Max-Planck-Institut für Mathematik
Bonn

Irregular primes with respect to Genocchi numbers and Artin's primitive root conjecture

by

Su Hu
Min-Soo Kim
Pieter Moree
Min Sha

Max-Planck-Institut für Mathematik
Preprint Series 2018 (63)

Irregular primes with respect to Genocchi numbers and Artin's primitive root conjecture

Su Hu
Min-Soo Kim
Pieter Moree
Min Sha

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

Department of Mathematics
South China University of Technology
Guangzhou 510640
China

Division of Mathematics, Science
and Computers
Kyungnam University
7 (Woryeong-dong) Kyungnamdaehak-ro
Masanhappo-gu, Changwon-si
Gyeongsangnam-do 51767
Republic of Korea

Department of Computing
Macquarie University
Sydney NSW 2109
Australia

MPIM 18-63

IRREGULAR PRIMES WITH RESPECT TO GENOCCHI NUMBERS AND ARTIN'S PRIMITIVE ROOT CONJECTURE

SU HU, MIN-SOO KIM, PIETER MOREE, AND MIN SHA

Abstract. In this paper, we introduce and study a variant of Kummer's notion of (ir)regularity of primes which we call G-irregularity. It is based on Genocchi numbers G_n, rather than Bernoulli number B_n. We say that an odd prime p is G-irregular if it divides at least one of the integers $G_2, G_4, \ldots, G_{p-3}$, and G-regular otherwise. We show that, as in Kummer's case, G-irregularity is related to the divisibility of some class number. Furthermore, we obtain some results on the distribution of G-irregular primes. In particular, we show that each primitive residue class contains infinitely many G-irregular primes and establish non-trivial lower bounds for their number up to a given bound x as x tends to infinity. As a by-product, we obtain some results on the distribution of primes in arithmetic progressions with a prescribed near-primitive root.

1. Introduction

1.1. **The classical case.** The n-th Bernoulli polynomial $B_n(x)$ is implicitly defined as the coefficient of t^n in the generating function

$$\frac{te^{xt}}{e^t-1}=\sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!},$$

where e is the base of the natrual logarithm. Then, the Bernoulli numbers B_n are defined by $B_n = B_n(0), n = 0, 1, 2, \ldots$. It is well-known that $B_0 = 1$, and $B_n = 0$ for any odd integer $n > 1$.

Throughout the paper, p always denotes a prime. An odd prime p is said to be *B-irregular* if p does not divide the numerator of at least one of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$, and *B-regular* otherwise. The first twenty B-irregular primes are

$$37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263,$$
$$271, 283, 293, 307, 311, 347, 353, 379, 389.$$

Kummer, who introduced the notion of irregularity, proved that Fermat's Last Theorem is true for B-regular prime exponents p.

The notion of B-irregularity has an important application in algebraic number theory. Let $\mathbb{Q}(\zeta_p)$ be the p-th cyclotomic field, and h_p the class number of $\mathbb{Q}(\zeta_p)$. Denote by h_p^+ the class number of $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ and put $h_p^- = h_p/h_p^+$. Kummer proved that h_p^- is an integer (now called the *relative class number* of $\mathbb{Q}(\zeta_p)$) and gave the following

2010 *Mathematics Subject Classification.* 11B68, 11A07,11R29.

Key words and phrases. Irregular prime, Bernoulli number and polynomial, Euler number and polynomial, Genocchi number, refined class number, primitive root, Artin's primitive root conjecture.

characterization (see [31, Theorem 5.16]). (Here and in the sequel, for any integer $n \geq 1$, ζ_n denotes an n-th primitive root of unity.)

Theorem 1.1 (Kummer). *An odd prime p is B-irregular if and only if $p \mid h_p^-$.*

Jensen [14] was the first to prove that there are infinitely many B-irregular primes. More precisely, he showed that there are infinitely many B-irregular primes not of the form $4n + 1$. This was generalized by Montgomery [20], who showed that 4 can be replaced by any integer greater than 2. To the best of our knowledge, the following result due to Metsänkylä [19] is the best.

Theorem 1.2 (Metsänkylä [19]). *Given an integer $m > 2$, let $\mathbb{Z}_m^*$ be the multiplicative group of the residue classes modulo m, and let H be a proper subgroup of $\mathbb{Z}_m^*$. Then, there exist infinitely many B-irregular primes not lying in the residue classes in H.*

Let $\mathcal{P}_B$ be the set of B-irregular primes. Carlitz [3] gave a simple proof of the infinitude of this set, and recently Luca, Pizarro-Madariaga and Pomerance [18, Theorem 1] made this more quantitative:

$$\mathcal{P}_B(x) \geq (1 + o(1)) \frac{\log\log x}{\log\log\log x} \tag{1.1}$$

as $x \to \infty$. (Here and in the sequel, if S is a set of natural numbers, then $S(x)$ denotes the number of elements in S not exceeding x.) Heuristics predicts a much stronger result (consistent with numerical data).

Conjecture 1.3 (Siegel [26]). *Asymptotically we have*

$$\mathcal{P}_B(x) \sim \Big(1 - \frac{1}{\sqrt{e}}\Big)\pi(x),$$

where $\pi(x)$ denotes the prime counting function.

The reasoning behind this conjecture is as follows. We assume that the numerator of B_{2k} is not divisible by p with probability $1-1/p$. Therefore, assuming the independence of divisibility by distinct primes, we expect that p is B-regular with probability

$$\Big(1 - \frac{1}{p}\Big)^{\frac{p-3}{2}},$$

which with increasing p tends to $e^{-1/2}$.

Moreover, for any positive integers a, d with $\gcd(a, d) = 1$, let $\mathcal{P}_B(d, a)$ be the set of B-irregular primes congruent to a modulo d. The following conjecture is also consistent with numerical data, which suggests that B-irregular primes are uniformly distributed in arithmetic progressions.

Conjecture 1.4. *For any positive integers a, d with $\gcd(a, d) = 1$, asymptotically we have*

$$\mathcal{P}_B(d, a)(x) \sim \frac{1}{\varphi(d)}\Big(1 - \frac{1}{\sqrt{e}}\Big)\pi(x),$$

where φ is Euler's totient function.

Although we know that there are infinitely many B-irregular primes, it is still an open problem to show that there are infinitely many B-regular primes.

1.2. **Some generalizations.** In [3] Carlitz gave a similar notion of irregular prime with respect to Euler numbers.

The Euler numbers E_n are a sequence of integers defined by the relation

$$\frac{2}{e^t+e^{-t}} = \sum_{n=0}^{\infty} E_n \frac{t^n}{n!}.$$

Moreover, $E_0 = 1$, and $E_n = 0$ for any odd $n \geq 1$. Euler numbers, just as Bernoulli numbers, can be defined via special polynomial values. The Euler polynomials $E_n(x)$ are implicitly defined as the coefficient of t^n in the generating function

$$\frac{2e^{xt}}{e^t+1} = \sum_{n=0}^{\infty} E_n(x) \frac{t^n}{n!}.$$

Then, $E_n = 2^n E_n(1/2), n = 0, 1, 2, \ldots$.

An odd prime p is said to be *E-irregular* if it divides at least one of the integers $E_2, E_4, \ldots, E_{p-3}$, and *E-regular* otherwise. The first twenty E-irregular primes are

$$19, 31, 43, 47, 61, 67, 71, 79, 101, 137, 139,$$
$$149, 193, 223, 241, 251, 263, 277, 307, 311.$$

Vandiver [28] proved that Fermat's Last Theorem is true for a prime exponent p if p is E-regular. This criterion makes it possible to discard many of the exponents Kummer could not handle:

$$37, 59, 103, 131, 157, 233, 257, 271, 283, 293, \ldots.$$

Carlitz [3] showed that there are infinitely many E-irregular primes. Luca, Pizarro-Madariaga and Pomerance in [18, Theorem 2] showed that the number of E-irregular primes up to x satisfies the same lower bound as in (1.1). Regarding their distribution, we currently only know that there are infinitely many E-irregular primes not lying in the residue classes $\pm 1 \pmod 8$, which was proven by Ernvall [4].

The computations suggest that the asymptotic behaviour of E-irregular primes follows the same rules as predicted in Conjectures 1.3 and 1.4.

It is not known whether or not the E-regularity can be related to the divisibility of some class number of a number field.

Later on, Ernvall [5, 6] introduced χ-irregular primes and proved the infinitude of such irregular primes for any Dirichlet character χ, including B-irregular primes and E-irregular primes as special cases. In addition, Hao and Parry [8] defined m-regular primes for any square-free integer m, and Holden [11] defined regular and irregular primes by using the values of zeta functions of totally real number fields.

In this paper, we introduce a new kind of irregular primes based on Genocchi numbers and study their distribution in detail.

1.3. **Regularity with respect to Genocchi numbers.** The Genocchi numbers G_n are defined by the relation

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

It is well-known that $G_1 = 1$, $G_{2n+1} = 0$ for $n \geq 1$, and $(-1)^n G_{2n}$ is an odd positive integer. The Genocchi numbers G_n are related to Bernoulli numbers B_n by the formula

$$G_n = 2(1 - 2^n)B_n. \tag{1.2}$$

In view of the definitions of G_n and $E_n(x)$, we directly obtain

$$G_n = nE_{n-1}(0), \quad n \geq 1. \tag{1.3}$$

In analogy with Kummer and Carlitz, we here define an odd prime p to be *G-irregular* if it divides at least one of the integers $G_2, G_4, \ldots, G_{p-3}$, and *G-regular* if it does not. The first twenty G-irregular primes are

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

Clearly, if an odd prime p is B-irregular, then it is also G-irregular.

Recall that a *Wieferich prime* is an odd prime p such that $2^{p-1} \equiv 1 \pmod{p^2}$, which arose in the study of Fermat's Last Theorem. So, if an odd prime p is a Wieferich prime, then p divides G_{p-1}, and otherwise it does not divide G_{p-1}. Currently there are only two Wieferich prime known, namely 1093 and 3511. If there are further ones they are larger than 10^{17}. Both 1093 and 3511 are G-irregular primes. However, 1093 is B-regular, and 3511 is B-irregular.

As in the classical case the G-regularity of primes can be linked to the divisibility of some class numbers of cyclotomic fields. Let S be the set of infinite places of $\mathbb{Q}(\zeta_p)$ and T the set of places above the prime 2. Denote by $h_{p,2}$ the (S,T)*-refined class number* of $\mathbb{Q}(\zeta_p)$. Similarly, let $h^+_{p,2}$ be the refined class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ with respect to its infinite places and places above the prime 2 (for the definition of the refined class number of global fields, we refer to Gross [7, Section 1] or Hu and Kim [13, Section 2]). Define

$$h^-_{p,2} = h_{p,2}/h^+_{p,2},$$

It turns out that $h^-_{p,2}$ is an integer (see [13, Proof of Proposition 3.4]).

Theorem 1.5. *Let p be an odd prime. Then, if p is G-irregular, we have $p \mid h^-_{p,2}$. If furthermore p is not a Wieferich prime, the converse is also true.*

1.3.1. *Global distribution of G-irregular primes.* Let g be a non-zero integer. For an odd prime $p \nmid g$, let $\mathrm{ord}_p(g)$ be the multiplicative order of g modulo p, that is the smallest positive integer k such that $g^k \equiv 1 \pmod{p}$.

Theorem 1.6. *A prime p is G-regular if and only if it is B-regular and satisfies* $\mathrm{ord}_p(4) = (p-1)/2$.

Note that $\mathrm{ord}_p(4) \mid (p-1)/2$. Using quadratic reciprocity it is not difficult to show (see Proposition 2.2), that if $p \equiv 1 \pmod 8$, then $\mathrm{ord}_p(4) \neq (p-1)/2$. Thus Theorem 1.6 has the following corollary.

Corollary 1.7. *Primes p satisfying $p \equiv 1 \pmod 8$ are G-irregular.*

Although the B-irregular primes are very mysterious, the set of primes p such that $\mathrm{ord}_p(4) = (p-1)/2$ is far less so. Its distributional properties are analyzed in detail in Proposition 1.10. That result with $a = d = 1$ then yields in combination with Theorem 1.6 the following estimate.

Theorem 1.8. *Let $\mathcal{P}_G$ be the set of G-irregular primes. Let $\epsilon > 0$ be arbitrary and fixed. Then we have, for every x sufficiently large,*

$$\mathcal{P}_G(x) > (1 - \frac{3}{2}A - \epsilon)\frac{x}{\log x},$$

with A the Artin constant

$$A = \prod_{\textit{prime } p}\Big(1 - \frac{1}{p(p-1)}\Big) = 0.3739558136192022880547280543464\ldots. \tag{1.4}$$

Note that $1 - 3A/2 = 0.4390662795\ldots$.

Using Siegel's heuristic, one arrives at the following conjecture.

Conjecture 1.9. *Asymptotically we have*

$$\mathcal{P}_G(x) \sim \Big(1 - \frac{3A}{2\sqrt{e}}\Big)\pi(x) \ (\approx 0.6597765 \cdot \pi(x)).$$

The heuristic behind this conjecture is straightforward. Under the Generalized Riemann Hypothesis (GRH) it can be shown that the set of primes p such that $\mathrm{ord}_p(4) = (p-1)/2$ has density $3A/2$ (Proposition 1.10 with $a = d = 1$). By Siegel's heuristic one expects a fraction $3A/(2\sqrt{e})$ of these to be B-regular. The conjecture follows on invoking Theorem 1.6.

1.3.2. *G-irregular primes in prescribed arithmetic progressions.* Using the following result we can give a non-trivial lower bound for the number of G-irregular primes in a prescribed arithmetic progression. Recall that if $S \subseteq T$ are sets of natural numbers, then the relative density of S in T is defined as

$$\lim_{x\to\infty}\frac{S(x)}{T(x)},$$

if this limit exists.

We use the notations gcd and lcm for greatest common divisor, respectively least common multiple, but often will write (a, b), rather than $\gcd(a, b)$. We also use the big O notation O, and we write O_ρ to emphasise the dependence of the implied constant on some parameter (or a list of parameters) ρ.

Proposition 1.10. *Given two coprime positive integers a and d, we put*

$$\mathcal{Q}(d, a) = \{p > 2 : \ p \equiv a \pmod d, \ \mathrm{ord}_p(4) = (p-1)/2\}. \tag{1.5}$$

Let ϵ be arbitrary and fixed. Then, for every x sufficiently large we have

$$\mathcal{Q}(d, a)(x) < \frac{(\delta(d, a) + \epsilon)}{\varphi(d)}\frac{x}{\log x} \tag{1.6}$$

with

$$\delta(d, a) = c(d, a)R(d, a)A,$$

where

$$R(d,a) = 2\prod_{p\mid(a-1,d)}\Big(1-\frac{1}{p}\Big)\prod_{p\mid d}\Big(1+\frac{1}{p^2-p-1}\Big),$$

and

$$c(d,a) = \begin{cases} 3/4 & \text{if } 4\nmid d;\\ 1/2 & \text{if } 4\mid d, 8\nmid d,\ a\equiv 1 \pmod 4;\\ 1 & \text{if } 4\mid d, 8\nmid d,\ a\equiv 3 \pmod 4;\\ 1 & \text{if } 8\mid d,\ a\not\equiv 1 \pmod 8;\\ 0 & \text{if } 8\mid d,\ a\equiv 1 \pmod 8,\end{cases}$$

is the relative density of the primes $p\not\equiv 1 \pmod 8$ *in the set of primes* $p\equiv a \pmod d$.

Under GRH, we have

$$\mathcal{Q}(d,a)(x) = \frac{\delta(d,a)}{\varphi(d)}\frac{x}{\log x} + O_d\left(\frac{x\log\log x}{\log^2 x}\right). \tag{1.7}$$

A numerical demonstration of this result is given in Section 6. By Proposition 2.2, in case $8|d$ and $a\equiv 1 \pmod 8$, we in fact have $\mathcal{Q}(d,a)=\emptyset$ and so $\mathcal{Q}(d,a)(x)=0$.

Combination of Theorem 1.6 and Proposition 1.10 yields directly the following result.

Theorem 1.11. *Given two coprime positive integers a and d, we put*

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

Let ϵ be arbitrary and fixed. For every x sufficiently large, we have

$$\mathcal{P}_G(d,a)(x) > \frac{(1-\delta(d,a)-\epsilon)}{\varphi(d)}\frac{x}{\log x}, \tag{1.8}$$

where $\delta(d,a)$ is defined in Proposition 1.10.

Under GRH we have

$$\mathcal{P}_G(d,a)(x) \ge \frac{(1-\delta(d,a))}{\varphi(d)}\frac{x}{\log x} + O_d\Big(\frac{x(\log\log x)^2}{\log^2 x}\Big). \tag{1.9}$$

Note that the inequality (1.8) (with $a=d=1$) yields Theorem 1.8 as a special case.

An easy analysis (see (2.6) in Section 2.2) shows that $\delta(d,a)<1$, and so we obtain the following corollary, which can be compared with Theorem 1.2.

Corollary 1.12. *Each primitive residue class contains a subset of G-irregular primes having positive density.*

Moreover, by Corollary 1.7 in case $a\equiv 1 \pmod 8$ and $8|d$, the relative density is 1 and in fact we have $\mathcal{P}_G(d,a)(x)=\pi(x;d,a)$, where

$$\pi(x;d,a) = \#\{p\le x : p\equiv a \pmod d\}.$$

In the remaining cases for a and d, we have $\delta(d,a)>0$, and so $1-\delta(d,a)<1$. However, $1-\delta(d,a)$ can be arbitrarily close to 1 (see Proposition 2.3), and the same holds for the relative density of $\mathcal{P}_G(d,a)$ by Theorem 1.11.

The reasoning that leads us to Conjecture 1.9 in addition with the assumption that B-irregular primes are equidistributed over residue classes with a fixed modulus, suggests that the following conjecture might be true.

Conjecture 1.13. *Given two coprime positive integers a and d, asymptotically we have*

$$\mathcal{P}_G(d,a)(x) \sim \Big(1 - \frac{\delta(d,a)}{\sqrt{e}}\Big)\pi(x;d,a),$$

where $\delta(d,a)$ is defined in Proposition 1.10.

Note that this conjecture implies Conjecture 1.9 (choosing $a = d = 1$). On observing that $\delta(a,d) = 0$ if and only if $8 \mid d$ and $a \equiv 1 \pmod 8$, it also implies the following conjecture.

Conjecture 1.14. *Consider the subset of G-regular primes in the primitive residue class $a \pmod d$. It has a positive density, provided we are not in the case $8 \mid d$ and $a \equiv 1 \pmod 8$.*

2. Preliminaries

In this section, we gather some results which are used later on.

2.1. **Elementary results.** For a primitive Dirichlet character χ with an odd conductor f, the generalized Euler numbers $E_{n,\chi}$ are defined by (see [15, Section 5.1])

$$2\sum_{a=1}^{f} \frac{(-1)^a \chi(a) e^{at}}{e^{ft}+1} = \sum_{n=0}^{\infty} E_{n,\chi}\frac{t^n}{n!}.$$

For any odd prime p, let ω_p be the Teichmüller character of $\mathbb{Z}/p\mathbb{Z}$, and then any multiplicative character of $\mathbb{Z}/p\mathbb{Z}$ is of the form ω_p^k for some $1 \le k \le p-1$. In particular, the odd characters are ω_p^k, $k = 1, 3, \ldots, p-2$.

Lemma 2.1. *Suppose that p is an odd prime and k, n are non-negative integers. Then $E_{k,\omega_p^{n-k}} \equiv E_n(0) \pmod p$.*

Proof. Here we use some notation from [15]. By [15, Proposition 5.4], for any integers $k, n \ge 0$, we have

$$E_{k,\omega_p^{n-k}} = \int_{\mathbb{Z}_p} \omega_p^{n-k}(a) a^k d\mu_{-1}(a). \tag{2.1}$$

By [15, Proposition 2.1 (1)] also $E_n(0)$ can be expressed as a p-adic integral, namely

$$E_n(0) = \int_{\mathbb{Z}_p} a^n d\mu_{-1}(a). \tag{2.2}$$

Since $\omega_p(a) \equiv a \pmod p$, we have

$$\omega_p^{n-k}(a) \equiv a^{n-k} \pmod p \quad \text{and} \quad \omega_p^{n-k}(a)a^k \equiv a^n \pmod p. \tag{2.3}$$

From (2.1), (2.2) and (2.3), we deduce that

$$E_{k,\omega_p^{n-k}} - E_n(0) = \int_{\mathbb{Z}_p} (\omega_p^{n-k}(a)a^k - a^n) d\mu_{-1}(a) \equiv 0 \pmod p. \qquad \square$$

We remark that Lemma 2.1 is an analogue of a well-known result for the generalized Bernoulli numbers; see [31, Corollary 5.15].

Recall that $\mathcal{Q}(d,a)$ is defined in (1.5). For ease of notation we put

$$\mathcal{Q} = \mathcal{Q}(1,1) = \{p > 2 : \mathrm{ord}_p(4) = (p-1)/2\}. \tag{2.4}$$

For the understanding of the distribution of the primes in $\mathcal{Q}$, it turns out to be very useful to consider their residue modulo 8.

Proposition 2.2. *For $j = 1,3,5,7$ we put $\mathcal{Q}_j = \mathcal{Q}(8,j)$. We have*

$$\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_3 \cup \mathcal{Q}_5 \cup \mathcal{Q}_7,$$

with $\mathcal{Q}_1 = \emptyset$, and, for $j = 3,5$,

$$\mathcal{Q}_j = \{p : p \equiv j \pmod 8,\ \mathrm{ord}_p(2) = p-1\},$$

and, furthermore,

$$\mathcal{Q}_7 = \{p : p \equiv 7 \pmod 8,\ \mathrm{ord}_p(2) = (p-1)/2\}.$$

Proof. If $p \equiv 1 \pmod 8$, then by quadratic reciprocity $2^{(p-1)/2} \equiv 1 \pmod p$, and we conclude that $\mathrm{ord}_p(4) \mid (p-1)/4$ and hence $\mathcal{Q}_1 = \emptyset$.

Note that

$$\mathrm{ord}_p(4) = \begin{cases} \mathrm{ord}_p(2) & \text{if } \mathrm{ord}_p(2) \text{ is odd;} \\ \mathrm{ord}_p(2)/2 & \text{otherwise.} \end{cases}$$

In case $p \equiv \pm 3 \pmod 8$, we have $2^{(p-1)/2} \equiv -1 \pmod p$, and so $\mathrm{ord}_p(2)$ must be even. The assumption that p is in $\mathcal{Q}$ now implies that $\mathrm{ord}_p(2) = 2 \cdot \mathrm{ord}_p(4) = p-1$. In case $p \equiv 7 \pmod 8$, we have $2^{(p-1)/2} \equiv 1 \pmod p$, and so $\mathrm{ord}_p(2)$ must be odd. The assumption that p is in $\mathcal{Q}$ now implies that $\mathrm{ord}_p(2) = \mathrm{ord}_p(4) = (p-1)/2$. $\square$

2.2. **The size of $\delta(d,a)$.** In this section we study the extremal behaviour of the quantity $\delta(d,a)$ defined in Proposition 1.10. We put

$$H(d) = \prod_{p \mid d} \left(1 + \frac{1}{p^2 - p - 1}\right), \qquad F(d) = \frac{\varphi(d)}{d} G(d).$$

An easy calculation gives that

$$H(d) = \frac{1}{A} \prod_{p \nmid d} \left(1 - \frac{1}{p(p-1)}\right) = \frac{1}{A}\left(1 + O(\frac{1}{q})\right),$$

where q is the smallest prime not dividing d. Trivially, $H(d) < 1/A$, and $H(d) < 1/(2A)$ when d is odd.

It is a classical result that

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

where γ is the Euler-Mascheroni constant ($\gamma = 0.577215664901532\ldots$). The proof is in essence an application of Mertens' theorem (see, for instance, [1, Theorem 13.14])

$$\prod_{p \le x} (1 - \frac{1}{p}) \sim \frac{e^{-\gamma}}{\log x}. \tag{2.5}$$

An easy variation of the latter proof yields

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

Recall that

$$R(d,a) = 2H(d)\prod_{p\mid b}\left(1-\frac{1}{p}\right) = 2H(d)\frac{\varphi(b)}{b},\ \text{with } b=(a-1,d).$$

Note that

$$2F(d) \le R(d,a) \le 2H(d)/(2,d) < 1/A,$$

and hence $\delta(d,a)=0$ or

$$0 < AF(d) \le \delta(d,a) \le 2AH(d)/(2,d) < 1. \tag{2.6}$$

Proposition 2.3. *We have*

$$\liminf_{d\to\infty} \min_{\substack{1\le a<d\\(a,d)=1\\\delta(d,a)>0}} \delta(d,a)\log\log d = e^{-\gamma} \ \textit{and}\ \limsup_{d\to\infty} \max_{\substack{1\le a<d\\(a,d)=1}} \delta(d,a) = 1$$

Proof. From the above remarks it follows that the limit inferior and superior are $\ge e^{-\gamma}$, respectively ≤ 1. We consider two infinite families of pairs (a,d) to show that these bounds are actually sharp.

Let $n\ge 3$ be arbitrary. Put $d_n=\prod_{3\le p\le n} p$. We have $c(4d_n,1)=1/2$ and

$$\delta(4d_n,1) = (1+o(1))\prod_{2\le p\le n}(1-1/p), \quad (n\to\infty)$$

by Proposition 1.10. Using Mertens' theorem (2.5) and the prime number theorem, we deduce that

$$\delta(4d_n,1)\sim\frac{e^{-\gamma}}{\log n}\sim\frac{e^{-\gamma}}{\log\log(4d_n)}, \quad (n\to\infty),$$

and so the limit inferior actually equals $e^{-\gamma}$.

Put

$$a_n = \begin{cases} 2+3d_n & \text{if } d_n\equiv 7 \pmod 8;\\ 2+d_n & \text{otherwise.}\end{cases}$$

We have $a_n\not\equiv 1 \pmod 8$, $1\le a_n<8d_n$, $(a_n,8d_n)=1$, and $(a_n-1,8d_n)$ is a power of two. We infer that $R(8d_n,a_n)=1/A+O(1/n)$ and $c(8d_n,a_n)=1$, and so $\delta(8d_n,a_n) = 1+O(1/n)$, showing that the limit superior equals 1. □

The two constructions in the above proof are put to the test in Table 1. The table also gives an idea of how fast the lower bound $1-\delta(4d_n,1)$ for the relative density of the set $\mathcal{P}_G(4d_n,1)$ established in Theorem 1.11, tends to 1.

TABLE 1. Some values of $\delta(4d_n, 1)$ and $\delta(8d_n, a_n)$

n	10^3	10^4	10^5	10^6	10^7
$\delta(4d_n, 1) \approx$	0.080954	0.060884	0.048752	0.040638	0.034833
$\delta(4d_n, 1)e^\gamma \log\log(4d_n) \approx$	0.989659	0.997633	0.999422	0.999851	0.999960
$\delta(8d_n, a_n) \approx$	0.999872	0.999990	0.999999	0.9999999	0.99999999

3. Some results related to Artin's primitive root conjecture

It is natural to wonder whether the set $\mathcal{Q}$, see (2.4), is an infinite set or not. This is closely related to Artin's primitive root conjecture stating that if $g \neq -1$ or a square, then infinitely often $\mathrm{ord}_p(g) = p-1$ (which is maximal by Fermat's little theorem). In case g is a square, the maximal order is $(p-1)/2$ and one can wonder whether this happens infinitely often. If this is so for $g = 4$, then our set $\mathcal{Q}$ is infinite. We now go into a bit more technical detail.

We say that a set of primes $\mathcal{P}$ has density $\delta(\mathcal{P})$ and satisfies a Hooley type estimate, if

$$\mathcal{P}(x) = \delta(\mathcal{P})\frac{x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}\right), \tag{3.1}$$

where the implied constant may depend on $\mathcal{P}$.

Let $g \notin \{-1, 0, 1\}$ be an integer. Put

$$\mathcal{P}_g = \{p : \mathrm{ord}_p(g) = p-1\}.$$

Artin in 1927 conjectured that this set, when g is not a square, is infinite and also conjectured a density for it. To this day, this conjecture is open. Hooley [12] proved in 1967 that if the Riemann Hypothesis holds for the number fields $\mathbb{Q}(\zeta_n, g^{1/n})$ with all square-free n (this is a weaker form of the GRH), then the estimate (3.1) holds for the set $\mathcal{P}_g$ with

$$\delta(g) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, g^{1/n}) : \mathbb{Q}]},$$

where μ is the Möbius function, and he showed that $\delta(g)/A$ is rational, with A the Artin constant (see (1.4)), and he explicitly determined this rational number. For example, in case $g = 2$ we have $\delta(2) = A$.

By the Chebotarev density theorem the density of primes $p \equiv 1 \pmod n$ such that $\mathrm{ord}_p(g) \mid (p-1)/n$ is equal to $1/[\mathbb{Q}(\zeta_n, g^{1/n}) : \mathbb{Q}]$. Note that in order to ensure that $\mathrm{ord}_p(g) = p-1$, it is enough to show that there is no prime q such that $\mathrm{ord}_p(g) \mid (p-1)/q$. By inclusion and exclusion we are then led to expect that the set $\mathcal{P}_g$ has natural density $\delta(g)$. The problem with establishing this rigorously is that the Chebotarev density theorem only allows one to take finitely many splitting conditions into account. Let us now consider which result we can obtain on restricting to the primes $q \le y$. Put

$$\delta_y(g) = \sum_{P(n)\le y} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, g^{1/n}) : \mathbb{Q}]}, \tag{3.2}$$

where $P(n)$ denotes the largest prime factor of n. Now we may apply the Chebotarev density theorem and we obtain, for every fixed $y \geq 3$, that

$$\mathcal{P}_g(x) \leq (\delta_y(g) + \epsilon)\frac{x}{\log x}, \tag{3.3}$$

where $\epsilon > 0$ is arbitrary and x is sufficiently large (where sufficiently large may depend on the choice of ϵ).

Completing the sum in (3.2) and using that $[\mathbb{Q}(\zeta_n, g^{1/n}) : \mathbb{Q}] \gg_g n\varphi(n)$ (see [30, Proposition 4.1]), we obtain that

$$\delta_y(g) = \delta(g) + O_g\Big(\sum_{n \geq y} \frac{1}{n\varphi(n)}\Big) = \delta(g) + O_g\big(1/y\big).$$

On combining this with (3.3) we obtain the estimate

$$\mathcal{P}_g(x) \leq (\delta(g) + \epsilon)\frac{x}{\log x}, \tag{3.4}$$

where $\epsilon > 0$ is arbitrary and x is sufficiently large (where sufficiently large may depend on the choices of ϵ and g).

For any integer $g \notin \{-1, 0, 1\}$ and any integer $t \geq 1$, put

$$\mathcal{P}(g,t) = \{p :\ p \equiv 1 \pmod{t},\ \mathrm{ord}_p(g) = (p-1)/t\}.$$

Now, if the Riemann Hypothesis holds for the number fields $\mathbb{Q}(\zeta_{nt}, g^{1/nt})$ with all square-free n, then Hooley's proof can be easily extended, resulting in the estimate (3.1) for the set $\mathcal{P}(g,t)$ with density

$$\delta(g,t) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_{nt}, g^{1/nt}) : \mathbb{Q}]}, \tag{3.5}$$

and with $\delta(g,t)/A$ a rational number; see [16]. This number was first computed explicitly by Wagstaff [30, Theorem 2.2], which can be done much more compactly and elegantly these days using the character sum method of Lenstra et al. [17].

By Wagstaff's work [30] we have $\delta(\mathcal{Q}) = \delta(4,2) = 3A/2$. Alternatively it is an easy and instructive calculation to determine $\delta(4,2)$ oneself. Since $\sqrt{2} \in \mathbb{Q}(\zeta_n)$ if and only if $8 \mid n$, we see that if $4 \nmid n$, then $[\mathbb{Q}(\zeta_{2n}, 2^{1/2n}) : \mathbb{Q}] = \varphi(2n)n$ and so by (3.5),

$$\delta(4,2) = \sum_{n=1}^{\infty} \frac{\mu(n)}{\varphi(2n)n} = \sum_{2\nmid n}^{\infty} \frac{\mu(n)}{\varphi(n)n} + \sum_{2\mid n}^{\infty} \frac{\mu(n)}{2\varphi(n)n} = \frac{3}{4}\sum_{2\nmid n}^{\infty} \frac{\mu(n)}{\varphi(n)n} = \frac{3}{2}A,$$

where we use the fact that

$$\sum_{\substack{n=1 \\ (m,n)=1}}^{\infty} \mu(n)f(n) = \prod_{p\nmid m}(1 - f(p))$$

holds certainly true if the sum is absolutely convergent and $f(n)$ is a multiplicative function defined on the square free integers (cf. Moree and Zumalacárregui [24], where a similar problem with $g = 9$ instead of $g = 4$ is considered).

The following result generalizes the above to the case where we require the primes in $\mathcal{P}(g,t)$ to also be in some prescribed arithmetic progression. It follows from Lenstra's work [16], who introduced Galois theory into the subject.

Theorem 3.1. *Let $1 \le a \le d$ be coprime integers. Let $t \ge 1$ be an integer. Put*

$$\mathcal{P}(g,t,d,a) = \{p : \ p \equiv 1 \pmod{t}, \ p \equiv a \pmod{d}, \ \mathrm{ord}_p(g) = (p-1)/t\}.$$

Let σ_a be the automorphism of $\mathbb{Q}(\zeta_d)$ determined by $\sigma_a(\zeta_d) = \zeta_d^a$. Let $c_a(m)$ be 1 if the restriction of σ_a to the field $\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_m, g^{1/m})$ is the identity and $c_a(m) = 0$ otherwise. Put

$$\delta(g,t,d,a) = \sum_{n=1}^{\infty} \frac{\mu(n) c_a(nt)}{[\mathbb{Q}(\zeta_d, \zeta_{nt}, g^{1/nt}) : \mathbb{Q}]}.$$

Then, assuming RH for all number fields $\mathbb{Q}(\zeta_d, \zeta_{nt}, g^{1/nt})$ with n square-free, we have

$$\mathcal{P}(g,t,d,a)(x) = \delta(g,t,d,a)\frac{x}{\log x} + O_{g,t,d}\left(\frac{x \log\log x}{\log^2 x}\right), \tag{3.6}$$

Unconditionally we have the weaker statement that

$$\mathcal{P}(g,t,d,a) \le (\delta(g,t,d,a) + \epsilon)\frac{x}{\log x}, \tag{3.7}$$

where $\epsilon > 0$ is arbitrary and x is sufficiently large (where sufficiently large may depend on the choice of ϵ, g, t, d and a).

It seems that this result has not been formulated in the literature. It is a simple combination of two cases each of which have been intensively studied, namely the primes having a near-primitive root ($d = 1, t > 1$), and the primes in arithmetic progression having a prescribed primitive root ($t = 1$).

As before $\delta(g,t,d,a)/A$ is a rational number that can be explicitly computed. The case $g = t = 2$, $d = 8$ and $a = 7$ is one of the most simple cases. This is a lucky coincidence, as in our proof of Proposition 1.10 we will apply Theorem 3.1 in order to determine $\delta(\mathcal{Q}_7) = \delta(2,2,8,7)$.

4. Proofs of the main results

It suffices to prove Theorems 1.5 and 1.6 and Proposition 1.10.

4.1. **Proof of Theorem 1.5.** By [13, Proposition 3.4], we obtain

$$h_{p,2}^- = (-1)^{\frac{p-1}{2}} 2^{2-p} E_{0,\omega_p} E_{0,\omega_p^3} \cdots E_{0,\omega_p^{p-2}}.$$

Using Lemma 2.1 and (1.3), we then infer that

$$\begin{aligned} h_{p,2}^- &\equiv (-1)^{\frac{p-1}{2}} 2^{2-p} E_1(0) E_3(0) \cdots E_{p-2}(0) \\ &\equiv \frac{(-1)^{\frac{p-1}{2}} 2^{2-p}}{(p-1)!} G_2 G_4 \cdots G_{p-3} G_{p-1} \pmod{p}, \end{aligned}$$

which implies the desired result. $\square$

4.2. **Proof of Theorem 1.6.** Given an odd prime p, if it is G-regular, then there is no $1 \le k \le (p-3)/2$ such that p divides the integer G_{2k}, that is, $2(1-2^{2k})B_{2k}$ by (1.2). Now if $\mathrm{ord}_p(4) \le (p-3)/2$, then $p \mid 2^{2k}-1$ with $k = \mathrm{ord}_p(4) \le (p-3)/2$. If $\mathrm{ord}_p(4) = (p-1)/2$, then we have $p \nmid 2^{2k}-1$ for $k = 1, 2, \ldots, (p-3)/2$. The desired result follows. □

4.3. **Proof of Proposition 1.10.** The proof relies on Theorem 3.1. We only establish the assertion under GRH, as the proof of the unconditional result is very similar. Namely, it uses the unconditional estimate (3.7) instead of (3.6).

It is enough to prove the result in case $8 \mid d$. In fact, in case $8 \nmid d$ we lift the congruence class $a \pmod d$ to congruence classes with modulus $\mathrm{lcm}(8,d)$. The ones among those that are $\not\equiv 1 \pmod 8$ have relative density $AR(\mathrm{lcm}(8,d),a) = AR(d,a)$ (as $R(d,a)$ only depends on the odd prime factors of d). The one that is $\equiv 1 \pmod 8$ (if it exists at all) has relative density zero. It follows that the relative density of the unlifted congruence equals $c(d,a)R(d,a)A$ with $c(d,a)$ the relative density of the primes $p \not\equiv 1 \pmod 8$ in the congruence class $a \pmod d$. The easy determination of $c(d,a)$ is left to the interested reader.

From now on we assume that $8 \mid d$. We can write $a \equiv j \pmod 8$ for some $j \in \{1,3,5,7\}$ and distinguish three cases.

Case I: $j = 1$. By Proposition 2.2 the set $\mathcal{Q}(d,a)$ is empty and the result holds trvially true.

Case II: $j \in \{3,5\}$. By Proposition 2.2,

$$\mathcal{Q}(d,a) = \{p : \ p \equiv a \pmod d, \ \mathrm{ord}_p(2) = p-1\}.$$

By Theorem 3.1, under GRH, this set has density $\delta(2,1,d,a)$. For arbitrary g,d,a the third author determined the rational number $\delta(g,1,d,a)/A$, see [21, Theorem 1] or [22, Theorem 1.2]. On applying his result, the proof of this subcase is then completed.

Case III: $j = 7$. By Proposition 2.2,

$$\mathcal{Q}(d,a) = \{p : \ p \equiv a \pmod d, \ \mathrm{ord}_p(2) = (p-1)/2\}.$$

For simplicity we write $\delta = \delta(\mathcal{Q}(d,a))$. By Theorem 3.1 we have

$$\delta = \delta(2,2,d,a) = \sum_{n=1}^{\infty} \frac{\mu(n)c_a(2n)}{[\mathbb{Q}(\zeta_d, \zeta_{2n}, 2^{1/2n}) : \mathbb{Q}]}. \tag{4.1}$$

In case n is even, then trivially $\mathbb{Q}(\sqrt{-1}) \subseteq \mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{2n}, 2^{1/2n})$. As σ_a acts by conjugation on $\mathbb{Q}(\sqrt{-1})$, cf. [22, Lemma 2.2], and not as the identity, it follows that $c_a(2n) = 0$.

Next assume that n is odd and square-free. Then by [22, Lemma 2.4] we infer that

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

Since

$$\sigma_a\big|_{\mathbb{Q}(\sqrt{2})} = \mathrm{id.} \quad \text{and} \quad \sigma_a\big|_{\mathbb{Q}(\zeta_{(d,2n)})} \begin{cases} = \mathrm{id.} & \text{if } a \equiv 1 \pmod{(d,2n)}; \\ \neq \mathrm{id.} & \text{otherwise,} \end{cases}$$

we infer that

$$c_a(2n) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod{(d, 2n)}; \\ 0 & \text{otherwise.} \end{cases}$$

Note that the assumptions on a, d and n imply that $a \equiv 1 \pmod{(d, 2n)}$ iff $a \equiv 1 \pmod{2(d, n)}$ iff $a \equiv 1 \pmod{(d, n)}$. We conclude that (4.1) simplifies to

$$\delta = \sum_{\substack{2\nmid n \\ a\equiv 1 \pmod{(d,n)}}} \frac{\mu(n)}{[\mathbb{Q}(\zeta_d, \zeta_{2n}, 2^{1/2n}) : \mathbb{Q}]}.$$

When n is odd and square-free, using [22, Lemma 2.3] we obtain

$$[\mathbb{Q}(\zeta_d, \zeta_{2n}, 2^{1/2n}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{\mathrm{lcm}(d,2n)}, 2^{1/2n}) : \mathbb{Q}] = n\varphi(\mathrm{lcm}(d, 2n)) = n\varphi(\mathrm{lcm}(d, n)).$$

We thus obtain that

$$\varphi(d)\delta = \sum_{\substack{2\nmid n \\ a\equiv 1 \pmod{(d,n)}}} \frac{\mu(n)\varphi(d)}{n\varphi(\mathrm{lcm}(d, n))}.$$

Put

$$w(n) = \frac{n\varphi(\mathrm{lcm}(d, n))}{\varphi(d)}.$$

In this notation we obtain

$$\delta = \frac{1}{\varphi(d)} \sum_{\substack{2\nmid n \\ a\equiv 1 \pmod{(d,n)}}} \frac{\mu(n)}{w(n)},$$

where the argument in the sum is multiplicative in n. Using [22, Lemma 3.1] and the notation used there and in [22, Theorem 1.2], we find

$$\begin{aligned} \varphi(d)\delta &= S(1) - S_2(1) = 2S(1) = 2A(a, d, 1) \\ &= 2A \prod_{p|(a-1,d)} (1 - \frac{1}{p}) \prod_{p|d} \left(1 + \frac{1}{p^2 - p - 1}\right) = \delta(d, a), \end{aligned}$$

as was to be proved. □

5. Outlook

A small improvement of the upper bound (1.6) (and consequently the lower bound (1.8)) would be possible if instead of the estimate (3.7) a Vinogradov type estimate for $\mathcal{P}(g, t, d, a)(x)$ could be established, say

$$\mathcal{P}(g, t, d, a)(x) \le \delta(g, t, d, a)\frac{x}{\log x} + O_{g,t,d}\Big(\frac{x(\log\log x)^2}{\log^{5/4} x}\Big). \tag{5.1}$$

Vinogradov [29] established the above result in case $a = d = t = 1$. Establishing (5.1) seems technically quite involved. Recent work by Pierce et al. [25] offers perhaps some hope that one can even improve on the error term in (5.1).

TABLE 2. The ratio $\mathcal{P}_G(x)/\pi(x)$

x	experimental	theoretical
10^5	0.661592	0.659776
10^6	0.659558	
$2 \cdot 10^6$	0.660860	
$3 \cdot 10^6$	0.661413	
$4 \cdot 10^6$	0.660683	
$5 \cdot 10^6$	0.660864	

TABLE 3. The ratio $\mathcal{P}_G(d,a)(x)/\pi(x;d,a)$ for $x = 5 \cdot 10^6$

$p \equiv a \pmod{d}$	experimental	theoretical
$p \equiv 1 \pmod{3}$	0.728296	0.727821
$p \equiv 2 \pmod{5}$	0.643010	0.641870
$p \equiv 1 \pmod{4}$	0.771512	0.773184
$p \equiv 9 \pmod{20}$	0.757311	0.761246
$p \equiv 11 \pmod{12}$	0.460584	0.455642
$p \equiv 19 \pmod{20}$	0.528567	0.522493
$p \equiv 7 \pmod{8}$	0.550086	0.546368
$p \equiv 13 \pmod{24}$	0.634191	0.637094

6. Some numerical experiments

In this section, using the Bernoulli numbers modulo p function developed by David Harvey in Sage [27] (see [2, 9, 10] for more details and improvements), we provide numerical evidence for the truth of Conjectures 1.9 and 1.13 (both concerning G-irregular primes) and also for (1.7) in Proposition 1.10.

In the data, we only record the first six digits of the decimal parts.

Table 2 gives the ratio $\mathcal{P}_G(x)/\pi(x)$ for various values of x, and the value in the column 'theoretical' is the limit value $1 - 3A/(2\sqrt{e})$ predicted by Conjecture 1.9.

Table 3 gives the ratio $\mathcal{P}_G(d,a)(x)/\pi(x;d,a)$ for $x = 5 \cdot 10^6$ in the column 'experimental' for various choices of a and d, and the corresponding limit values $1 - c(d,a)R(d,a)A/\sqrt{e}$ predicted by Conjecture 1.13 are in the column 'theoretical'.

Table 4 gives the ratio $\mathcal{P}(d,a)(x)/\pi(x;d,a)$ for $x = 5 \cdot 10^6$ in the column 'experimental' for various choices of a and d. In the column 'theoretical', there is the corresponding relative density $\delta(d,a)$ predicted in (1.7) and known to be true under GRH.

In view of the definition of the constant $c(d,a)$ in Proposition 1.10, there are four cases excluding the case $8|d$ and $a \equiv 1 \pmod{8}$ (which gives $c(d,a) = 0$). For each of these four cases there are two instances in Tables 3 and 4.

Acknowledgement

This work was supported by the National Natural Science Foundation of China, Grant No. 11501212. The research of Min-Soo Kim and Min Sha was also supported by the

TABLE 4. The ratio $\mathcal{Q}(d,a)(x)/\pi(x;d,a)$ for $x = 5 \cdot 10^6$

$p \equiv a \pmod{d}$	experimental	theoretical
$p \equiv 1 \pmod{3}$	0.449049	0.448746
$p \equiv 2 \pmod{5}$	0.589614	0.590456
$p \equiv 1 \pmod{4}$	0.374664	0.373955
$p \equiv 9 \pmod{20}$	0.395498	0.393637
$p \equiv 11 \pmod{12}$	0.898284	0.897493
$p \equiv 19 \pmod{20}$	0.789316	0.787275
$p \equiv 7 \pmod{8}$	0.747300	0.747911
$p \equiv 13 \pmod{24}$	0.598815	0.598329

Kyungnam University Foundation Grant, 2017, respectively the Macquarie University Research Fellowship. The authors thank Bernd Kellner and Peter Stevenhagen for very helpful feedback, without the former the name Genocchi would not have appeared in the title.

References

[1] T.M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

[2] J.P. Buhler and D. Harvey, *Irregular primes to 163 million*, Math. Comp. **80** (2011), 2435–2444.

[3] L. Carlitz, *Note on irregular primes*, Proc. Amer. Math. Soc. **5** (1954), 329–331.

[4] R. Ernvall, *On the distribution mod 8 of the E-irregular primes*, Ann. Acad. Sci. Fenn. Ser. A I, **1** (1975), 195–198.

[5] R. Ernvall, *Generalized Bernoulli numbers, generalized irregular primes, and class number*, Ann. Univ. Turku., Ser. AI **178** (1979), 72 pp.

[6] R. Ernvall, *Generalized irregular primes*, Mathematika **30** (1983), 67–73.

[7] B. Gross, *On the values of abelian L-functions at $s = 0$*, J. Fac. Sci. Univ. Tokyo **35** (1988), 177–197.

[8] F.H. Hao and C.J. Parry, *Generalized Bernoulli numbers and m-regular primes*, Math. Comp. **43** (1984), 273–288.

[9] W. Hart, D. Harvey and W. Ong, *Irregular primes to two billion*, Math. Comp. **86** (2017), 3031–3049.

[10] D. Harvey, *A multimodular algorithm for computing Bernoulli numbers*, Math. Comp. **79** (2010), 2361–2370.

[11] J. Holden, *Irregularity of prime numbers over real quadratic fields*, Algorithmic number theory (J.P. Buhler, ed.), Springer, Lect. Notes Comput. Sci. **1423** (1998), 454–462.

[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] K.L. Jensen, *Om talteoretiske Egenskaber ved de Bernoulliske Tal*, Nyt Tidsskr. Mat. **26**, Afd. B (1915), 73–83.

[15] M.-S. Kim and S. Hu, *On p-adic Hurwitz-type Euler zeta functions*, J. Number Theory **132** (2012), 2977–3015.

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

[17] H.W. Lenstra, Jr., P. Moree and P. Stevenhagen, *Character sums for primitive root densities*, Math. Proc. Cambridge Philos. Soc. **157** (2014), 489–511.

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

[19] T. Metsänkylä, *Distribution of irregular prime numbers*, J. Reine Angew. Math. **282** (1976), 126–130.

[20] H.L. Montgomery, *Distribution of irregular primes*, Illinois J. Math. **9** (1965), 553–558.

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

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

[23] P. Moree, *Artin's primitive root conjecture − a survey*, Integers **12A** (2012), A13.

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

[25] L.B. Pierce, C.L. Turnage-Butterbaugh and M.M. Wood, *An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups*, arXiv:1709.09637, preprint, 2017.

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

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

[28] H.S. Vandiver, *Note on Euler number criteria for the first case of Fermat's last theorem*, Amer. J. Math. **62** (1940). 79–82.

[29] A.I. Vinogradov, *Artin's L-series and his conjectures*, (English. Russian original), Proc. Steklov Inst. Math. **112**, 124–142 (1971); translation from Trudy Mat. Inst. Steklov **112**, 123–140 (1971).

[30] S.S. Wagstaff, Jr., *Pseudoprimes and a generalization of Artin's conjecture*, Acta Arith. **41** (1982), 141–150.

[31] L.C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer-Verlag, New York, 1997.

Department of Mathematics, South China University of Technology, Guangzhou 510640, China

E-mail address: mahusu@scut.edu.cn

Division of Mathematics, Science, and Computers, Kyungnam University, 7(Woryeong-dong) kyungnamdaehak-ro, Masanhappo-gu, Changwon-si, Gyeongsangnam-do 51767, Republic of Korea

E-mail address: mskim@kyungnam.ac.kr

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

E-mail address: moree@mpim-bonn.mpg.de

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: shamin2010@gmail.com