.1. **The case $\ell = 2$.** The original Genocchi numbers are obtained on taking $\ell = 2$. These numbers have received considerable attention in the literature. It follows from (12) and $H_n = G_n/2n$ that

$$\frac{2t}{e^t + 1} = \sum_{n=1}^{\infty} G_n \frac{t^n}{n!}.$$

It is well-known that $G_1 = 1$, $G_{2n+1} = 0$ for $n \ge 1$, and that $(-1)^n G_{2n}$ is an odd positive integer.

Dumont [8] showed that $|G_{2n}|$ equals the number of permutations p of $\{1, 2, \ldots, 2n-1\}$ such that $p(i) < p(i+1)$ for $p(i)$ odd and $p(i) > p(i+1)$ for $p(i)$ even ($1 \le i \le 2n-2$). For a survey of related material see Stanley [33].

Setting $\ell = 2$ in (13), in case $p - 1 \nmid 2n$ we obtain

$$H_{2n} \equiv -2^{2n-1} \sum_{j=(p+1)/2}^{p-1} j^{2n-1} \equiv 2^{2n-1} \sum_{j=1}^{(p-1)/2} j^{2n-1} \pmod{p}. \tag{43}$$

A related result is due to Emma Lehmer [17], who showed in case $2n \not\equiv 2 \bmod (p-1)$ that

$$H_{2n} \equiv - \sum_{j=1}^{(p-1)/2} (p-2j)^{2n-1} \bmod p^2.$$

Under the same assumption on n and in the same spirit she showed that

$$\sum_{j=1}^{[p/4]}(p-4j)^{2n-1}\equiv -H_{2n}(2^{2n-1}+1) \bmod p^2, \quad p>3.$$

In case $2n\equiv 2 \bmod (p-1)$ both congruences still hold true modulo p.

For $|t|<\pi/2$ we have (see, e.g., [2, Prop. 1.17])

$$\tan t=\sum_{n=1}^{\infty}T_n\frac{t^{2n-1}}{(2n-1)!}, \text{ with } T_n=(-4)^n H_{2n}.$$

The numbers T_n are called *tangent numbers* and count the number of all alternating permutations of length $2n-1$ (see Entringer [9] or Knuth and Buckholtz [15]).

Let $p>3$ be a prime satisfying $p\equiv 3 \pmod 4$ and put $m=(p-1)/2$. Then the class number $h(-p)$ of the quadratic field $\mathbb{Q}(\sqrt{-p})$ satisfies

$$h(-p)=\frac{1}{2-(\frac{2}{p})}\sum_{j=1}^{m}(\frac{j}{p})\equiv\frac{1}{2-2^m}\sum_{j=1}^{m}j^m\equiv\frac{2^{-m}}{2-2^m}H_{\frac{p+1}{2}}\equiv -2B_{\frac{p+1}{2}} \pmod p,$$

a congruence due to Cauchy. The first identity is an easy consequence of Dirichlet's class number formula (see, for example, [2, p. 99]), the second congruence follows from (43) on setting $n=(p+1)/4$. The first identity implies that $h(-p)\le (p-1)/2$ and thus the congruence uniquely determines the value of $h(-p)$. For some related results we refer to the recent preprint by Minč et al. [20].

8.2. **The case ℓ is odd.** Despite the enormous literature on variations of Bernoulli numbers, we found only very little earlier work on ℓ-Genocchi numbers for odd ℓ. For example, in case $\ell=3$ and $p>3$, Emma Lehmer [17] showed that

$$H_{2n}\equiv -2\sum_{j=1}^{[p/3]}(p-3j)^{2n-1} \bmod p^2.$$

The deepest result we found gives a connection with functions related to polylogarithms. Namely, given any integer k consider the formal series

$$l_k(s)=\sum_{n=1}^{\infty}\frac{s^n}{n^k}.$$

Wójcik [35] found an explicit formula for l_k for $k\le 0$, namely

$$l_k(s)=-\frac{sR_n(s)}{(s-1)^{n+1}},$$

where $n=-k$ and the $R_n\in\mathbb{Z}[s]$ are the classical Euler-Frobenius polynomials defined by the formula

$$\frac{1-s}{e^t-s}=\sum_{n=0}^{\infty}\frac{R_n(s)}{(1-s)^n}\frac{t^n}{n!}.$$

The individual terms in the first sum of (12) can be connected with the series $l_k(s)$, namely it can be shown (cf. Urbanowicz and Williams [34, p. 132]) that

$$\frac{z}{e^t-z}=\sum_{n=1}^{\infty}(-1)^n l_{-n}(z)\frac{t^n}{n!}.$$

From (12) we then infer on equating Taylor coefficients

$$H_n = (-1)^n \sum_{a=1}^{\ell-1} l_{1-n}(\zeta_\ell^a).$$

9. Experimental data

In this section we provide some numerical examples for the densities of G-, H^+- and H^--irregular primes, and G-irregular primes in arithmetic progressions and compare them with our conjectural predictions. As customary, $\pi(x)$ is the number of primes $p \le x$. All data have been produced with SageMath [30].

Table 1. The ratio $\mathcal{P}_G(x)/\pi(x)$ for $x = 10^5$

ℓ	experimental	theoretical
2	0.661593	0.659776
3	0.635113	0.637095
5	0.657214	0.653807
7	0.660863	0.657010
11	0.660133	0.658736
13	0.659612	0.659045
17	0.662948	0.659358
19	0.657110	0.659444

Table 2. The ratios $\mathcal{P}_{H^+}(x)/\pi(x)$ and $\mathcal{P}_{H^-}(x)/\pi(x)$ for $x = 10^5$

	$\mathcal{P}_{H^+}(x)/\pi(x)$		$\mathcal{P}_{H^-}(x)/\pi(x)$	
ℓ	experimental	theoretical	experimental	theoretical
2	0.599145	0.596279	0.603315	0.603072
3	0.568390	0.571007	0.588198	0.591731
5	0.563699	0.559070	0.599458	0.600088
7	0.575271	0.571007	0.604671	0.601689
11	0.571726	0.571007	0.604462	0.602552
13	0.571518	0.569544	0.600292	0.602706
17	0.573499	0.570170	0.607173	0.602863
19	0.569537	0.571007	0.599875	0.602906

TABLE 3. The ratio $\mathcal{P}_G(d,a)(x)/\pi(x;d,a)$ for $x = 10^5$

ℓ	d	a	experimental	theoretical
3	3	1	0.816097	0.818547
	3	2	0.454337	0.455642
	4	1	0.717473	0.727821
	4	3	0.552752	0.546368
5	3	1	0.725396	0.723046
	3	2	0.589241	0.584569
	4	1	0.763970	0.761246
	4	3	0.550459	0.546368
7	3	1	0.723311	0.725608
	3	2	0.598624	0.588412
	4	1	0.764178	0.767652
	4	3	0.557548	0.546368

ℓ	d	a	experimental	theoretical
11	7	1	0.695580	0.700353
	7	2	0.661802	0.650412
	7	3	0.649291	0.650412
	7	4	0.649917	0.650412
	7	5	0.670559	0.650412
	7	6	0.634279	0.650412
	15	1	0.753962	0.770096
	15	2	0.576314	0.568929
	15	4	0.706422	0.712620
	15	7	0.724771	0.712620
	15	8	0.573812	0.568929
	15	11	0.649708	0.655144
	15	13	0.712260	0.712620
	15	14	0.583820	0.568929

Acknowledgement

The authors thank Karl Dilcher, Bakir Farhi, Masanobu Kaneko and Bernd Kellner for kindly answering some Bernoulli number related questions. A very helpful e-mail exchange with Efthymios Sofos led to a simplified proof of Proposition 7. Thanks to Antonella Perucca for her constant support and encouragement.

References

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

[2] T. Arakawa, T. Ibukiyama and M. Kaneko, *Bernoulli Numbers and Zeta Functions*, with an appendix by D. Zagier, Springer Monographs in Mathematics, Springer, Tokyo, 2014.

[3] F.R. Beyl, Cyclic subgroups of the prime residue group, *Amer. Math. Monthly* **84** (1977), 46–48.

[4] A.I. Borevich and I.R Shafarevich, *Number Theory*, Translated from the Russian by Newcomb Greenleaf Pure and Applied Mathematics **20**, Academic Press, New York-London, 1966.

[5] A. Ciolan and P. Moree, Browkin's discriminator conjecture, *Colloq. Math.* **156** (2019), 25–56.

[6] D.A. Cox, *Primes of the Form x^2+ny^2. Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989.

[7] R.C. Daileda, An application of a generalization of Artin's primitive root conjecture in the theory of monoid rings, `https://arxiv.org/abs/2112.09080`, preprint.

[8] D. Dumont, Interprétations combinatoires des nombres de Genocchi, *Duke Math. J.* **41** (1974), 305–318.

[9] R.C. Entringer, A combinatorial interpretation of the Euler and Bernoulli numbers, *Nieuw Arch. Wisk. (3)* **14** (1966), 241–246.

[10] A. Granville and M.B. Monagan, The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389, *Trans. Amer. Math. Soc.* **306** (1988), 329–359.

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

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

[13] S. Hu and M.-S. Kim, *The $(S,\{2\})$-Iwasawa theory*, J. Number Theory **158** (2016), 73–89.

[14] S. Hu, M.-S. Kim, P. Moree and M. Sha, Irregular primes with respect to Genocchi numbers and Artin's primitive root conjecture, *J. Number Theory* **205** (2019), 59–80.

[15] D.E. Knuth and T.J. Buckholtz, Computation of tangent, Euler, and Bernoulli numbers, *Math. Comp.* **21** (1967), 663688.

[16] A. Kumar, M. Kumari, P. Moree and S.K. Singh, Ramanujan-style congruences for prime level, `https://arxiv.org/abs/2111.15287`, *Math. Z.*, to appear.

[17] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math.* (2) **39** (1938), no. 2, 350-360.

[18] H.W. Lenstra, Jr., On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.* **42** (1977), 202–224.

[19] F. Luca, A. Pizarro-Madariaga and C. Pomerance, On the counting function of irregular primes, *Indag. Math.* **26** (2015), 147–161.

[20] J. Minč, T.T. Nguyen and D.T. Nguyn, Fekete polynomials, quadratic residues and arithmetic, arXiv:2111.05256, to appear in *J. Number Theory.*

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

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

[23] P. Moree, On primes in arithmetic progression having a prescribed primitive root. II, *Funct. Approx. Comment. Math.* **39** (2008), 133–144.

[24] P. Moree, Artin's primitive root conjecture – a survey, *Integers* **12A** (2012), No. 6, 1305–1416.

[25] P. Moree, Near-primitive roots, *Funct. Approx. Comment. Math.* **48.1** (2013), 133–145.

[26] P. Moree and B. Sury, Primes in a prescribed arithmetic progression dividing the sequence $\{a^k + b^k\}_{k=1}^{\infty}$, *Int. J. Number Theory* **5** (2009), 641–665.

[27] P. Moree and A. Zumalacárregui, Salajan's conjecture on discriminating terms in an exponential sequence, *J. Number Theory* **160** (2016), 646–665.

[28] M.R. Murty, *Introduction to p-adic Analytic Number Theory*, AMS/IP Studies in Advanced Mathematics **27**, American Mathematical Society, Providence, RI; International Press, Somerville, MA, 2002.

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

[30] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 8.2)*, 2018, `http://www.sagemath.org`.

[31] A. Schinzel, Abelian binomials, power residues and exponential congruences, *Acta Arith.* **32** (1977), No. 3, 245-274.

[32] C.L. Siegel, Zu zwei Bemerkungen Kummers, *Nachr. Akad. d. Wiss. Goettingen Math. Phys. Kl.* **II** (1964), 51–62.

[33] R.P. Stanley, A survey of alternating permutations, *Combinatorics and graphs*, 165–196, *Contemp. Math.* **531**, Amer. Math. Soc., Providence, RI, 2010.

[34] J. Urbanowicz and K.S. Williams, *Congruences for L-functions*, Mathematics and its Applications **511**, Kluwer Academic Publishers, Dordrecht, 2000.

[35] A. Wójcik, Linear congruence relations for 2-adic L-series at integers, *Compositio Math.* **111** (1998), 289–304.

MAX-PLANCK-INSTITUT FÜR MATHEMATIK, VIVATSGASSE 7, D-53111 BONN, GERMANY
E-mail address: `moree@mpim-bonn.mpg.de`

UNIVERSITY OF LUXEMBOURG, DEPARTMENT OF MATHEMATICS, 6 AVENUE DE LA FONTE, L-4364 ESCH-SUR-ALZETTE, LUXEMBOURG
E-mail address: `pietro.sgobba@uni.lu`