ARTIN’S PRIMITIVE ROOT CONJECTURE
- a survey -

PIETER MOREE
(with contributions by A.C. Cojocaru, W. Gajda and H. Graves)

To the memory of John L. Selfridge (1927-2010)

ABSTRACT. One of the first concepts one meets in elementary number theory is that of the multiplicative order. We give a survey of the literature on this topic emphasizing the Artin primitive root conjecture (1927). The first part of the survey is intended for a rather general audience and rather colloquial, whereas the second part is intended for number theorists and ends with several open problems. The contributions in the survey on ‘elliptic Artin’ are due to Alina Cojocaru. Wojciec Gajda wrote a section on ‘Artin for K-theory of number fields’, and Hester Graves (together with me) on ‘Artin’s conjecture and Euclidean domains’.

CONTENTS

1. Introduction 2
2. Naive heuristic approach 5
3. Algebraic number theory 5
3.1. Analytic algebraic number theory 6
4. Artin’s heuristic approach 8
5. Modified heuristic approach (à la Artin) 9
6. Hooley’s work 10
6.1. Unconditional results 12
7. Probabilistic model 13
8. The indicator function 17
8.1. The indicator function and probabilistic models 17
8.2. The indicator function in the function field setting 18
9. Some variations of Artin’s problem 20
9.1. Elliptic Artin (by A.C. Cojocaru) 20
9.2. Even order 22
9.3. Order in a prescribed arithmetic progression 24
9.4. Divisors of second order recurrences 25
9.5. Lenstra’s work 29
9.6. Artin’s conjecture and Euclidean domains (written with Hester Graves) 29
9.7. Miscellaneous 35
10. Open problems 59
11. Acknowledgement 68
References 68
1. Introduction

Gauss [175] considered in articles 315-317 of his Disquisitiones Arithmeticae (1801) the decimal expansion of numbers of the form \( \frac{1}{p} \) with \( p \) prime. For example, \( \frac{1}{7} = 0.142857142857 \ldots \), \( \frac{1}{11} = 0.090909 \ldots \).

These decimal expansions for \( p \neq 2 \) and \( p \neq 5 \) are purely periodic. It is easy to see that the period is equal to the smallest positive integer \( k \) such that \( 10^k \equiv 1 \pmod{p} \). This integer \( k \) is the multipliclicative order of 10 modulo \( p \) and is denoted by \( \text{ord}_p(10) \). The integer \( k \) equals the order of the group generated by 10 in \( \mathbb{Z}/p\mathbb{Z}^* \), the multiplicative subgroup of residue classes modulo \( p \). By Lagrange’s theorem the order of a subgroup of a finite group is a divisor of the number of elements in the group. Since \( \mathbb{Z}/p\mathbb{Z}^* \) has \( p - 1 \) elements, we conclude that \( \text{ord}_p(10) \mid (p - 1) \). If \( \text{ord}_p(10) = p - 1 \), we say that 10 is a primitive root mod \( p \). The decimal expansion we have given for \( \frac{1}{7} \) shows that 10 is a primitive root mod 7. Gauss’ table gives several other such examples and he must have asked himself whether there are infinitely many such primes, that is, primes \( p \) for which the decimal period is \( p - 1 \).

Some light on this question can be shed on using the simple observation (due to Chebyshev) that if \( q = 4p + 1 \) is a prime with \( p \) a prime satisfying \( p \equiv 2 \pmod{5} \), then 10 is a primitive root modulo \( q \). Note that, a priori, \( \text{ord}_q(10) \in \{1, 2, 4, p, 2p, 4p\} \). Now, using the law of quadratic reciprocity, see, e.g., Lemmermeyer [291], one deduces that

\[
10^{2p} \equiv \left( \frac{10}{q} \right) = \left( \frac{2}{q} \right) \left( \frac{5}{q} \right) = (-1)^{\frac{q-1}{8}} \left( \frac{q}{5} \right) = -\left( \frac{4}{5} \right) \equiv -1 \pmod{q},
\]

where we also used that \( q \equiv 4 \pmod{5} \) and \( q \equiv 5 \pmod{8} \). Since no prime divisor of \( 10^4 - 1 \) satisfies the requirements (and hence \( \text{ord}_q(10) \nmid 4 \)), one sees that \( \text{ord}_q(10) = 4p = q - 1 \).

The logarithmic integral \( \text{Li}(x) \) is defined as \( \int_2^x \frac{dt}{\log t} \). By partial integration one has that \( \text{Li}(x) \sim x/\log x \) (i.e. the quotient of the r.h.s. and l.h.s. tends to 1 as \( x \) tends to infinity). The prime number theorem in the form

\[
\pi(x) := \#\{p \leq x\} \sim \text{Li}(x), \quad x \to \infty,
\]

suggests that the ‘probability that a number \( n \) is prime’ is \( 1/\log n \). (Then we expect \( \sum_{2 \leq n \leq x} 1/\log n \) primes \( \leq x \) and asymptotically this is equal to \( \text{Li}(x) \).) Thus for both \( n \) and \( 4n + 1 \) to be prime and \( n \equiv 2 \pmod{5} \) we expect a probability of \( 1/(5\log^2 n) \), assuming independence of these three events. Since they are not, we have to correct by some positive constant \( c \) and hence expect that up to \( x \) there are at least \( cx/\log^2 x \) (note that \( \sum_{2 \leq n \leq x} \log^{-2} n \sim x \log^{-2} x \) primes \( p \) such that 10 is a primitive root mod \( p \). Hence we expect that there are infinitely many primes \( p \) having 10 as a primitive root mod \( p \). This conjecture is commonly attributed to Gauss, however, to the author’s knowledge there is no written evidence for it.

Emil Artin in 1927, led by a partial heuristic argument (sketched in §4), made the following conjecture, where for a given \( g \in \mathbb{Q}^* \) we define

\[
\mathcal{P}(g) = \{ p : \text{ord}_p(g) = p - 1 \} \quad \text{and} \quad \mathcal{P}(g)(x) = \#\{p \in \mathcal{P}(g) : p \leq x\}.
\]

(In general, if \( S \) is a set, we define \( S(x) = \#\{s \in S : s \leq x\} \).)
Conjecture 1. Artin’s primitive root conjecture (1927).
Let $g \in \mathbb{Q}\backslash\{-1,0,1\}$.
(Qualitative form) The set $\mathcal{P}(g)$ is infinite if $g$ is not a square of a rational number.
(Quantitative form) Let $h$ be the largest integer such that $g = g_0^h$ with $g_0 \in \mathbb{Q}$. We have, as $x$ tends to infinity,

$$
\mathcal{P}(g)(x) = \prod_{q \mid h} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right) \frac{x}{\log x} + o \left(\frac{x}{\log x}\right).
$$

(1)
Here an Euler product $\prod_q f(q)$ appears, where $f(q) = 1 + O(q^{-2})$ (to ensure convergence) and $q$ runs over the primes. We will come across many more Euler products in this paper. Usually they have an interpretation as a density.

Write the main term in (1) as $A(h) x / \log x$. In case $h$ is even, $A(h)$ equals a positive rational multiple of $A(1) = \prod_q \left(1 - \frac{1}{q(q-1)}\right) = 0.3739558136192 \ldots$, the Artin constant. Thus the quantitative form implies the qualitative form.

The product defining the Artin constant does not converge quickly. It turns out that for numerical approximations it is possible and indeed much more efficient to write $A = \prod_{k=2}^{\infty} \zeta(k)^{-e_k}$, with $e_k \in \mathbb{N}$ and $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ the celebrated Riemann zeta function. This then allows one to determine $A$ without too much effort with a precision of 1000 decimals, as zeta values can be easily evaluated with high numerical precision. This method applies to all Euler products that occur in the sequel, cf. [22, 95, 157, 341].

Usually one speaks about the Artin primitive root conjecture, rather than Artin’s conjecture since there are various unresolved conjectures due to Artin (most notably the Artin holomorphy conjecture). Indeed, there are even papers where both these conjectures make an appearance, e.g. [321].

The starting point of our analysis of Artin’s primitive root conjecture is the following observation:

$$
p \in \mathcal{P}(g) \iff g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \text{ for every prime } q \text{ dividing } p - 1. \quad (2)
$$

"\implies" Obvious.
"\impliedby" Suppose $p \notin \mathcal{P}(g)$. Then $g^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ for some $k | p - 1$, $k > 1$. But this implies that $g^{\frac{p-1}{q_1}} \equiv 1 \pmod{p}$ for some prime divisor $q_1$ of $k$. This is a contradiction.

Thus, associated with a prime $p$ we have conditions for various $q$. We are going to interchange the role of $p$ and $q$, that is for a fixed $q$ we consider the set of primes $p$ such that $p \equiv 1 \pmod{q}$ and $g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$.

This set of primes can be considered heuristically (§2), but also studied on invoking (analytic) algebraic number theory and hence we make a brief excursion to this
area (§3) before taking up our Artinian considerations in §4 again.

Remark 1. Instead of asking whether infinitely often the period length is maximal, one might ask the easier question of whether infinitely often the period length is even. Here the answer is yes and much more is known. We come back to this in §9.2.

Remark 2. There is more to decimal expansions than meets the eye. For example, Girstmair [177] proved that if a prime $p$ is such that its decimal expansion $1/p = 0.x_1x_2\ldots x_{p-1}x_1\ldots$ has period $p-1$, then the difference between the sums of its even and odd places, namely $(x_2 + x_4 + \ldots + x_{p-1}) - (x_1 + x_3 + \ldots + x_{p-2})$, is $11h_{Q(\sqrt{-p})}$ if $p \equiv 3 \pmod{4}$ and is zero otherwise, where $h_{Q(\sqrt{-p})}$ denotes the so-called class number of the imaginary quadratic number field $Q(\sqrt{-p})$ (number fields are briefly discussed in §3.) For a variation of this result involving $\sum_{k=1}^{p-1}(-1)^k x_k x_{k+r}$ see Aguirre and Peral [2]. Hirabayashi [232] generalized Girstmair’s formula to all imaginary abelian number fields. Ram Murty and Thangadurai [380] generalized Girstmair’s result to the case where the period is $(p-1)/r$, where now $r > 1$ is also allowed. Here generalized Bernoulli numbers $B_{1,\chi}$ enter the picture. Other examples are provided in §9.2 and Khare [256].

Historical remark. To the modern number theorist it is a bit strange that Gauss spent such an effort on the rather recreational topic of decimal periods. However, Bullynck [54] points out that this was a German research topic (1765-1801), and that the young Gauss, being aware of these developments, placed the whole theory on a firm number-theoretic foundation, thereby solving most of the problems left by the mathematicians before him. One might have expected him to raise the question of whether the period is maximal for infinitely many primes. There does not seem to be evidence for this. As Bullynck (personal communication) points out, this kind of existential question is not typical for 18th century mathematics.

In Hasse’s mathematical diary (Tagebuch) of the year 1927 there is (information provided by Roquette) an entry entitled “Die Dichte der Primzahlen $p$, für die $\alpha$ primitive Wurzel ist (nach mündlicher Mitteilung von Artin 13. IX. 27)” under the date of 27 Sep. 1927. Although the Artin conjecture presumably predates the 13th of September of 1927, for lack of written evidence of this, the author takes the 13th of September of 1927 to be its birthday.

The Artin conjecture has already been formulated before Artin. It can already be found in a paper of Cunningham [117], but, in contrast to Artin, Cunningham’s insights into the problem do not seem to go beyond numerical observations. Today Cunningham is best known for the Cunningham Project which seeks to factor the numbers $b^n \pm 1$ for $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers $n$, see, e.g., [484].

Warning. This survey aims to be fairly complete, but still it reflects the (un)familiarity of its author with various aspects of the topic. He sought to compensate for this
in some cases by inviting a ‘guest surveyor’ to write something on aspects not so familiar to him, where there is a more extensive literature available.

2. Naive heuristic approach

Fix any prime $q$. We try to compute the density of primes $p$ such that both $p \equiv 1 \pmod{q}$ and $g^{p-1}/q \equiv 1 \pmod{p}$. The prime number theorem for arithmetic progressions states that, as $x$ tends to infinity,

$$
\pi(x; d, a) := \sum_{\substack{p \leq x \\ p \equiv a \pmod{d}}} 1 \sim \frac{x}{\varphi(d) \log x}.
$$

(3)

The residue classes $a \pmod{d}$ with $(a, d) = 1$ are said to be primitive. Note that given an integer $d$, with finitely many exceptions, a prime must be in a primitive residue class modulo $d$. Since there are $\varphi(d)$ primitive residue classes modulo $d$, (3) says that the primes are asymptotically equidistributed over the primitive residue classes modulo $d$ (in view of the prime number theorem). Dirichlet’s theorem (1837) is the weaker statement that any primitive residue class contains infinitely many primes.

By (3) $p \equiv 1 \pmod{q}$ holds true for primes $p$ with frequency $1/\varphi(q) = 1/(q - 1)$. Recall Fermat’s little theorem which asserts that $g^{p-1} \equiv 1 \pmod{p}$ if $p \nmid g$. Using this we infer, in case $p \nmid g$, that $g^{q-1}$ is a solution of $x^q \equiv 1 \pmod{p}$. We expect there to be $q$ solutions and we want a solution to be 1 modulo $q$. Thus we expect to be successful with probability $1/q$, except when $q | h$. Then $g^{p-1}/q = g_0^{h^{-1}} \equiv 1 \pmod{p}$, trivially. If we assume that these events are independent, then the probability that both events occur is $1/q$ if $q \nmid h$ and $1/q^{-1}$ otherwise.

By (2) the above events should not occur for any $q$ in order to ensure that $p \in \mathcal{P}(g)$. This suggests a natural density of

$$
\prod_{q \nmid h} \left(1 - \frac{1}{q(q - 1)}\right) \prod_{q | h} \left(1 - \frac{1}{q - 1}\right) = A(h)
$$

for such primes and hence we expect (1) to hold true.

3. Algebraic number theory

In order to understand Artin’s approach to his conjecture we need some facts about algebraic number theory. We say $\alpha$ is algebraic over $\mathbb{Q}$ if it satisfies an equation of the form $f(\alpha) = 0$ with $f(x) \in \mathbb{Z}[x]$. We say $\alpha$ is an algebraic integer over $\mathbb{Q}$ if it satisfies an equation of the form $f(\alpha) = 0$, where $f(x) \in \mathbb{Z}[x]$ is monic. A number field over $\mathbb{Q}$ is a field obtained by adjoining finitely many algebraic numbers $\alpha_1, \ldots, \alpha_s$ to $\mathbb{Q}$. That is, $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_s)$. By $\mathbb{Q}(\alpha_1, \ldots, \alpha_s)$ we denote the smallest field containing $\alpha_1, \ldots, \alpha_s$ and $\mathbb{Q}$. The so called theorem of the primitive element asserts that for a given number field $K$ there exists an algebraic integer $\alpha$ such that $K = \mathbb{Q}(\alpha)$. The element $\alpha$ is said to be a primitive element. For an algebraic integer $\alpha$ let $f_\alpha(x)$ be the unique (as it turns out) monic polynomial $f_\alpha(x)$ of smallest degree such that $f_\alpha(\alpha) = 0$. Then $K = \mathbb{Q}(\alpha)$ is isomorphic to $\mathbb{Q}[x]/(f_\alpha(x))$. The
degree \([K : \mathbb{Q}]\) of \(K\) is defined as \(\deg f_\alpha(x)\). The compositum of two fields \(K\) and \(L\) is defined as the smallest field containing both \(K\) and \(L\).

**Example.** Let \(\alpha = i\). Then \(f_\alpha(x) = x^2 + 1\). Note that \(\mathbb{Q}[x]\) contains elements of the form \(\sum_{j=0}^{m} a_j x^j\). These elements correspond with an element in \(\mathbb{Q}[x]/(x^2 + 1)\) obtained by replacing every \(x^2\) by \(-1\). Thus, as a set, \(\mathbb{Q}[x]/(x^2 + 1) \cong \{a + bx \mid a, b \in \mathbb{Q}\}\). Similarly, as a set, \(\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}\). It is not difficult to see that a field isomorphism between \(\mathbb{Q}(i)\) and \(\mathbb{Q}[x]/(x^2 + 1)\) is given by sending \(x\) to \(i\).

For a general number field \(K\), we have the following picture:

\[
\mathbb{Q}(\alpha) = K \supset \mathcal{O}_K \cup \cup \mathbb{Q} \supset \mathbb{Z}
\]

Here \(\mathcal{O}_K\) is the ring of integers of the field \(K\). It plays a role analogous to that of \(\mathbb{Z}\) in \(\mathbb{Q}\) (in our example \(\mathcal{O}_K\) is \(\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}\) the ring of Gaussian integers). The main theorem of arithmetic states that, up to the order of factors, factorisiation into primes in \(\mathbb{Z}\) is unique. One might hope for a ring inside \(K\) with similar properties. Let us consider the set of algebraic integers over \(\mathbb{Q}\) that are inside \(K\). This set is actually a ring, the ring of integers, \(\mathcal{O}_K\), of \(K\). It usually does not have unique factorization in elements. It, however, has unique factorization into terms of prime ideals (up to order of factors). The prime ideal \((p)\) in \(\mathbb{Z}\) turns out to factor as \(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}\) inside \(\mathcal{O}_K\). The equivalent statement of \(p = \#\mathbb{Z}/p\mathbb{Z}\) in \(\mathbb{Z}\), reads in \(\mathcal{O}_K\): \(p^{f_i} = \#\mathcal{O}_K/\mathfrak{P}_i \mathcal{O}_K\). Here \(f_i\) is called the degree of the prime ideal \(\mathfrak{P}_i\).

More generally, \(\#\mathcal{O}_K/\mathfrak{a} \mathcal{O}_K\), notation \(N\mathfrak{a}\) is the norm of the ideal \(\mathfrak{a}\). We have the relationship \(\sum_{i=1}^{g} e_i f_i = n\), with \(n\) the degree of \(K\). We say that a rational prime \(p\) splits completely in \(\mathcal{O}_K\) if \(e_i = f_i = 1\) for \(i = 1, \ldots, g\). Note that in this case \(g = n\). If a prime \(p\) splits completely in the ring of integers \(\mathcal{O}_K\), with \(K \cong \mathbb{Q}[x]/(f(x))\), then over \(\mathbb{Z}/p\mathbb{Z}\), \(f(x)\) splits into \(n\) distinct linear factors.

### 3.1. Analytic algebraic number theory

Let \(\mathfrak{D}\) run through the non-zero integral ideals of \(\mathcal{O}_K\), with \(K\) a number field. For \(\Re(s) > 1\), we define \(\zeta_K(s) = \sum_{\mathfrak{D}} N\mathfrak{D}^{-s}\) and elsewhere by analytic continuation. Note that if \(K = \mathbb{Q}\), then \(\zeta_K(s) = \zeta(s)\), the usual Riemann zeta-function. For \(\Re(s) > 1\) we have an Euler product, \(\zeta_K(s) = \prod_{\mathfrak{P}} (1 - N\mathfrak{P}^{-s})^{-1}\), where the product runs over all prime ideals \(\mathfrak{P}\) of \(\mathcal{O}_K\). In 1903, Landau proved the Prime Ideal Theorem to the effect that

\[
\pi_K(x) := \sum_{N\mathfrak{P} \leq x} 1 \sim \text{Li}(x), \quad x \to \infty.
\]

Assuming the Riemann Hypothesis for the field \(K\), that is, assuming that all the non-trivial zeros of \(\zeta_K(s)\) are on \(\Re(s) = \frac{1}{2}\), one obtains the much sharper estimate

\[
\pi_K(x) = \text{Li}(x) + O_K(\sqrt{x} \log x), \quad x \to \infty,
\]

where the implied constant depends at most on \(K\). (For Landau’s big O-notation and related notation like \(\Omega(x)\) we refer to any introductory book on analytic number theory, e.g., [11, 330, 473].)

In the analysis of Artin’s primitive root conjecture an infinite family of fields will
play a role and we need an error term in (4) that is explicit in its dependency on $K$. Such a result was folklore and finally written down by Lang [282]:

$$\pi_K(x) = \text{Li}(x) + O(\sqrt{x} \log(x^{[K:Q]}|D_K|)),$$

(5)

where $D_K$ denotes the discriminant of the field $K$.

The function $\pi_K(x)$ is heavily biased towards prime ideals of degree one:

$$\pi_K(x) = \sum_{N\mathfrak{P} \leq x, N\mathfrak{P} = p} 1 + \cdots$$

$$= \sum_{N\mathfrak{P} \leq x, N\mathfrak{P} = p} 1 + O([K:Q] \sum_{p \leq x} 1) = \sum_{N\mathfrak{P} \leq x, N\mathfrak{P} = p} 1 + O([K:Q]\sqrt{x}).$$

In Artin’s problem one is specifically interested in so called normal fields. For such a field all prime ideals of degree one, with at most finitely many exceptions, come from rational primes $p$ that split completely. Throwing out these exceptions we have the following picture:

$$\mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_n \quad \mathfrak{P}_1' \mathfrak{P}_2' \cdots \mathfrak{P}_n'$$

(A $[K:Q]$-fold covering of the rational primes.) Thus, for a normal field we have

$$\pi_K(x) = [K:Q] \sum_{p \text{ splits completely in } K} 1 + O([K:Q]\sqrt{x} \log x),$$

that is, by the Prime Ideal Theorem,

$$\sum_{\substack{p \leq x \\text{p splits completely in } K}} 1 \sim \frac{1}{[K:Q]} \frac{x}{\log x}, \quad x \to \infty.$$  

(6)

This is a particular case of a very important result called the Chebotarev density theorem. For a nice introductory account see Lenstra and Stevenhagen [470]. Another recommendable paper (research level) on this topic is a paper by Serre [454].

Example. (Cyclotomic fields). A cyclotomic field $K$ is a field of the form $K = \mathbb{Q}(\zeta_n)$ with $\zeta_n = e^{2\pi i/n}$ and $n$ a natural number. One can show that

$$f_{\zeta_n}(x) = \prod_{\substack{a=1 \\text{mod } n \atop (a,n)=1}}^n (x - \zeta_n^a) = \Phi_n(x) \in \mathbb{Z}[x].$$

The polynomial $\Phi_n(x)$ is the $n$th cyclotomic polynomial. From this we deduce that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(x) = \varphi(n)$. The cyclotomic fields are normal. It can be shown that $p$ splits completely in $K$ iff $p \equiv 1 \text{mod } n$ iff $x^n - 1$ factors completely over $\mathbb{Z}/p\mathbb{Z}$. 
Applying (6) we deduce that
\[ \sum_{p \leq x \atop p \equiv 1 \pmod{n}} 1 \sim \frac{x}{\varphi(n) \log x}, \quad x \to \infty, \]
a particular case of (3). The same result can be deduced for every primitive residue class modulo \( n \) on invoking Chebotarev’s density theorem. Thus the Chebotarev density theorem implies the prime number theorem for arithmetic progressions (3).

4. Artin’s heuristic approach

We have now assembled the required preliminaries to continue the story on the progress made on Artin’s primitive root conjecture. Remember that we are interested in the set of all primes \( p \) satisfying
\[ p \equiv 1 \pmod{q}, \quad g^{\frac{p-1}{q}} \equiv 1 \pmod{p}, \]
where \( q \) is any fixed prime. By what we have learned about cyclotomic fields the primes \( p \equiv 1 \pmod{q} \) are precisely those for which the equation \( x^q \equiv 1 \pmod{p} \) has \( q \) distinct solutions mod \( p \). Claim: if \( g^{\frac{p-1}{q}} \equiv 1 \pmod{p} \), then \( x^q \equiv g \pmod{p} \) has a solution mod \( p \). To see this, write \( g = \gamma^a \) with \( \gamma \) a primitive root mod \( p \). Then \( \gamma^{aq} \equiv 1 \pmod{p} \). A power of a primitive root can only be congruent to \( 1 \pmod{p} \) if the exponent is a multiple of \( p - 1 \), hence \( q|a \). This implies \( a = bq \). Then \( (\gamma^b)^q \equiv g \pmod{p} \) and this proves the claim. Let \( \alpha_1, \ldots, \alpha_q \) be the distinct mod \( p \) solutions of \( x^q \equiv 1 \pmod{p} \). Then we see that \( \alpha_1 \gamma^b, \ldots, \alpha_q \gamma^b \) are all distinct solutions of \( x^q \equiv g \pmod{p} \). We conclude that a prime which satisfies \( p \equiv 1 \pmod{q} \) and \( g^{\frac{p-1}{q}} \equiv 1 \pmod{p} \) splits completely in the number field
\[ k_q := \mathbb{Q}(\zeta_q, g^{\frac{1}{q}}). \quad (7) \]
(Note that it does not make a difference which \( q \)th root of \( g \) we take, since we always end up with the same field.) We leave it to the reader to show that if \( p \) splits completely in \( k_q \), then \( p \equiv 1 \pmod{q} \) and \( g^{\frac{p-1}{q}} \equiv 1 \pmod{p} \). Thus we have
\[ p \equiv 1 \pmod{q}, \quad g^{\frac{p-1}{q}} \equiv 1 \pmod{p} \iff p \text{ splits completely in } k_q. \]
Let us denote the degree of \( k_q \) by \( n(q) \). It is not difficult to show that \( k_q \) is normal. Hence we may apply (6) to deduce that the number of primes \( p \leq x \) that do not split completely in \( k_q \) equals \((1 - 1/n(q))x/\log x \), asymptotically. So one expects \( \prod_q (1 - 1/n(q)) \) as the density of primes \( p \) for which \( g \) is a primitive root mod \( p \).

This heuristic argument was thought to be plausible until about 1960, when the Lehmers [289] made some numerical calculations that did not seem to always match with Artin’s heuristic. Then, in 1968, Heilbronn realized that the events ‘\( p \) does not split completely in \( k_q \)” are not necessarily independent as \( p \) and \( q \) range through all primes and published a corrected quantitative conjecture. Artin, however, made this correction much earlier, namely in 1958 in a letter to the Lehmers in a response to a letter of the Lehmers regarding his numerical work. Artin did not publish his corrected conjecture, nor did the Lehmers refer to Artin in their paper [289].
although they give the correction factor. As late as 1964 Hasse provided a correction factor in the 1964 edition of his book [217] that is incorrect if \( g \equiv 1(\mod 4) \) is not a prime. For some excerpts of the correspondence between Artin and the Lehmers, see Stevenhagen [168].

Take for example \( g = 5 \), thus \( h = 1 \) (with \( h \) defined as in Conjecture 1). Then \( k_2 = \mathbb{Q}(\sqrt{5}) \subseteq k_3 = \mathbb{Q}(\zeta_5, 5^{1/5}) \), i.e. \( k_2 \) is a subfield of \( k_3 \) (since \( \sqrt{5} = \zeta_5^2 - \zeta_5^3 + \zeta_5^4 \)). Now if \( K \subseteq L \) and \( p \) splits completely in \( L \), then \( p \) must split completely in \( K \). This means that the condition ‘\( p \) does not split completely in \( k_2 \)’ implies the condition ‘\( p \) does not split completely in \( k_3 \)’. So, assuming that there are no further dependencies between the various conditions on \( q \), we expect that

\[
P(5)(x) \sim \prod_{q \neq 5} \left( 1 - \frac{1}{n(q)} \right) \frac{x}{\log x} \sim \prod_{q \neq 5} \left( 1 - \frac{1}{q(q-1)} \right) \frac{x}{\log x}, \ x \to \infty.
\]

Note that the Euler product involved equals \( 20A/19 \). This turns out to be more consistent with the numerical data than Artin’s prediction \( A \).

5. Modified heuristic approach (à la Artin)

Recall that \( k_q \) is defined in [7] for prime \( q \). Let \( m \) be squarefree. We define \( k_m \) to be the compositum of the fields \( k_q \) with \( q|m \) and prime. It can be shown that \( k_m = \mathbb{Q}(\zeta_m, g^{1/m}) \). We are interested in the density of primes \( p \) that do not split completely in any \( k_q \) (if this exists). We can try to compute it by inclusion-exclusion. So we start writing down \( 1 - \frac{1}{n(2)} - \frac{1}{n(3)} \cdots \). However, we have counted double here the primes \( p \) that split completely in both \( k_2 \) and \( k_3 \). It can be shown that the primes that split completely in both \( k_n \) and \( k_m \) are precisely the primes that split completely in \( k_{\text{lcm}(n,m)} \). Thus we have to add \( \frac{1}{n(6)} \). Continuing in this way we arrive at the heuristic

\[
P(g)(x) \sim \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(\zeta_k, g^{1/k}) : \mathbb{Q}]} \frac{x}{\log x}, \ x \to \infty.
\]

Here \( \mu \) is the M"obius function. It is defined by \( \mu(1) = 1 \), and if \( n > 1 \), then \( \mu(n) = (-1)^s \), where \( s \) denotes the number of distinct prime factors of \( n \) if \( n \) is squarefree, and \( \mu(n) = 0 \) otherwise. If we are only interested in the primes \( p \) that do not split completely in any of a finite set of number fields, then there would be little to prove (by invoking Chebotarev’s theorem). It is the infinitely many \( q \) that makes the problem hard.

Artin’s heuristic amounts to assuming that the fields \( k_{q_1} \) and \( k_{q_2} \) are linearly disjoint over \( \mathbb{Q} \) (i.e. \( k_{q_1} \cap k_{q_2} = \mathbb{Q} \)), for distinct primes \( q_1 \) and \( q_2 \). This has as a consequence that \([k_{q_1,q_2} : \mathbb{Q}] = [k_{q_1} : \mathbb{Q}][k_{q_2} : \mathbb{Q}]\) and in general for squarefree \( k \) that \( n(k) = k\varphi(k)/(k,h) \). Thus, according to Artin we should have

\[
\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} = \sum_{k=1}^{\infty} \frac{\mu(k)(k,h)}{k\varphi(k)} = \prod_{q|h} \left( 1 - \frac{1}{q(q-1)} \right) \prod_{q|h} \left( 1 - \frac{1}{q-1} \right) = A(h),
\]
where in the derivation of the last equality we used the fact (see, e.g., [330, Theorem 1.9]) that if $f(k)$ is a multiplicative function, then
\[
\sum_{k=1}^{\infty} |f(k)| < \infty \Rightarrow \sum_{k=1}^{\infty} f(k) = \prod_q (1 + f(q) + f(q^2) + \cdots).
\]

(A function $f$ on the integers is called multiplicative if when $(n, m) = 1$, then $f(nm) = f(n)f(m)$.) It can be shown that if $g \neq -1$ and $g$ is not a square, then
\[
\sum_{k=1}^{\infty} \mu(k) n(k) = c_g A,
\]
where $c_g > 0$ is a rational number depending on $g$.

Let $g \neq -1$ or a square. Hooley [238] proved in 1967 that if the Riemann Hypothesis holds for the number fields $\mathbb{Q}(\zeta_k, g^{1/k})$ with $k$ squarefree, then we have
\[
\mathcal{P}(g)(x) = \frac{x}{\log x} \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(\zeta_k, g^{1/k}) : \mathbb{Q}]} + O_g \left( \frac{x \log \log x}{\log^2 x} \right),
\]
and he explicitly evaluated the latter sum, say $\delta(g)$, as
\[
\delta(g) = \left\{ \begin{array}{ll}
A(h) & \text{if } d \not\equiv 1 \pmod{4};
\left( 1 - \mu(|d|) \prod_{q \mid d} \frac{1}{q - 1} \prod_{p \mid h} \frac{1}{p - 1} \right) A(h) & \text{otherwise},
\end{array} \right.
\]
with $d$ the discriminant of $\mathbb{Q}(\sqrt{g})$. For convenience we denote the assumption on the fields $\mathbb{Q}(\zeta_k, g^{1/k})$ made by Hooley as Hooley’s Riemann Hypothesis (HRH) and the quantity $x \log \log x / \log^2 x$ as $R(x)$.

6. HOOLEY’S WORK

For simplicity we assume $g = 2$ and sketch Hooley’s proof [238]. The restriction $g = 2$ allows us to focus exclusively on the analytical aspects, the algebraic aspects being discussed elsewhere in this survey.

A large part of his paper is devoted to proving an estimate for
\[
P(x, l) = \# \{ p \leq x : p \text{ splits completely in } k_l \},
\]
for which the implied constant in the error term does not depend on $l$. His result on this is a special case of the result [5] of Lang [282] (proven a few years later):
\[
P(x, l) = \frac{\text{Li}(x)}{[k_l : \mathbb{Q}]} + O(\sqrt{x} \log (lx)),
\]
where we assume the Riemann Hypothesis for $k_l$. Another quantity needed is
\[
N(x, \eta) = \# \{ p \leq x : p \text{ does not split completely in } k_q, \ \forall q \leq \eta \}.
\]
By inclusion-exclusion we have $N(x, \eta) = \sum_{l'} \mu(l') P(x, l')$, where $l'$ ranges over all divisors of $\prod_{q \leq \eta} q$. Note that, for $\eta$ large enough,
\[
\prod_{q \leq \eta} q = e^{\sum_{q \leq \eta} \log q} \leq e^{2\eta},
\]
where we used that \( \sum_{q \leq \eta} \log q \sim \eta \) (which is equivalent with the prime number theorem). Observe that \( P(2)(x) = N(x, x - 1) \). The problem in estimating \( N(x, \eta) \) is that by using inclusion-exclusion and \( (\mathcal{I}) \) we can only estimate \( N(x, \eta) \) for rather small \( \eta \), whereas one would like to take \( \eta = x - 1 \) and so we are forced to work with \( N(x, \eta) \) for \( \eta \) rather smaller than \( x \). We will actually choose \( \eta = \frac{1}{6} \log x \) and thus \( l' < e^{2n} = x^{1/3} \) (for \( x \) large enough). Let us introduce a third quantity \( M(x, \eta_1, \eta_2) = \# \{ p \leq x : p \text{ splits completely in some } k_q, \eta_1 < q < \eta_2 \} \). It is easy to see that

\[
N(x, \xi_1) - M(x, \xi_1, \xi_2) - M(x, \xi_2, \xi_3) - M(x, \xi_3, x - 1) \leq P(2)(x) \leq N(x, \xi_1),
\]

that is,

\[
P(2)(x) = N(x, \xi_1) + O(M(x, \xi_1, \xi_2)) + O(M(x, \xi_2, \xi_3)) + O(M(x, \xi_3, x - 1)).
\]

We will choose \( \xi_1 = \frac{1}{6} \log x, \xi_2 = \sqrt{x} \log^{-2} x \) and \( \xi_3 = \sqrt{x} \log x \). Note the small gap between \( \xi_2 \) and \( \xi_3 \). This is the ‘hard region’ and unfortunately it seems out of reach to close it, and work say with

\[
P(2)(x) = N(x, \xi_1) + O(M(x, \xi_1, \xi_2)) + O(M(x, \xi_2, x - 1)).
\]

Now using the estimate for \( P(x, l) \) one easily arrives at

\[
N(x, \xi_1) = \text{Li}(x) \sum_{l' \leq x^{1/4}} \frac{\mu(l')}{l' \varphi(l')} + O \left( \frac{x}{\log^2 x} \right)
\]

\[
= A \text{Li}(x) + O \left( \frac{x}{\log^2 x} \right)
\]

Again using the estimate for \( P(x, q) \) we arrive at

\[
M(x, \xi_1, \xi_2) \leq \sum_{\xi_1 \leq q \leq \xi_2} P(x, q) = O \left( \frac{x}{\log^2 x} \right).
\]

In the region \((\xi_2, \xi_3)\) we use the fact that the primes \( p \) counted by \( P(x, q) \) certainly satisfy \( p \equiv 1 \pmod{q} \). Thus \( P(x, q) \leq \pi(x, q, 1) \). Then using the Brun-Titchmarsh estimate

\[
\pi(x, q, 1) \leq \frac{2x}{\varphi(q) \log(x/q)}, \quad 1 \leq q < x,
\]

we obtain

\[
M(x, \xi_2, \xi_3) \leq \sum_{\xi_2 \leq q \leq \xi_3} P(x, q) \leq \sum_{\xi_2 \leq q \leq \xi_3} \pi(x, q, 1) = O \left( \frac{x}{\log x} \sum_{\xi_2 \leq q \leq \xi_3} \frac{1}{q} \right).
\]

Using a result of Mertens to the effect that

\[
\sum_{p \leq x} \frac{1}{p} = \log \log x + \text{constant} + O \left( \frac{1}{\log x} \right),
\]

it then follows that

\[
\sum_{\xi_2 \leq p \leq \xi_3} \frac{1}{p} = O \left( \frac{\log \log x}{\log x} \right).
\]
and hence $M(x; \xi_2, \xi_3) = O(R(x))$. Finally, if a prime $p$ is counted by $M(x, \xi_3, x - 1)$, then its order is less than $\frac{x}{\xi_3} = \frac{\sqrt{x}}{\log x}$ and thus it divides $2^m - 1$ for some $m < \sqrt{x}/\log x$.

Now

$$2^{M(x, \xi_3, x - 1)} < \prod_{p \text{ counted by } M(x, \xi_3, x - 1)} p \leq \prod_{m < \frac{\sqrt{x}}{\log x}} (2^m - 1).$$

Thus

$$M(x, \xi_3, x - 1) < \sum_{m < \frac{\sqrt{x}}{\log x}} m = O\left(\frac{x}{\log^2 x}\right).$$

On gathering all terms we obtain $\mathcal{P}(2)(x) = A\text{Li}(x) + O(R(x))$.

Repeating this argument for arbitrary $g \neq -1$ or a square, we arrive at HRH, which implies the truth of the qualitative form of Artin’s primitive root conjecture and a modified form of the quantitative version. This completes the sketch of the proof.

Vinogradov [482] has shown that unconditionally

$$\mathcal{P}(g)(x) \leq \delta(g)\pi(x) + O_g\left(\frac{x(\log \log x)^2}{\log^{5/4} x}\right),$$

where $\delta(g)$ is the density of primitive roots as determined by Hooley (given by (10)). Vinogradov’s proof contains some small errors that have been corrected by Van der Waall [478]. Wiertelak [501] has established a version of this result (with a larger error term, however), where he made the $g$ dependence of the error explicit.

6.1. Unconditional results. If one asks for unconditional results, the state of affairs is quite appalling. There is no known number $g$ for which $\mathcal{P}(g)$ is known to be infinite! In 1986, however, Heath-Brown [222] proved (improving on earlier fundamental work by Gupta, Ram Murty and Srinivasan [202, 379]) a result which implies that there are at most two primes $q_1$ and $q_2$ for which $\mathcal{P}(q_1)$ and $\mathcal{P}(q_2)$ are finite and at most three squarefree numbers $s_1, s_2, s_3$ for which $\mathcal{P}(s_1), \mathcal{P}(s_2)$ and $\mathcal{P}(s_3)$ are finite.

Remember the observation that if $q = 4p + 1$ and $p \equiv 2(\text{mod} 5)$, then $q \in \mathcal{P}(10)$. Sieve theory cannot prove presently that there are infinitely many such primes. However, the so called lower bound sieve method combined with the Chen-Iwaniec switching method gave rise to $\gg x \log^{-2} x$ primes $p \leq x$ such that either $p - 1 = 2^e q$ for some prime $q$ or $p - 1 = 2^e q_1 q_2$ with $p^\alpha < q_1 < p^\beta$ for some $\alpha > \frac{1}{4}$ and $\delta < \frac{1}{2}$. This together with a rather elementary argument, is then enough to establish Heath-Brown’s result.

Reznikov and Moree [128] established a variant of Heath-Brown’s result and used it to make considerable progress regarding a conjecture of Lubotzky and Shalev to the extent that for all $d$ sufficiently large the number of subgroups of index $d$ in the fundamental group $\pi_1(M)$ of a hyperbolic three manifold $M$ is at least $e^{cd(M)}$, for some positive constant $c(M)$ depending at most on $M$.

Skolem has raised the question of whether all the integral solutions of $X_1X_2 - X_3X_4 = 1$ can be obtained from a fixed polynomial solution by letting the variables
run through \( \mathbb{Z} \) and expressed his belief in favour of a negative answer. Zannier has shown that if one not only considers solutions in integers, but those in \( S \)-integers, where \( S \) is a finite set of places, then for a suitable finite \( S \) the answer to Skolem’s question is positive. His proof makes use of a fundamental lemma, the proof of which makes use of a variation of Heath-Brown’s arguments.

6.1.1. Variants for quadratic fields. Narkiewicz proved the unconditional result, valid for a certain subclass of abelian number fields, that if \( a_1, a_2, a_3 \) are multiplicatively independent integers in \( \mathcal{O}_K \) with their norms satisfying certain conditions, then at least one of the numbers \( a_1, a_2, a_3 \) is a primitive root for infinitely many prime ideals of \( K \) of the first degree. The proof uses ideas from the papers by Gupta and Ram Murty and Heath-Brown.

Given a nontrivial unit in a real quadratic number field, for a rational prime \( p \) which is inert in the field the maximal order of the unit modulo \( p \) is \( p + 1 \). An extension of Artin’s conjecture is that there are infinitely many such inert primes for which this order is maximal. This is known at present only under GRH. Unconditionally, J. Cohen showed that for any choice of 7 units in different real quadratic fields satisfying a certain simple restriction, at least one of these units satisfies this version of Artin’s conjecture.

Given an algebraic number from a quadratic field, for a rational prime \( p \) which is inert in the field the maximal order of the unit modulo \( p \) is \( p^2 - 1 \). An extension of Artin’s conjecture is that there are infinitely many such inert primes for which this order is maximal. J. Cohen recently showed that, given a quadratic field \( K \), for any choice of 85 algebraic numbers satisfying a certain simple restriction, at least one of them has order modulo \( p \) at least \( (p^2 - 1)/24 \) for infinitely many inert primes \( p \) in \( K \).

7. Probabilistic model

Is there a probabilistic model for a prime \( p \) to be such that \( g \) is a primitive root mod \( p \)? That is, does there exist a function \( f_g(p) \) such that

\[
\sum_{p \in S, p \leq x} f_g(p) \sim \sum_{p \in S, p \leq x} 1, \tag{13}
\]

where \( S \) must be a set of primes having a positive natural density.

There are \( \varphi(p - 1) \) primitive roots mod \( p \) and thus one could try to take \( f_g(p) = \varphi(p - 1)/(p - 1) \), assuming that the primitive roots are randomly distributed over \( 1, \ldots, p - 1 \). Results of Elliott, Cobeli and Zaharescu, Rudnick and Zaharescu, and Wang and Bauer indeed all suggest that the distribution of the primitive roots over \( 1, \ldots, p - 1 \) is to a large extent governed by Poisson processes. Thus we would hope to find something like

\[
\sum_{p \leq x} \frac{\varphi(p - 1)}{p - 1} \sim \mathcal{P}(g)(x), \quad x \to \infty. \tag{14}
\]
However, by Hooley’s theorem there are under HRH \( g_1 \) and \( g_2 \) such that \( \mathcal{P}(g_1)(x) \sim \mathcal{P}(g_2)(x) \). Thus (14) cannot be true for all \( g \). Let us not be deterred by this and try to evaluate \( \sum_{p \leq x} \frac{\varphi(p-1)}{p-1} \). Note that \( \frac{\varphi(n)}{n} = \prod_{p \mid n} (1 - \frac{1}{p}) = \sum_{d \mid n} \frac{\mu(d)}{d} \). Thus

\[
\sum_{p \leq x} \frac{\varphi(p-1)}{p-1} = \sum_{p \leq x} \sum_{d \mid p-1} \frac{\mu(d)}{d} = \sum_{d \leq x} \frac{\mu(d)}{d} \sum_{p \leq x, p \equiv 1(d)} 1 = \sum_{d \leq x} \frac{\mu(d)}{d} \pi(x, d, 1).
\]

Let \( c_1 \) be a fixed real number. Then the estimate

\[
\pi(x; d, a) = \frac{\text{Li}(x)}{\varphi(d)} + O(x e^{-c_2 \sqrt{\log x}}) \tag{15}
\]

holds uniformly for all integers \( a \) and \( d \) such that \((a,d) = 1\) and \( 1 \leq d \leq \log c_1 x \), with \( c_2 \) some positive constant. This is a well-known result due to Siegel and Walfisz and sharpens (3). On applying it we obtain

\[
\sum_{p \leq x} \frac{\varphi(p-1)}{p-1} = \text{Li}(x) \sum_{d \leq \log c_1 x} \frac{\mu(d)}{d \varphi(d)} + O \left( \frac{x}{\log^c x} \right) = A \text{Li}(x) + O \left( \frac{x}{\log^c x} \right).
\]

(This result is Lemma 1 in Stephens [466], an earlier argument along the same lines is given in Pillai [418] who considered \( \sum_{p \leq x} \varphi(p-1) \).)

Recall that Artin’s heuristic answer was not always correct because it failed to take into account quadratic interactions. So let us try to incorporate this into our model. In order that \( g \) is a primitive root mod \( p \) it is necessary that \((g/p) = -1\) and this is a quadratic condition. In particular if \( g \) has to be a primitive root it must be a non-square mod \( p \). There are \((p-1)/2\) non-squares and \( 2\varphi(p-1)/(p-1) \) is their density. Thus it makes sense to try to evaluate the sum in the identity below.

Assuming HRH, by a computation a little more complicated than for the sum with the condition \((g/p) = -1\) omitted:

\[
2 \sum_{p \leq x, (\frac{q}{p}) = -1} \frac{\varphi(p-1)}{p-1} = \mathcal{P}(g)(x) + O(R(x)).
\]

In case \( h > 1 \), with \( h \) as in Conjecture 1, equality does not always hold. The effect we have to take into account there is that if \((p-1, h) > 1\), then

\[
g^{\frac{p-1}{(p-1, h)}} \equiv \left( g_{\frac{p-1}{p}}^{(p-1, h)} \right)^{p-1} \equiv 1 \pmod{p},
\]

and thus \( g \) cannot be a primitive root mod \( p \).

Here is a proposal for \( f_g(p) \):

\[
f_g(p) = \begin{cases} 
2 \varphi(p-1) & \text{if } \left( \frac{2}{p} \right) = -1 \text{ and } (p-1, h) = 1; \\
0 & \text{otherwise}.
\end{cases} \tag{16}
\]

It can be shown assuming HRH (see [339]) that

\[
\sum_{p \leq x} f_g(p) = \mathcal{P}(g)(x) + O(R(x)), \tag{17}
\]
and thus if $S$ is the set of all primes, then \[ (16) \] gives a probabilistic model that works.

On noting that the naive heuristic fails the traditional approach was to show that it holds true on average:

$$\frac{1}{N} \sum_{g \leq N} \mathcal{P}(g)(x) = \frac{1}{N} \sum_{p \leq x} M_p(N),$$

where $M_p(N)$ is the number of integers $g \leq N$ that are primitive roots modulo $p$. Clearly $M_p(N) = \phi(p - 1)\left\{ \frac{N}{p} + O(1) \right\}$. Thus

$$\frac{1}{N} \sum_{g \leq N} \mathcal{P}(g)(x) = \sum_{p \leq x} \frac{\phi(p - 1)}{p - 1} + O \left( \frac{x^2}{N \log x} \right) + O \left( \frac{x}{\log^D x} \right),$$

provided that $N > x^2 \log^{D-1} x$. Less trivial unconditional results in this direction were obtained by Goldfeld \[179\] and Stephens \[466\], see also Li \[304\]. (For an analogue for number fields see Egami \[129\].)

It is relatively easy to compute the first sum in \[13\] with $S = \{ p : p \equiv a (\mod f) \}$ and one obtains a relatively complicated but completely explicit Euler product. The question is whether the true behaviour of

$$\mathcal{P}(g, f, a)(x) := \# \{ p \leq x : p \in \mathcal{P}(g), p \equiv a (\mod f) \}$$

works with this.

Lenstra’s work \[292\], which introduced Galois theory into the subject, implies the following result on $\mathcal{P}(g, f, a)(x)$.

**Theorem 1.** Let $1 \leq a \leq f, (a, f) = 1$. Let $\sigma_a$ be the automorphism of $\mathbb{Q}(\zeta_f)$ determined by $\sigma_a(\zeta_f) = \zeta_f^a$. Let $c_a(n)$ be 1 if the restriction of $\sigma_a$ to the field $\mathbb{Q}(\zeta_f) \cap \mathbb{Q}(\zeta_n, g^{1/n})$ is the identity and $c_a(n) = 0$ otherwise. Put

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

Then, assuming RH for all number fields $\mathbb{Q}(\zeta_f, \zeta_n, g^{1/n})$ with $n$ squarefree,

$$\mathcal{P}(g, f, a)(x) = \delta(a, f, g) \frac{x}{\log x} + O_{g,f}(R(x)).$$

Inspired by the relatively easy Euler product coming from quadratic heuristics, the author set out to explicitly evaluate $\delta(a, f, g)$ and managed to find an Euler product for it (see the 2008 paper \[353\] which appeared earlier as a MPIM-preprint in 1998):

**Theorem 2.** Let $g$ be an integer with $|g| > 1$. Let $h$ be the largest integer such that $g$ is an $h$-th power of an integer. Write $g = g_1 g_2^2$ with $g_1, g_2$ integers and $g_1$ squarefree. Put

$$A(a, f, h) = \prod_{q | (a-1, f)} \left( 1 - \frac{1}{q} \right) \prod_{q | f, p \mid h} \left( 1 - \frac{1}{q - 1} \right) \prod_{p \mid f, p \not| h} \left( 1 - \frac{1}{q(q-1)} \right)$$
if \((a - 1, f, h) = 1\) and \(A(a, f, h) = 0\) otherwise. Let 
\[
\beta = \frac{g_1}{(g_1, f)} \quad \text{and} \quad \gamma_1 = \begin{cases} (-1)^{\frac{\beta - 1}{2}}(f, g_1) & \text{if } \beta \text{ is odd;} \\ 1 & \text{otherwise.} \end{cases}
\]

We have 
\[
\delta(a, f, g) = \frac{A(a, f, h)}{\varphi(f)} \left(1 - \frac{\gamma_1}{\alpha} \prod_{q|\beta, \, q \mid h} (q - 2) \prod_{p|\beta, \, p \mid h} (q^2 - q - 1) \right)^{\mu(|\beta|)}
\]
in case \(g_1 \equiv 1(\text{mod } 4)\) or \(g_1 \equiv 2(\text{mod } 4)\) and \(8|f\) or \(g_1 \equiv 3(\text{mod } 4)\) and \(4|f\) and
\[
\delta(a, f, g) = \frac{A(a, f, h)}{\varphi(f)},
\]
otherwise. Here \((\cdot)\) denotes the Kronecker symbol.

This formula is the same as the one found with quadratic heuristics! As a consequence we have the following result \[339\], which generalizes \[17\]:

**Theorem 3.** Assume RH for all number fields \(\mathbb{Q}(\zeta_f, \zeta_n, g^{1/n})\) with \(n\) squarefree. Then
\[
\sum_{p \leq x \atop p \equiv a(\text{mod } f)} f_g(p) = \mathcal{P}(g, f, a)(x) + O_{g,f}(R(x)).
\]

A rather more insightful derivation of the Euler product for \(\delta(a, f, g)\) is given in a paper by Lenstra, Moree and Stevenhagen \[296\], as a consequence of a more explicit approach involving quadratic characters in the line of Lenstra’s earlier work. This approach is the most powerful thus far in finding explicit Euler products for primitive root densities. For a preview of this work see Stevenhagen \[468\]. The upshot is that the density for a whole class of Artin type problems can be always written as
\[
\delta = (1 + \prod_q E_q) \prod_q A_q,
\]
where the \(E_q\) are (real)-character averages and hence satisfy \(-1 \leq E_p \leq 1\). Only finitely many of them are distinct from 1. The infinite product \(\prod_q A_q\) can be regarded as the ‘canonical’ density of the problem at hand. In this formulation the situations where \(\delta = 0\) can be relatively easily computed (from the expression of the density as an infinite sum this can be quite hard, cf. the formula for \(\delta(a, f, g)\) in Theorem \[1\]). For the original Artin problem a very easy computation yields \(\prod_q A_q = A(h)\) and \(1 + \prod_q E_q = E\) and one finds \[10\] again, see \[468\]. In the same paper the method is applied to deal with near-primitive roots (see §9.7.3), improving on earlier treatments of this problem. In particular, the first satisfactory treatment of the vanishing in the near-primitive root problem is given. In a sequel to this paper, authored by Moree and Stevenhagen \[361\], the method is used to deal with some higher-rank variations of Artin’s primitive root conjecture. Again this leads to the quickest known proofs of Euler product forms of the relevant densities.

Rodier \[432\], in connection with a coding theoretical result involving Dickson polynomials, was interested in the set of primes \(p\) such that \(p \equiv a(\text{mod } 28)\), with
\(a \in \{-1, 3, 19\}\). Assuming equidistribution over the congruence classes modulo 28 one would expect (as did Rodier) that the density of this set of primes is \(3A/\phi(28) = A/4\). Moree \[334\] computed the density of primes \(p\) (on GRH) such that \(2\) is a primitive root modulo \(p\), \(\left(\frac{2}{p}\right) = \epsilon_j\), for \(1 \leq j \leq s\) and \(p \equiv \epsilon_0(\text{mod} \ 4)\), with \(\epsilon_0, \ldots, \epsilon_s \in \{\pm 1\}\) and the \(l_j\) distinct odd primes. Applying this result with \(\epsilon_0 = -1\), \(s = 1\), \(\epsilon_1 = -1\) and \(l_1 = 7\), it then follows that Rodier’s set has density \(21A/82\) on GRH, contradicting his conjecture. Of course one can also use Theorem \[2\] to arrive at this density.

One can ask for which \(f\) and \(g\) we have equidistribution over the congruence classes modulo \(f\) of the primes \(p\) for which \(g\) is a primitive root modulo \(p\), that is for which \(f\) and \(g\) does there exist \(\delta\) such that \(\delta(a, f, g) = \delta\) for all \(a\) with \((a, f) = 1\)? The explicit formula for \(\delta(a, f, g)\) allows one to determine the \(f\) such that the primes in \(P(g)\) are equidistributed in the various primitive residue classes mod \(f\). This was done earlier by Moree \[338\] using an Euler product for \(\delta(1, f, g)\) (which is easier to obtain) and some Galois theoretic arguments. Using the Euler product for \(\delta(a, f, g)\) given in \[353\] a shorter proof can be given (in the same article). Basically \(f\) must be a power of two in case \(h = 1\). Also \(2^a 3^b\) can occur, the smallest positive integer \(g\) for which this happens is \(g = 21^7\).

8. The indicator function

8.1. The indicator function and probabilistic models. Let \(G\) be a finite cyclic group of order \(n\) and put \(f(g) = 1\) if \(G\) is generated by \(g\) and \(f(g) = 0\) otherwise. It was already observed a long time ago (see, e.g., \[280\], Satz 496 and \[225\] for a version over number fields) that

\[
f(g) = \frac{\phi(n)}{n} \sum_{d|n} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \mod d} \chi(g),
\]

where the sum is over the characters \(\chi\) of \(G\) having order \(d\). Using this, one deduces that

\[
P(g)(x) = \sum_{p \leq x} \frac{\varphi(p - 1)}{p - 1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \mod d} \chi(g),
\]

where the inner sum is over the characters of \((\mathbb{Z}/p\mathbb{Z})^*\) of order \(d\). Now write \(P(g)(x) = \sum_{d \leq x} S_d(x)\), with

\[
S_d(x) = \frac{\mu(d)}{\varphi(d)} \sum_{p \leq x, \ p \equiv 1(\text{mod} \ d)} \frac{\varphi(p - 1)}{p - 1} \sum_{\chi \mod d} \chi(g).
\]

Note that

\[
S_1(x) = \sum_{p \leq x} \frac{\varphi(p - 1)}{p - 1}
\]

and that

\[
S_2(x) = -\left(\frac{g}{p}\right) \sum_{p \leq x} \frac{\varphi(p - 1)}{p - 1}.
\]
with \((\frac{g}{p})\) the Legendre symbol. The term \(S_d(x)\) can be written as a linear combination of terms
\[
\frac{1}{\pi(x)} \sum_{p \leq x, \ p \equiv 1 \pmod{d}} \left(\frac{g}{p}\right) d,
\]
where \((\frac{g}{p})_d\) denotes the \(d\)-th power residue symbol, cf. Lemmermeyer [291, p. 111].

In case \(g\) is squarefree these terms are \(o(S_1(x))\) for every \(d > 2\) and \(\delta\). Hence we expect that
\[
\mathcal{P}(g)(x) \sim (S_1(x) + S_2(x)) \sim 2 \sum_{\substack{p \leq x, \ (p-1,h) = 1 \ (\frac{g}{p}) = -1}} \frac{\varphi(p-1)}{p-1}, \ x \to \infty.
\]
A slightly more complicated argument leads to the conjecture
\[
\mathcal{P}(g)(x) \sim 2 \sum_{\substack{p \leq x, \ (p-1,h) = 1 \ (\frac{g}{p}) = -1}} \frac{\varphi(p-1)}{p-1}, \ x \to \infty,
\]
where \(g\) is not required to be squarefree. The problem in proving this (and hence a quantitative Artin’s primitive root conjecture) is that we have ‘too many error terms’ and can only achieve this if it can be established that there is sufficient cancellation, which is presently out of reach.

The analog of the latter conjecture for the general index \(t\) case (cf. §9.7.3) is far from easy to infer by ad hoc methods (as we managed to do for \(t = 1\) in the previous section), but can be merely computed using the approach sketched here. Furthermore, under the usual RH proviso this conjecture can then be shown to be true [340, Theorem 1]. A rather easier proof of this result is given in [342].

The unconditional results on Artin’s conjecture on average in [179, 466], were obtained on using the indicator function and estimates for character sums.

8.2. The indicator function in the function field setting. We now give another application of the identity [18]. Let \(\mathbb{F}_q\) be the finite field with \(q = p^n\) elements. Recall that its multiplicative group is cyclic. Let \(a(x)\) be a polynomial in the polynomial ring \(\mathbb{F}_p[x]\). We are interested in the number of irreducible polynomials \(p(x) \in \mathbb{F}_p[x]\) such that \(a(x)\) generates \((\mathbb{F}_p[x]/(p(x)))^*\). Recall that if \(p(x)\) is of degree \(n\), then \(\mathbb{F}_p[x]/(p(x))\) is isomorphic with \(\mathbb{F}_{p^n}\), where the isomorphism is given explicitly as follows: for \(h(x) \in \mathbb{F}_p[x]\), we write, using the Euclidean algorithm,
\[
h(x) = p(x)q(x) + r(x), \text{ with either } r(x) = 0 \text{ or } 0 \leq \deg r < \deg p = n.
\]
Let \(\rho \in \mathbb{F}_{p^n}\) be a root of \(p(x)\). Then
\[
h(\rho) = r(\rho) = a_0 + a_1\rho + \ldots + a_{n-1}\rho^{n-1}, \ a_i \in \mathbb{F}_p
\]
describes all the elements of \(\mathbb{F}_{p^n}\). Thus, \(a(x)\) generating \((\mathbb{F}_p[x]/(p(x)))^*\) is equivalent to \(a(\rho)\) generating \(\mathbb{F}_{p^n}\).

Hence, to count the number of irreducible \(p(x)\) of degree \(n\) for which \(a(x)\) is a generator is tantamount to counting the number of \(\rho\) of degree \(n\) for which \(a(\rho)\) generates \(\mathbb{F}_{p^n}\). Indeed, since each \(p(x)\) has \(n\) roots, we find that the number of
irreducible polynomials of degree $n$ in $\mathbb{F}_p[x]$ such that $a(x)$ generates $(\mathbb{F}_p[x]/(p(x)))^*$ is equal to the number of elements $\rho \in \mathbb{F}_p^n$ of degree $n$ such that $a(\rho)$ generates $\mathbb{F}_p^*$ divided by $n$. The latter number is by (18) equal to

$$\frac{1}{n} \sum_{\rho \in \mathbb{F}_p^n \atop \deg \rho = n} \frac{\varphi(p^n - 1)}{p^n - 1} \sum_{d | p^n - 1} \mu(d) \sum_{\ord \chi = d} \chi(a(\rho)).$$

By inclusion-exclusion we find that the number of irreducible polynomials of degree $n$ over $\mathbb{F}_q[x]$ equals

$$\frac{1}{n} \sum_{\rho \in \mathbb{F}_q^n \atop \deg \rho = n} 1 = \frac{1}{n} \sum_{d | n} \mu(d) p_n^d = p_n^n + O\left(\frac{p_n^2}{n}\right).$$

(For $t \geq 2$ we have $\sum_{d | n} \mu(d) t^{n/d} > t^n - \sum_{j=0}^{[n/2]} t^j > 0$ and hence that at least one irreducible polynomial of degree $n$ over $\mathbb{F}_q[x]$ exists.) Thus the contribution from the main term (the term with $d = 1$) is

$$\frac{p_n^n + O(p_n^2) \varphi(p_n - 1)}{p_n^n - 1},$$

and the error term is

$$\frac{\varphi(p_n - 1)}{n(p_n - 1)} \sum_{d | p_n - 1} \mu(d) \sum_{\ord \chi = d} \sum_{\rho \in \mathbb{F}_p^n} \chi(a(\rho)).$$

Applying Weil’s estimate for character sums and imposing the appropriate conditions on $a(x)$, the truth of Artin’s conjecture in this situation is then established, cf. Pappalardi and Shparlinski [406].

A little knowledge of the history of Weil’s estimate makes clear that we do not always need to invoke this powerful and deep result. Weil, in a period when he felt depressed, turned to the works of Gauss and started reading haphazardly. He soon found himself awestruck by Gauss’ approach in counting solutions mod $p$ of homogenous equations of the form $x_0^m + \ldots + x_s^m$. This approach involves Gauss sums (and Jacobi sums). Weil then started musing about generalisations of this beautiful work and the rest is mathematical history.... Thus we would expect that in case $a(x) = x^m + c$ the required estimate for the error term can be obtained using only Gauss sums over finite fields. This is indeed so, see Jensen and Ram Murty [246].

The situation described here is a particular case of the Artin primitive root conjecture for function fields. Hasse, who was at the cradle of Artin’s conjecture (Artin first formulated it in a discussion with Hasse), remained very interested in it throughout his life and tried to stimulate people to work on it, cf. [216]. One of them was his PhD student Bilharz [39], who in 1937 proved Artin’s conjecture for function fields assuming the RH for the zeta function corresponding to the function field. Indeed, much later this was proved by Weil and hence Artin’s primitive root conjecture is true for function fields! The result of Bilharz has been subsequently generalized by Hsu [240] toCarlitz modules, a particular case of rank one Drinfeld modules, and
in a subsequent paper to rank one Drinfeld modules \[242\]. (In the latter case the
authors work with an \(A\)-field \(K\) having an injective homomorphism \(\gamma: A \to K\), in
a more recent paper \[504\] the case where \(\gamma\) is not-injective is addressed.) Chen et
al. \[71\] generalized Bilharz’s theorem to all one-dimensional tori over global function
fields having a finite constant field. Rosen in his well-written book \[435\] devotes a
whole chapter to the Artin primitive root conjecture in the function field setting.

9. Some variations of Artin’s problem

9.1. Elliptic Artin (by A.C. Cojocaru). Artin’s problem is pertinent to many gen-
eralizations and variations. A natural generalization appears in the context of elliptic
curves and was formulated by S. Lang and H. Trotter in 1976 \[283\], as follows.

Let \(E/\mathbb{Q}\) be an elliptic curve defined over \(\mathbb{Q}\) and with arithmetic rank \(\geq 1\). Let \(a \in E(\mathbb{Q})\) be a point of infinite order. For a prime \(p\) of good reduction for \(E\), let \(\overline{E}/\mathbb{F}_p\) be the reduction of \(E\) modulo \(p\) and \(\overline{a}\) the reduction of \(a\) modulo \(p\). Here, we are also excluding the primes dividing the denominators of the coordinates of \(a\). Following standard notation, we let \(|E(\mathbb{F}_p)| = p + 1 - a_p\) denote the number of \(\mathbb{F}_p\)-
rational points of \(E\). The elliptic curve analogue of Artin’s problem is to determine
the density of the primes \(p\) for which

\[
\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle.
\]
In this case, we say that \(a\) is a primitive point of \(E\) modulo \(p\). In 1976, Lang and
Trotter conjectured that this density exists; moreover, they conjectured that there
exists a constant \(C_E(a) \geq 0\), depending on \(E\) and \(a\) such that as \(x \to \infty\),

\[
\#\{p \leq x : \overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle\} \sim C_E(a) \frac{x}{\log x}.
\]

In most cases, this is still an open question. The only result known is due to Rajiv
Gupta and Ram Murty \[203\] who proved that if \(E/\mathbb{Q}\) has Complex Multiplication
(CM) by the full ring of integers of an imaginary quadratic field \(K\), then under
GRH,

\[
\#\{p \leq x : a_p \neq 0, \overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle\} = C_E(a)\pi(x) + O\left(\frac{x \log \log x}{(\log x)^2}\right).
\]

Additionally, they proved that if 2 and 3 are inert in \(K\), or \(K = \mathbb{Q}(\sqrt{-11})\), then
\(C_E(a) > 0\); therefore, under GRH, as \(x \to \infty\),

\[
\#\{p \leq x : a_p \neq 0, \overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle\} \gg \frac{x}{\log x}.
\]

The method used by Gupta and Ram Murty is an elliptic curve adaptation of
Hooley’s method. It requires the assumption of GRH, even though it treats the
case of an elliptic curve with CM, which in many instances allows for unconditional
results. This attests to the difficulty of the elliptic curve analogue of Artin’s primitive
root conjecture. No results are known in the case that \(E/\mathbb{Q}\) is without CM.

It is a remarkable piece of history that the above result of Gupta and Ram Murty
led to the current best result on the original Artin primitive root conjecture. Indeed,
in their paper, Gupta and Ram Murty also considered variations of the elliptic curve
analogue of Artin’s problem: instead of working with only one point \( a \in E(\mathbb{Q}) \) of infinite order, they also worked with a free subgroup \( \Gamma \leq E(\mathbb{Q}) \) of rank \( > 1 \) and considered the question of counting the primes \( p \leq x \) for which \( E(\mathbb{F}_p) = \langle \Gamma(\mod p) \rangle \). Subsequently, they considered a similar variation of the classical Artin problem which led to the important results by Gupta and Ram Murty [202] and by Heath-Brown [222].

Another interesting feature of the elliptic curve analogue of Artin’s problem is that, in contrast with the classical situation for which the group \( \mathbb{F}_p^* \) is always cyclic, when we require that \( E(\mathbb{F}_p) = \langle a \rangle \) we are making two assumptions: first, \( E(\mathbb{F}_p) \) is cyclic, and second, it is generated by \( a \).

In general, \( E(\mathbb{F}_p) \) is the product of two cyclic groups. Therefore it is natural to consider the first question of finding the density of primes \( p \) for which \( E(\mathbb{F}_p) \) is cyclic.

This question was first studied by Borosh, Moreno and Porta [11] who conjectured that there are infinitely many such primes. A few years later [153] Serre proved this conjecture under GRH, by using an elliptic curve analogue of Hooley’s method. More precisely, by considering the field extensions \( \mathbb{Q}(E[k]) \) obtained by adjoining to \( \mathbb{Q} \) the \( x \) and \( y \) coordinates of the \( k \)-division points of \( E \), he showed that under GRH,

\[
\#\{ p \leq x : E(\mathbb{F}_p) \text{ is cyclic} \} = C_E \pi(x) + O \left( \frac{x \log \log x}{(\log x)^2} \right),
\]

where

\[
C_E = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]}.
\]

In the case that \( E \) is with CM, this result was made unconditional by Ram Murty [372], and later using a new simpler proof by A.C. Cojocaru [105]. Ram Murty did not provide an error term, Cojocaru provided the error term \( O(x/(\log x \log \log x)) \).

Recently this error term has been considerably sharpened by A. Akbary and Kumar Murty [8]. In the case that \( E \) is without CM, the GRH assumption was relaxed to a ‘quasi 3/4-GRH’ assumption by A.C. Cojocaru [103]. Unconditionally, it is known by Rajiv Gupta and Ram Murty [204] that, for any elliptic curve \( E/\mathbb{Q} \) with \( \mathbb{Q}(E[2]) \neq \mathbb{Q} \), the number of primes \( p \leq x \) such that \( E(\mathbb{F}_p) \) is cyclic is bounded from below by a constant times \( x/(\log x)^2 \). Thus, unconditionally, for any such \( E/\mathbb{Q} \), there are infinitely many primes \( p \) for which \( E(\mathbb{F}_p) \) is cyclic.

Recently, work of Banks and Shparlinski [37], combined with work of N. Jones [247], shows that, on average over a sufficiently large two-parameter family of elliptic curves \( E \) over \( \mathbb{Q} \), the cyclicity asymptotic formula \( \#\{ p \leq x : E(\mathbb{F}_p) \text{ is cyclic} \} \sim C_E \pi(x) \) holds without any additional hypothesis. However, such an average result does not imply that the formula holds for any curve \( E \).

The division fields \( \mathbb{Q}(E[k]) \) are natural generalizations of the cyclotomic fields \( \mathbb{Q}(\zeta_k) \), hence it is natural to expect that Hooley’s method (which requires the use of the Kummer extensions \( \mathbb{Q}(\zeta_k, a^{1/k}) \)) would be amenable to generalization to elliptic curves. However, the non-abelian nature and the size of the extensions \( \mathbb{Q}(E[k])/\mathbb{Q} \) lead to many obstacles in the elliptic curve case that cannot be overcome as in the classical case. For a nice exposition of such difficulties (such as Brun-Titchmarsh
type results for $\mathbb{Q}(E[k])/\mathbb{Q}$ put in the context of elliptic analogues of other classical analytic problems, the reader is referred to Kowalski [267].

For the Lang-Trotter conjecture on primitive points, the fields $\mathbb{Q}(E[k], k^{-1}a)$ that occur are direct generalizations of $\mathbb{Q}(\zeta_k, a^{1/k})$. In this case, the additional complications which arise because of the large size of the conjugacy classes involved could be overcome only if $E$ is with CM, under GRH. This is the content of the work by Gupta and Ram Murty mentioned above [203].

The positivity of the cyclicity constant $C_E$ was explained by Serre in [453] and proved rigorously by Cojocaru and Ram Murty in [110]: $C_E > 0$ iff $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. In [110], Cojocaru and Ram Murty also show that the asymptotic formula (19) can be proven with substantially better remainder terms: $O\left(x^{5/6}(\log x)^{2/3}\right)$ in the non-CM case and $O\left(x^{3/4}(\log x)^{1/2}\right)$ in the CM case, provided that the full strength of GRH holds. These results, together with the aforementioned ones, suggest that there is an important divergence between the cyclicity conjecture for elliptic curves and the Artin primitive root conjecture, as the latter does not seem to be amenable to all the approaches of the first one.

Similar problems have been considered in the context of elliptic curves over $\mathbb{F}_q[T]$ in works by Clark and Kuwata [87], Cojocaru and Tóth [111], and Hall and Voloch [211].

A different but related problem was also considered by Chen and Ju in [73]. Given an elliptic curve $E$ over a finite field $\mathbb{F}_p$, they considered the finite field extension $\mathbb{F}_p(E[l])$ obtained by adjoining the $l$-division points of $E$ to $\mathbb{F}_p$ with $l$ a prime, which has degree $\leq l^2 - 1$. Chen and Ju investigated how often this degree is actually equal to $l^2 - 1$. Under GRH they showed that when $E$ is not supersingular over $\mathbb{F}_p$, the set of primes $l$ for which $[\mathbb{F}_p(E[l]): \mathbb{F}_p] = l^2 - 1$ has a positive density which can be given explicitly in terms of

$$C_2 = \frac{1}{4} \prod_{q > 2} \left(1 - \frac{2}{q(q-1)}\right) = 0.133776753154159683 \ldots,$$

where the product is over the odd primes $p$. They reduce this problem to a variation of the Artin primitive root conjecture, which subsequently can be dealt with by the methods of Hooley [238].

We leave it as an exercise for the reader to show that $C_2 = T/\pi^2$, with

$$T = 2 \prod_{q > 2} \left(1 - \frac{1}{(q-1)^2}\right),$$

the twin prime constant.

9.2. Even order. Let $g \geq 2$ be an integer. As we saw in the introduction, for a prime $p$, the period of the decimal expansion of $1/p$ in base $g$ is maximal iff $\text{ord}_p(g) = p-1$. In 1969 Krishnamurty [268] wondered how often the period in these decimal expansions are even. This can be studied by algebraic methods similar to those sketched above.

We say that a prime $p$ divides a sequence of integers, if it divides at least one
non-zero term of the sequence. Notice that

\[ \text{ord}_p(g) \text{ is even } \iff g^x \equiv -1 \pmod{p} \text{ has a solution } \iff p|\{g^k + 1\}^\infty_{k=0}. \]

There is a unique \( j \geq 1 \) such that \( p \equiv 1 + 2^j (\mod 2^{j+1}) \). Now \( \text{ord}_p(g) \) is even iff

\[ g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}. \]

It is more natural to consider the primes \( p \) such that \( \text{ord}_p(g) \) is odd, that is the set \( \{ p : 2 \nmid \text{ord}_p(g) \} \). Let

\[ P_j = \{ p : p \equiv 1 + 2^j (\mod 2^{j+1}), \ 2 \nmid \text{ord}_p(g) \}. \]

Now \( P_j \) consists of the primes \( p \) that split completely in \( \mathbb{Q}(\zeta_{2^j}, g^{1/2^j}) \) but do not split completely in \( \mathbb{Q}(\zeta_{2^{j+1}}, g^{1/2^j}) \). Since \( \{ p : 2 \nmid \text{ord}_p(g) \} = \bigcup_{j=1}^\infty P_j \), and the \( P_j \) are disjoint, one expects that the natural density of the set \( \{ p : 2 \nmid \text{ord}_p(g) \} \) equals \( \sum_{j=1}^\infty \delta(P_j) \), where \( \delta(P_j) = \lim_{x \to \infty} \frac{P_j(x)}{\pi(x)} \). Now

\[ \sum_{j=1}^\infty \delta(P_j) = \sum_{j=1}^\infty \left( \frac{1}{[\mathbb{Q}(\zeta_{2^j}, g^{1/2^j}) : \mathbb{Q}]} - \frac{1}{[\mathbb{Q}(\zeta_{2^{j+1}}, g^{1/2^j}) : \mathbb{Q}]} \right). \]

Taking \( g = 2 \) one expects by computing the field degrees involved that the density of prime divisors of the sequence \( \{2^k + 1\}^\infty_{k=0} \) equals

\[ \delta = \left( \frac{1}{2} - \frac{1}{4} \right) + \left( \frac{1}{8} - \frac{1}{8} \right) + \sum_{j \geq 3} \left( \frac{4}{4^j} - \frac{2}{4^j} \right) = \frac{7}{24}. \]

With natural density replaced by Dirichlet density, this result had been proved in 1966 by Hasse [219]. Earlier, involving fewer technical complications, he had considered the Dirichlet density of primes \( p \) such that an odd prime \( l \) divides \( \text{ord}_p(a) \) [218]. The natural density of primitive divisors of sequences of the form \( \{a^k + b^k\}^\infty_{k=1} \) with \( a \) and \( b \) integers was computed independently along similar lines by Ballot [27], Odoni [395] and Wiertelak [495]. For the sequence \( \{a^k + b^k\}^\infty_{k=1} \) with \( a \) and \( b \) canonical, the density is 2/3. In particular if \( g = 10 \), one finds that the primes \( p \) such that the period of the decimal expansion of \( 1/p \) is even have density 2/3.

Note that this result, unlike Hooley’s, is unconditional. Both involve infinite towers of field extensions, but the one appearing in this problem is so sparse (in the sense that the degrees of the fields quickly increase) that the profusion of error terms that occur in the Artin primitive root conjecture does not arise and one can afford working with the relatively large error terms in \( \pi_K(x) \) that are conditionally known. A probabilistic model for \( \text{ord}_p(g) \) to be even was found by Moree [351]. For a related heuristic approach see Ballot [31].

Early authors working on divisors of sequences of the form \( \{a^k + b^k\}^\infty_{k=1} \) were interested in showing that primes in certain arithmetic progressions occur either all as divisors or non-divisors, see, e.g., [17] [444] [462]. Fermat was also interested in this and made some false claims in one of his letters to Mersenne [362] [444]. Moree and Sury [362] computed the density of primes \( p \) such that \( p \equiv c \pmod{d} \) and \( p|a^k + b^k \).
for some \( k \geq 1 \) in case both \( a \) and \( b \) are positive integers.

Midy (see Leavitt [286]) proved in 1836 that if \( 1/p \) has even period \( 2d \) (that is, \( \text{ord}_p(10) \) is even), then writing

\[
\frac{1}{p} = 0.(UV)(UV)\ldots,
\]

where \( U, V \) are blocks of \( d \) digits each, one has \( U + V = 10^d - 1 \). Example: \( 10^3 \equiv -1 \pmod{7} \), \( \frac{1}{7} = 0.142857142857\ldots \), and \( 142 + 857 = 999 \). The result of Midy was generalized by Gupta and Sury [201] to the case where the period is \( ld \), for some recent results in this direction see Lewittes [299] and H.W. Martin [322].

Instead of asking when \( 2 \mid \text{ord}_p(g) \), one can ask for \( m \mid \text{ord}_p(g) \) or for \( (m, \text{ord}_p(g)) = 1 \) an so forth. These questions with sharp error terms are dealt with in various papers of Wiertelak [496, 497, 498, 499, 500]. Again it turns out the corresponding density exists and is a rational number. Wiertelak [497] gave a complicated expression for this density for the ‘\( m \mid \text{ord}_p(g) \)’ problem that was substantially simplified by Pappalardi [403]. Pappalardi’s expression was simplified by Moree [345], who based himself on a simple to prove, yet previously unknown, identity for the associated counting function ([345, Proposition 1]). For a number field generalization of some of these results see Perucca [413].

### 9.3. Order in a prescribed arithmetic progression

The problem of determining for how many primes \( p \leq x \) one has \( \text{ord}_p(g) \equiv a \pmod{d} \), with \( a \) and \( d \) prescribed integers, was first considered by Chinen and Murata [76] in case \( d = 4 \). By a different method their results for \( d = 4 \) are reproved in Moree [346] for more general \( g \). This gives also a rather more compact formulation of their results. In the same paper also the case \( d = 3 \) was dealt with.

In this generality the problem turns out to be much harder than the case where \( d \mid a \). Under an appropriate generalization of RH it turns out that \( \delta_g(a, d) \), the density of primes \( p \leq x \) such that \( \text{ord}_p(g) \equiv a \pmod{d} \) exists (see Chinen and Murata [77] in case \( d \) is a prime power, [78, 347] in the general case). Let \( N_g(a, d)(x) \) be the associated counting function. The proof of the existence of \( \delta_g(a, d) \) by Moree [346] starts with noting the identity

\[
N_g(a, d)(x) = \sum_{t=1}^{\infty} \# \{ p \leq x : r_p(g) = t, \ p \equiv 1 + ta \pmod{dt} \},
\]

where \( r_p(g) = (p - 1)/\text{ord}_p(g) \) denotes the residual index. The individual terms can be dealt with by a variation of Hooley’s method, where now one also needs to keep track of the dependence on \( t \). The more novel aspects of the work rest in making the resulting formula for \( \delta_g(a, d) \) more explicit, which requires algebraic number theory. Chinen and Murata [78] express \( \delta_g(a, d) \) as a six fold sum, in [346] it is expressed as a double sum, Ziegler [512] generalized the author’s approach to \( N_g(a, d)(x) \) to the case where instead of primes one considers prime ideals, see Problem 10 below for more details.

The much simpler quantity \( \delta(a, d) \), the average density of elements of order
≡ a(mod d) in a field of prime characteristic also exists \[343\]. It turns out that under the latter RH variant for almost all g with \(|g| \leq x\) one has \(\delta_g(a,d) = \delta(a,d)\). Moreover, if \(\delta_g(a,d) \neq \delta(a,d)\), then \(|\delta_g(a,d) - \delta(a,d)|\) tends to be small. Nevertheless, it is possible to find specific g (usually appropriately chosen high powers of a small basis number), for which \(\delta_g(a,d)\) shows highly non-canonical behaviour. For precise formulations and proofs see \[348\].

Despite the subtle arithmetic behaviour of \(\delta_g(a,d)\), there are some surprises. For example, if \(g > 0\) then always \(\delta_g(1,4) \leq \delta_g(3,4)\). The rule of thumb that a rational density in an Artin type problem indicates that the associated tower of field extension is rather sparse, seems to be incorrect in this context.

The analogous problem of determining for how many primes \(p \leq x\) the residual index is in a prescribed congruence class modulo \(d\) was first studied by Pappalardi \[399\]. This turns out to be a much easier problem.

For a more detailed survey of the material in this section, see Moree \[349\]. The main results in \[346, 347\] are also obtained in papers by Chinen and Murata \[76, 77, 78\] by different methods (the comparison of \(\delta_g(a,d)\) with \(\delta(a,d)\) which is the theme of Moree \[348\], has not (yet) been considered by Chinen and Murata).

9.4. Divisors of second order recurrences. The sequences \(\{a^k + b^k\}_{k=1}^{\infty}\) are special cases of sequences satisfying a second order linear recurrence and one can wonder about prime divisors of such recurrences in general, cf. Ballot \[27\], or about divisors in general. A good general comprehensive survey on results on recurrences can be found in the book \[151\]. A lot of information on second order recurrences can also be found in the book by Ribenboim \[429\].

A general linear second order recurrence \(R\) has the form \(u_{n+2} = eu_{n+1} + fu_n\), with \(ef \neq 0\). Once the values of \(u_0\) and \(u_1\) are given, it is uniquely determined. The characteristic polynomial associated to the recurrence is defined as \(f(X) = X^2 - eX - f\). Stevenhagen \[469\] shows that the set of prime divisors, \(\pi_R\), of \(R\) is most conveniently described in terms of two parameters: the root quotient \(r\) of the characteristic polynomial and the initial quotient \(q\) of the sequence. In this characterization the integer sequence \(R\) no longer plays a role. It greatly clarifies the group structure introduced by Laxton \[284, 285\] on the set of equivalence classes of sequences satisfying a given second order recurrence. Stevenhagen introduces the notion of an equivalence class \([q,r]\) of a second order recurrence with root quotient \(r \neq \pm 1\) and a sequence group \(S(r)\).

9.4.1. Prime divisors of torsion second order recurrences. A second order recurrence with root quotient \(r\) and initial quotient \(q\) is said to be torsion if \([q,r]\) is an element of finite order in \(S(r)\). For example, the sequences \(\{a^k + b^k\}_{k=1}^{\infty}\) are torsion. Another case occurs when \(K\) is a quadratic number field, \(\epsilon\) its fundamental unit, \(\tilde{\epsilon}\) its conjugate, and \(L_n = \epsilon^n + \tilde{\epsilon}^n\) (this is a generalized Lucas sequence). Stevenhagen proved that a second order torsion sequence has a density of prime divisors that is positive and rational. In the case of \(L_n\) above the result is due to Moree and Stevenhagen \[358\], who extended a result of Moree \[333\], who on his turn generalized Lagarias’
result that the sequence of Lucas numbers $L_n$ (defined by $L_0 = 2$, $L_1 = 1$ and $L_{n+1} = L_n + L_{n-1}$) has natural density $2/3$.

9.4.2. Prime divisors of non-torsion second order recurrences. If the characteristic polynomial of the recurrence is reducible over $\mathbb{Q}$, then the recurrence has the form $R = \{ca^k - db^k\}_{k=0}^\infty$, and finding the prime divisors amounts to finding the prime divisors of the sequence with general term $(a/b)^k - d/c = \alpha^k - \beta$. Now $p$ is a prime divisor of $R$, with at most finitely many exceptions, iff $\text{ord}_p(\beta)|\text{ord}_p(\alpha)$. This can be phrased differently by saying that, with at most finitely many exceptions, $p$ divides $R$ iff the subgroup mod $p$ generated by $\beta$, $\langle \beta \rangle$, is contained in the subgroup $\langle \alpha \rangle$. One can then base a two variable Artin conjecture on this, of which the qualitative form says that the sequence $R$ should have infinitely many prime divisors. This is not difficult to prove, see Pólya [423]. (Schinzel [445, pp. 909-911] proved that if $a$ and $b$ are rational integers with $a > 0$ and $b \neq a$, then there are infinitely many primes $p$ that do not divide the sequence $\{a^k - b\}_{k=1}^\infty$.) To investigate the quantitative form, we put $S(x) = \sum_{p \leq x, p|R} 1$. Then

$$S(x) = \sum_{p \leq x} \sum_{\text{ord}_p(\beta)|\text{ord}_p(\alpha) = (p-1)/w} 1 = \sum_{w \leq x-1} \sum_{p \leq x \text{ (mod w)}} 1.$$

Now $p \equiv 1(\text{mod w})$ and $\text{ord}_p(\beta)|\text{ord}_p(\alpha) = (p-1)/w$ iff $p$ splits completely in $\mathbb{Q}(\alpha^{1/w}, \beta^{1/w}, \zeta_w)$ and $p$ does not split completely in any of the fields $\mathbb{Q}(\alpha^{1/w}, \beta^{1/w}, \zeta_{qw})$ with $q$ a prime. Denote the degree of the latter field by $n(qw)$. Then, as $x \to \infty$, the limit $S(x)/\pi(x)$ tends to

$$\sum_{w=1}^\infty \sum_{k=1}^\infty \frac{\mu(k)}{n(kw)},$$

provided a sufficiently strong generalisation of RH is true. The sum (20) equals a rational number times the Stephens constant

$$S = \prod_q \left(1 - \frac{q}{q^3 - 1}\right) = 0.5759599688929\ldots$$

This result is due to Moree and Stevenhagen [359] and improves on earlier work by Stephens [467]. Stephens evaluation of (20) (who restricted himself to the case where both $\alpha$ and $\beta$ are integers) is not always correct and was corrected in [359]. Using the average-character-sum method [296], a rather easier reproof can be given [361]. The Stephens constant, just like $A$, can also be evaluated with high numerical precision by expressing it in terms of zeta values at integer arguments [341].

A naive heuristic argument would lead us to expect that the density equals the average density (over the primes) of pairs $(u, v) \in F_p^* \times F_p^*$ such that $u \in \langle v \rangle$. It is not difficult to see that the density of the pairs $(u, v) \in F_p^* \times F_p^*$ such that $u \in \langle v \rangle$ equals

$$\frac{1}{(p-1)^2} \sum_{d|p-1} d \varphi(d).$$
Thus the naive heuristic would give
\[
\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{1 < p \leq x} \frac{1}{(p - 1)^2} \sum_{d|p-1} \varphi(d)
\]
as density. The above limit was evaluated by Luca [312] to be the Stephens constant, thus answering an open problem in von zur Gathen et al. [172]. Luca’s proof is quite similar to the evaluation of \(\sum_{p \leq x} \varphi(p-1)/(p-1)\) given in \(\S7\). Another interpretation of Stephens’ constant, see Korolev [266], is as the average value of
\[
\frac{1}{\varphi(n)} \sum_{\substack{k=1 \\ (k,n)=1}}^{n} \frac{1}{(k-1,n)}.
\]

Note that the problem considered here is a variant of Artin’s primitive root conjecture that is more complicated than the original one, whereas the variant discussed in \([9.2]\) is easier, although both deal with second order recurrences. The variants discussed in \([9.2]\) are torsion sequences. For every torsion sequence the prime density exists and is a rational number. It can be explicitly determined. Here the case when the characteristic polynomial is reducible over \(\mathbb{Q}\) is easier, than when it is irreducible. For a non-torsion sequence assuming GRH the density can be shown to exist and also be explicitly determined. Here again the case where the characteristic polynomial is irreducible is the most difficult. An example is given by the sequence \(a_n\) defined by \(a_0 = 3\), \(a_1 = 1\) and \(a_{n+1} = a_n + a_{n-1}\). Lagarias [276] raised the challenge here of determining the density of prime divisors. Moree and Stevenhagen [360] showed that under an appropriate generalisation of RH this density equals
\[
\frac{1573727}{1569610} S = 0.577470679956 \ldots
\]
Indeed, for every non-torsion sequence assuming GRH the density exists, can be explicitly evaluated and is a rational multiple of the Stephens’ constant \(S\).

For the convenience of the reader we give some references for the various cases:
- Torsion, reducible char. polynomial: [27, 218, 219, 395, 495]
- Torsion, irreducible char. polynomial: [276, 333, 358, 469]
- Non-torsion, reducible: [467, 359]
- Non-torsion, irreducible: [360].

Recently in addition to the techniques used in the above articles, also the theory of dynamical systems has been brought to bear on the issue of prime divisors of sequences, see, e.g., [186, 248, 249].

9.4.3. General divisors. One can also try to count the number of divisors \(\leq x\) of a given sequence. In case the sequence is \(S_{p,1}\), where \(S_{a,b}\) denotes the sequence \(\{a^k + b^k\}_{k=1}^{\infty}\), this plays a role in the analysis of the average behaviour of Ulmer’s rank formula, see [425]. The divisor counting problem also has some applications outside number theory. For example, Pless et al. [421] Theorem 3] have shown that a nontrivial cyclic self-dual code of length \(n\) exists iff \(n\) does not divide the sequence \(S_{2,1}\). Kanwar and López-Permouth [252] Theorem 4.5] proved that if \(p\) is a prime
not dividing \( n \) and \( m \) is even, then nontrivial self-dual cyclic \( \mathbb{Z}_p^m \)-codes exist iff \( n \) does not divide \( S_{p,1} \).

In Moree \[421\] it is shown that for any \( 0 < \epsilon \leq 1/24 \) and \( r \) the smallest integer such that \( \frac{1}{2}(1/2^{r+3}) \leq \epsilon \), there exist positive constants \( c_1, \ldots, c_r \) such that \( G(x) \), the number of divisors \( n \) of the sequence \( S_{2,1} \) that are \( \leq x \), satisfies

\[
G(x) = \frac{x}{\log x} \left( c_1 \log 1/3 x + c_2 \log^{7/24} x + \sum_{k=0}^r c_{3+k} \log^{2-(k-3)/3} x + O(\log^\epsilon x) \right).
\]

Similar results for divisors of the sequence \( S_{a,b} \), with \( a \) and \( b \) integers are derived in Moree \[335\], and for Lucas numbers in Moree \[337\].

The divisibility of certain sequences is related to the level (Stufe) of a field \( F \), \( s(F) \), which is the smallest integer \( s \) (if it exists) such that \( -1 = \alpha_1^2 + \cdots + \alpha_s^2 \) with \( \alpha_i \) in \( F \). In case \(-1\) cannot be written as a sum of squares from \( K \) we put \( s(K) = \infty \). Pfister \[417\] (cf. \[198, pp. 203-208\]) proved that in case \( s(F) \) is finite we have \( s(F) = 2^j \) for some \( j \geq 0 \). Hilbert (cf. \[279\], XI, Theorem 1.4) proved that if \( F \) is an algebraic number field, then \( s(F) \leq 4 \). It follows that \( s(F) \in \{1, 2, 4\} \) in this case. Note that \( s(F) = 1 \) iff \( \sqrt{-1} \in F \).

Let us put \( K_n = \mathbb{Q}(\zeta_n) \). If \( 4|n \), then \( s(K_n) = 1 \). If \( n \) is odd, then clearly \( s(K_{2n}) = s(K_n) \) since \( K_n = K_{2n} \). Thus we may assume that \( n \) is odd. P. Chowla \[80\] proved that \( s(K_p) = 2 \) when \( p \equiv 3(\text{mod } 8) \) is a prime. In later unpublished papers John H. Smith and P. Chowla proved independently that \( s(K_p) = 2 \) also when \( p \equiv 5(\text{mod } 8) \). In 1970, P. Chowla and S. Chowla \[81\] proved that \( s(K_p) = 4 \) when \( p \equiv 7(\text{mod } 8) \). Fein et al. \[153\] proved that for an odd prime \( p \) we have \( s(K_p) = 2 \) iff \( p \mid S_{2,1} \) (and so \( s(K_p) = 4 \) iff \( p \nmid S_{2,1} \)). Apparently unaware of Hasse’s work \[218\], they gave their own proof of the fact that the Dirichlet density of prime divisors of \( S_{2,1} \) is \( 17/24 \). Moree \[335\], Theorem 7] gave an asymptotic for the number of integers \( m \leq x \) such that \( s(K_m) = 4 \).

Recently Nassirou \[389\] considered the level of \( \mathbb{Q}_p(\zeta_n) \) with \( p \) odd, where \( \mathbb{Q}_p \) denotes the \( p \)-adic field. Since \( s(\mathbb{Q}_p) = 1 \) when \( p \equiv 1(\text{mod } 4) \), we may assume that \( p \equiv 3(\text{mod } 4) \). Let \( q \neq p \) be an odd prime. The results of Nassirou imply that \( s(\mathbb{Q}_p(\zeta_q)) = 1 \) iff \( q \mid S_{p,1} \) and \( s(\mathbb{Q}_p(\zeta_q)) = 2 \) iff \( q \nmid S_{p,1} \).

In the above we considered a fixed sequence \( a^k + b^k \). In the context of supersingular Fermat varieties, a reverse problem comes up. Here one fixes an integer \( m \) and asks for the density \( \delta(m) \) of primes \( p \) such that \( m \) divides the sequence \( \{p^k + 1\}_{k=1}^\infty \). For this Yui \[505\] and independently Waterhouse \[492\] gave an explicit formula. It is known that the Jacobian variety of a Fermat curve \( X^m + Y^m = Z^m \) considered in characteristic \( p \), is supersingular (i.e. isogenous to a product of supersingular elliptic curves), iff \( m \) divides the sequence \( \{p^n + 1\}_{n=1}^\infty \), see, e.g., \[457\], \[492\], \[505\]. Using the explicit formula of Yui and Waterhouse, Schwarz and Waterhouse \[452\] gave an asymptotic formula for \( \sum_{2 < m \leq x} \delta(m) \). This was improved on by Nowak \[394\], who proved that for every fixed \( K \) there exist positive constants \( A_0, A_1, \ldots, A_K \) such that,

\[
\sum_{2 < m \leq x} \delta(m) = x \sum_{k=0}^K A_k (\log x)^{2-k/3-1} + O(x(\log x)^{2-K/4-1}),
\]
where the implied constant may depend on the integer $K$ and $x$ tends to infinity. Note the similarity of this formula with that given above for $G(x)$.

9.5. **Lenstra’s work.** The most far reaching generalisation of the Artin primitive root conjecture was considered by Lenstra [292], in the context of his research on Euclidean number fields: Let $K$ be a global field (that is a finite extension of $\mathbb{Q}$ or a function field in one variable over a finite field) and $F$ a finite normal extension of $K$. Let $C$ be a subset of Gal($F/K$) which is stable under conjugation and let $d$ be a positive integer (coprime to the characteristic of $K$ in the case of a function field). Consider a finitely generated subgroup $W$ of $K^*$ which has, modulo torsion, rank $r \geq 1$, and let $M$ be the set of prime ideals $\mathfrak{P}$ of $K$ satisfying

(1) the Artin symbol $(\mathfrak{P}, F/K) \subseteq C$

(2) the normalized exponential valuation attached to $\mathfrak{P}$ satisfies $\text{ord}_{\mathfrak{P}}(w) = 0$ for all $w \in W$.

(3) if $\psi : W \to \overline{K}_{\mathfrak{P}}^*$ is the natural map, then the index of $\psi(W)$ in $\overline{K}_{\mathfrak{P}}^*$ divides $d$.

Here $\overline{K}_{\mathfrak{P}}^*$ denotes the multiplicative group of $\overline{K}_{\mathfrak{P}}$, the residue class field at $\mathfrak{P}$. Lenstra conjectured that $M$ has a density. He also obtained necessary and sufficient conditions for this density to be nonzero under a sufficiently strong generalisation of RH. His main result implies Theorem 1 for example. Lenstra applied his results to show that under the usual RH proviso certain principal ideal rings are Euclidean (see the next section).

9.6. **Artin’s conjecture and Euclidean domains** (written with Hester Graves).

A Euclidean algorithm for an integral domain $R$ is a map $\phi : R \setminus \{0\} \to W$, a well-ordered set, such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with $a = qb + r$ and $\phi(r) < \phi(b)$. From every Euclidean algorithm, one can create another Euclidean algorithm $\phi : R \setminus \{0\} \to W$, a well-ordered set, such that $\phi(0) = 0$ and for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with $a = qb + r$ and $\phi(r) < \phi(b)$ or $r = 0$. We will concern ourselves with this second type of Euclidean algorithm.

Nagata showed that one can replace “$W$, a well-ordered set” with “$W$ an ordered set with minimum condition” in the above definition. He was nonetheless able to show that every such Euclidean algorithm implied the existence of a Euclidean algorithm that mapped to a well-ordered set. In other words, his definition expanded the set of possible Euclidean algorithms, but not the set of possible Euclidean rings.

If an integral domain has a Euclidean algorithm, then all of its ideals are principal. The converse of this is not true in general. Not all principal rings of integers of imaginary quadratic fields are Euclidean. The nine quadratic imaginary number fields with class number one are $\mathbb{Q}(\sqrt{-d})$ with $d = 1, 2, 3, 7, 11, 19, 43, 67$ and $163$; only the rings of integers of $\mathbb{Q}(\sqrt{-d})$ with $d = 1, 2, 3, 7$, or $11$ are Euclidean.

An integral domain $R$ equipped with a Euclidean algorithm is called a Euclidean domain. For algebraic number fields the Euclidean algorithm most often studied is the absolute value of the norm. Such fields and their rings of integers are called norm-Euclidean. The classification of rings of algebraic integers which are Euclidean (not necessarily for the norm function) is a major unsolved problem.
Dedekind showed in Supplement XI to Dirichlet’s *Vorlesungen über Zahlentheorie* [125] that $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean for $d = -11, -7, -3, -2, -1, 2, 3, 5, 13$. Now it’s known that the full list of norm-Euclidean quadratic fields also includes $d = 6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57$ and $73$. Lemmermeyer [290] determined all real cubic norm-Euclidean fields with discriminant less than 4692. Clark [86] gave two examples of cubic fields which are Euclidean but not norm-Euclidean. Further examples were found by Cavallar and Lemmermeyer [68].

Motzkin [363] constructed the so-called minimal Euclidean algorithm. Given a nonempty collection of Euclidean algorithms $\phi_j$ on $R$, the map defined by $\phi(r) = \min_j \phi_j(r)$ is easily seen to also be a Euclidean algorithm on $R$. If the minimum is taken over all the Euclidean algorithms of the ring $R$, the resulting algorithm $\phi$ is called the minimal algorithm. Let $A_0 = \{0\}$, and define $A_j$ for $j \geq 1$ by

$$A_j - A_{j-1} = \{a \in R : \text{each residue class of } R/(a) \text{ contains an element of } A_{j-1}\}.$$  

Note that $A_1 - A_0$ is the set of units of $R$. If

$$R = \bigcup_{j=0}^{\infty} A_j,$$

then $R$ is Euclidean, with $\phi(a) = \min \{j : a \in A_j\}$. Motzkin [363] proved that the condition (21) is also necessary if $R$ is to be Euclidean. As an example, if $R = \mathbb{Z}$, then $A_1 = \{-1, 0, 1\}$. This set consists of three consecutive integers and thus it provides representatives for the classes mod 2 and mod 3, so that $A_2 = \{-3, -2, -1, 0, 1, 2, 3\}$. Here we have 7 consecutive integers so that $A_3$ is the interval $[-7, +7]$ consisting of 15 consecutive integers. It can be easily shown that if $\theta(n)$ denotes the number of binary digits of $|n|$, then the minimal algorithm on $\mathbb{Z}$ is given by $\theta$. Using the sets $A_n$ we can easily see, for example, why $\mathbb{Q}(\sqrt{-19})$ is not Euclidean for any algorithm. This follows because $\pm 1$ are its only units and every non-trivial ideal has norm at least 4 so the construction of the sets $A_n$ stops at $A_1$. If the reader wants to learn more about Euclidean rings, Lenstra [295] wrote an introductory account. Samuel [441] wrote a more advanced survey on Euclidean rings. In this survey, he studied the function $\theta$ defined below in Theorem 6 and noticed that the condition on the value of $n_p$ (defined in order to study $\theta$) was similar to Artin’s conjecture. He may have been the first to notice the connection between Euclidean rings and Artin’s conjecture. In addition, Samuel asked questions that shaped the study of Euclidean rings. For example, he asked whether there were a real quadratic number field such that its ring of integers were Euclidean but not norm-Euclidean; he suggested the ring $\mathbb{Z}[\sqrt{14}]$ as a candidate.

Two years later, assuming GRH, Weinberger [494] was able to use Hooley’s work on Artin’s conjecture in the Euclidean ring situation and established the following result.

**Theorem 4.** (GRH). Let $K$ be an algebraic number field whose ring of integers both is a principal ideal domain and has infinitely many units. Then the ring of integers of $K$ is Euclidean.

At first sight GRH seems to have little to do with the statement of the result. It comes from the fact that the following variant of Artin’s primitive root conjecture
is needed for the proof of Theorem 4 and can presently be only proved assuming GRH.

**Theorem 5. (GRH).** Let $K$ be an algebraic number field whose ring of integers $R$ both is a principal ideal domain and has infinitely many units. Let $\epsilon$ be a fundamental unit of $R$, i.e. $\epsilon \neq \epsilon_1^n$ for all units $\epsilon_1$ and all integers $n > 1$. Let $p$ be a prime ideal of $K$ and let $I$ be the multiplicative group of ideals of $K$ prime to $p$ and let $H = \{a \in I : a \equiv (1) \pmod{p}\}$. Then every ideal class of $I/H$ contains infinitely many prime ideals $q$ for which $\epsilon$ is a primitive root mod $q$, i.e. the class of $\epsilon$ generates the (cyclic) group of units in the finite field $R/q$.

The proof of this result is a variant of Hooley’s proof of the original Artin conjecture.

The proof that Theorem 5 implies Theorem 4 consists of two steps. We first define irreducibility; an element $b$ is irreducible if the ideal $(b)$ is prime. Assuming GRH, one uses Theorem 5 to show that every irreducible of $R$ is in $A_3$. If one chooses an irreducible element $p$, then every ideal class of $I/H$ has infinitely many prime ideals $q = (q)$ such that $(R/q)^* = \langle \epsilon \rangle$. This implies the $q$ are in $A_2$ and therefore, for all $a \in R - (p)$, there exists an irreducible $q \in A_2$ such that $a \equiv q \pmod{p}$. We conclude that $p$ is in $A_3$.

This means that every element of $R - A_1$ can be written as a product of irreducibles in $A_2 - A_1$ and in $A_3 - A_2$. If $n_2$ is the number of these irreducibles in $A_2 - A_1$ and $n_3$ is the number of these irreducibles in $A_3 - A_2$, then we define the height of $b$ to be $\text{ht}(b) = 2n_2 + 3n_3$. One then shows that if $b \in R - A_1$, then $b \in A_{\text{ht}(b)}$. Thus the sets $A_j$ exhaust $R$ and so $R$ is Euclidean.

Let $K$ be a global field, and let $S$ be a non-empty set of prime divisors of $K$ containing the set $S_\infty$ of archimedean prime divisors of $K$. The ring of $S$-integers of $K$ is $R_S = \{x \in K : \nu_p(x) \geq 0 \text{ for all primes } p \not\in S\}$. Lenstra [292] generalized the result of Weinberger above as follows.

**Theorem 6.** Suppose that $R_S$ is a principal ideal ring, and that $\#S \geq 2$. Further, if $K$ is a number field, assume that for every squarefree integer $n$ and every finite subset $S' \subset S$ the Dedekind zeta function $\zeta_K(c_n, R_S^{1/n})(s)$ satisfies the Riemann Hypothesis. Then $R_S$ is Euclidean, and its minimal algorithm $\theta$ is given by

$$\theta(x) = \sum_{p \not\in S} \nu_p(x) n_p \quad (x \in R_S, \ x \neq 0),$$

where the sum is over all primes $p$ of $K$ which are not in $S$ and

$$n_p = \begin{cases} 
1 & \text{if the natural map } R_S^* \to K_p^* \text{ is surjective;} \\
2 & \text{else.}
\end{cases}$$

The function field case of this result is due to Queen [426]. Lenstra also points out that the Euclidean algorithm given by Weinberger is not the minimal one. The assumption $\#S \geq 2$ is only an apparent restriction in the latter result, as in case $\#S = 1$ Lenstra gives the complete list of $R_S$, both for the number and function field situations, that are principal and those that are Euclidean.
Under some further assumptions, the GRH condition is not needed. Gupta, Ram Murty, and Kumar Murty [205] established the following result.

**Theorem 7.** Let $K$ be a number field Galois over $\mathbb{Q}$ and let $g$ be the gcd of the numbers $N_{K,\mathbb{Q}}(\mathfrak{P}) - 1$ for $\mathfrak{P} \in S - S_\infty$. If

(a) $|S| \geq \max(5, 2[K : \mathbb{Q}] - 3)$, and

(b) $K$ has a real embedding or $\zeta_g \in K$,

then the ring of $S$-integers $R_S$ is principal iff it is Euclidean.

The proof combines ideas from a paper by Gupta and Ram Murty on Artin’s conjecture [202] and from a paper of Ram Murty and Kumar Murty [374] on an analogue of the Bombieri-Vinogradov theorem.

Harper and Ram Murty published further results on Euclidean rings that did not assume GRH. In his thesis [214], Harper adapted Motzkin’s construction of the sets $A_j$ defined above in the number field situation. He decided to define $B_0 = \{0 \cup R^*\}$ and $B_i = B_{i-1} \cup \{\text{irreducible elements } p : R^* \rightarrow (R/(p))^*\}$. Using Dirichlet’s theorem on primes in arithmetic progressions, he showed that if $R$ is principal and $\cup B_i$ contains every irreducible element of $R$, then $R$ is Euclidean. He then further refined the sets by augmenting $B_0$ by an ‘admissible set of primes.’ A set of primes $\{\pi_1, \ldots, \pi_s\}$ is called admissible if, for all integers $\beta$ composed of only these primes, every coprime residue class modulo $\beta$ can be represented by a unit. He then used the large sieve to show that if $|\{b \in B_1 : \text{Nm}(b) \leq x\}| \gg \frac{x}{\log^2 x}$, then $\cup B_i$ contains all of the irreducible elements of $R$. In particular, if a real quadratic field has two admissible primes, then its ring of integers is principal iff it is Euclidean. He found two such primes in the ring $\mathbb{Z}[\sqrt{14}]$ and used them to show that $\mathbb{Z}[\sqrt{14}]$ is Euclidean, thereby answering Samuel’s question. He then used the same techniques to show that if the ring of integers of a cyclotomic field, $\mathbb{Z}[\zeta_d]$, is principal, then it is Euclidean.

Harper and Ram Murty [215] generalized this work by proving that if $K$ is a finite Galois extension of $\mathbb{Q}$ with unit rank greater than 3, and if the ring of integers of $K$ is principal, then there exists a large enough set of admissible primes, implying that the ring of integers is a Euclidean domain. The truth of this result assuming GRH was previously established by Weinberger (Theorem 4).

Petersen and Ram Murty extended Ram Murty’s earlier work with Harper by removing the Galois condition in certain cases. They showed that if $K$ is a number field with ring of integers $R$, $\text{rank}(R^*) > 3$ and $M$ is a subfield of $K$ such that $K$ is a Galois extension of $M$ of degree $> 3$, then $R$ is a principal ideal domain iff $R$ is a Euclidean ring [376]. It is worth noting that Petersen and Ram Murty did other work involving Artin’s conjecture. They showed that if $1 \leq a < q$, with $(a,q) = 1$, and if $K$ is a finite Galois extension of $\mathbb{Q}$ such that $\text{rank}(R^*) > 3$ and $\zeta_q \notin K$, then there are infinitely many prime ideals $\mathfrak{p}$ of first degree in $R$ such that $|\text{Nm}(\mathfrak{p})| \equiv a \pmod{q}$ and $R^* \rightarrow (R/\mathfrak{p})^* \not\equiv$ [375]. They used this to show that if $K$ is a finite Galois extension of $\mathbb{Q}$, $\text{rank}(R^*) > 3$ and $\sqrt{-1} \notin K$, then there are infinitely many maximal $h_K$-cusped subgroups of $\text{PSL}_2(R)$ [375]. Previously, Petersen [114] proved such a result for all $K$ with positive unit rank and $\sqrt{-1} \notin K$, assuming the GRH. As all of these subgroups are congruence subgroups, this result is a contrast
to situation when $K$ is $\mathbb{Q}$ or an imaginary quadratic, where there are many maximal
$h_K$-cusped subgroups, but few of these are congruence subgroups. (cf. [416] and
[415]). The geometry is discussed in [375, 414, 415].

Harper’s proof that $\mathbb{Z}[\sqrt{14}]$ is Euclidean, but not norm-Euclidean, answered a
question that had inspired a great deal of mathematical activity. The earliest known
example of a quadratic Euclidean field that is not norm-Euclidean is $\mathbb{Q}(\sqrt{69})$ ([85,
390]). Since Samuel asked the question, much has been done to find a function other
than the norm which makes $\mathbb{Z}[\sqrt{14}]$ Euclidean (see [290]). Nagata was unable to
prove that $\mathbb{Z}[\sqrt{14}]$ is Euclidean. Instead, he introduced the concept of a ‘pairwise
algorithm’ and showed that $\mathbb{Z}[\sqrt{14}]$ has such an algorithm ([382]). Clark and Ram
Murty [88] proved that $\mathbb{Z}[\sqrt{14}, 1/p]$ is Euclidean for $p = 1298852237$. On combining
their techniques with earlier work of Gupta, Ram Murty and Kumar Murty [205],
Harper [214] observed that it can be shown that $\mathbb{Z}[\sqrt{14}, 1/p]$ is Euclidean for any $p$.

In 1995, Lemmermeyer [290] wrote a survey of known results and open questions
on Euclidean and non-Euclidean algebraic number fields. It was updated in 2004,
but in 2007, Narkiewicz proved that there are at most two real quadratic fields such
that their ring of integers is principal but not Euclidean [387]. He also showed that
there is at most one normal cubic number field with class number one that is not
Euclidean. He proved this by combining Harper and Ram Murty’s work with his
earlier results (Narkiewicz [380]) on units in residue classes. There have been no
other major advances in the study of Euclidean rings since then, but there has been
work on Euclidean ideals and Euclidean systems.

In 1979, Lenstra [294] introduced the notion of a Euclidean ideal class which
generalizes that of a Euclidean ring. As the existence of a Euclidean algorithm for a
domain implies trivial class group, the existence of a Euclidean ideal in a Dedekind
domain implies cyclic class group. Lenstra was inspired by norm-Euclidean rings of
integers. Suppose that $K$ is a number field and that $\mathcal{O}_K$ is its ring of integers. Let
Nm denote the field norm. If, for all $a, b \in \mathcal{O}_K$, $b \neq 0$, there exists some $q, r \in \mathcal{O}_K$
such that

$$a = qb + r, \text{ where } r = 0 \text{ or } |\text{Nm}(r)| < |\text{Nm}(b)|,$$

then

$$|\text{Nm} \left( \frac{a}{b} - q \right) | = |\text{Nm} \left( \frac{r}{b} \right) | < 1.$$

In other words, $R$ is norm-Euclidean iff, for all $x \in K$, there exists some $y \in \mathcal{O}_K$
such that

$$|\text{Nm}(x - y)| < 1 = \text{Nm}(R).$$

Lenstra then asked what would happen if $R$ were replaced by some fractional ideal
$C$. If, for all $x \in K$, there exists some $y \in C$ such that

$$|\text{Nm}(x - y)| < |\text{Nm}(C)|,$$

then $C$ is a norm-Euclidean ideal. The only quadratic number fields with a norm-
Euclidean ideal are $\mathbb{Q}(\sqrt{d})$, with $d = -1, -3, -5, -7, -11, -15, -20, 3, 5, 6, 7, 8, 10$
11, 13, 15, 17, 19, 21, 29, 33, 37, 41, 57, 73, and 85 ([294, 195]). Note that only for
$d = -15, -5, 10, 15, \text{ and } 85$, does $\mathbb{Q}(\sqrt{d})$ have a non-principal norm-Euclidean ideal.
As mentioned above, there are rings that are Euclidean but not norm-Euclidean. Lenstra generalized norm-Euclidean ideals as follows. For the rest of the section, we define \( E \) to be the set of all inverses of integral ideals of a Dedekind domain \( R \). Suppose that \( C \) is a fractional ideal of \( R \). If there exists a function \( \psi : E \to W \), \( W \) a well-ordered set, such that for all \( I \in E \) and all \( x \in IC \setminus C \), there exists some \( y \in C \) such that
\[
\psi((x + y)^{-1}IC) < \psi(I).
\]
We say \( \psi \) is a Euclidean algorithm for \( C \) and \( C \) is a Euclidean ideal.

If we define \( \mathbb{I} \) to be the set of all integral ideals of \( R \), we can rewrite this definition. A fractional ideal \( C \) is Euclidean if there exists a function \( \psi : \mathbb{I} \to W \), \( W \) a well-ordered set, such that for all integral ideals \( I \) and all \( x \in I^{-1}C \setminus C \), there exists some \( y \in C \) such that
\[
\psi((x - y)IC^{-1}) < \psi(I).
\]

If \( C \) is a Euclidean ideal, then so is every ideal in its ideal class. If \( C \) is a Euclidean ideal, then its ideal class \([C]\) is called a Euclidean ideal class. One can check that if \( R \) is a Euclidean ring, then \( \mathbb{I} \) is a Euclidean ideal class and \([R]\) is a Euclidean ideal class. If \( C \) is a Euclidean ideal, then its ideal class generates the class group of \( R \), implying that the class group is cyclic. Lenstra then proceeded to prove a generalization of Weinberger’s result for Euclidean ideals.

Lenstra showed \([294]\) by generalizing Weinberger’s work on Euclidean rings, that assuming GRH if \( K \) is a number field with cyclic class group and with \( \mathcal{O}_K \) having infinitely many units, then \([C]\) generates the class group of \( K \) iff \( C \) is a Euclidean ideal. To be more precise, the assumption is that for every squarefree \( n \), the \( \zeta \) function associated to \( K((\mathbb{R}^*_1)^{1/n}) \) satisfies the RH.

As in the Euclidean ring situation, there has been work to prove this without assuming the GRH. In her thesis \([193]\), Graves generalized Motzkin’s reformulation of the Euclidean algorithm and Harper’s work on Euclidean rings to the Euclidean ideal situation. One can define analogous constructions for the \( A_i \)'s and \( B_i \)'s. One can then, using a variation of the large sieve, prove Harper’s theoretical results for the Euclidean ideal situation. They imply that if \( K \) is a number field such that \( |\mathcal{O}_K^*| = \infty \), if \([C]\) generates \( \text{Cl}_K \), and if
\[
\left| \{ \text{prime ideals } p \mid \text{Nm}(p) \leq x, [p] = [C], \mathbb{R}^* \to (\mathbb{R}/p)\times \} \right| \gg \frac{x}{\log^2 x},
\]
then \( C \) is a Euclidean ideal. In a later paper \([192]\), she used this along with a result of Narkiewicz \([386]\), to show that \( \mathbb{Q}(\sqrt{15}, \sqrt{35}) \) has a Euclidean ideal.

Recently, Graves and Ram Murty used the above growth results to prove Lenstra’s result in some cases without assuming the GRH. More precisely, if \( K \) is a finite Galois extension of \( \mathbb{Q} \) with ring of integers \( R \), rank(\( R^* \)) > 3, and cyclic class group \( \text{Cl}_K \), such that its Hilbert class field \( H(K) \) has an abelian Galois group over \( \mathbb{Q} \), then \([C]\) generates \( \text{Cl}_K \) iff \([C]\) is a Euclidean ideal class \([194]\). They then used this to show that \( \mathbb{Q}(\sqrt{5}, \sqrt{21}, \sqrt{22}) \) has a non-principal Euclidean ideal class that is not
9.7. **Miscellaneous.** We mention some other related results without delving deeply into the mathematics involved.

1) **How many primes \( p \) are there with \( p - 1 \) squarefree?** There are two lines of attack. One is à la Artin’s primitive root conjecture. In this approach one notes that \( p - 1 \) is squarefree iff \( p \) does not split completely in any of the cyclotomic fields \( \mathbb{Q}(\zeta_q^2) \), where \( q \) runs over all primes. By inclusion-exclusion this gives then the conjectural natural density \( \delta = \sum_{n=1}^{\infty} \mu(n)/[\mathbb{Q}(\zeta_n^2) : \mathbb{Q}] \). The latter sum is easily seen to equal \( A \). An approach to this problem in this spirit was made by Knobloch [216, 261], a student of Hasse. It turns out, however, that a quite elementary proof is possible. It was found by Mirsky [325]. This uses the trivial identity \( \sum_{d \mid n} \mu(d) = 1 \) if \( n \) is not squarefree and zero otherwise. Note that the number of primes \( p \leq x \) such that \( p - 1 \) is squarefree equals \( \sum_{p \leq x} \sum_{a^2 \mid p - 1} \mu(a) \). Now swap the order of summation. The inner sum is a prime counting sum and can be estimated by the Siegel-Walfisz theorem [15] for a small enough. The contribution from all large \( a \) we can trivially estimate. Carrying out this procedure gives us the same sum for the density \( \delta \) as found in the earlier approach. (Mirsky gives the details of another proof and then for the relevant one for our purposes says it can be done similarly. This is worked out, however, in more detail in, e.g., Moree and Hommersom [356, pp. 17–20].) The same approach was recently followed by Broughan and Zhou [51] to show that the density of primes \( p \) such that \( p - 1 = 2^e m \) with \( m \) odd and squarefree, equals \( 2A \).

Clary and Fabrykowski [89] determined the density of primes \( p \equiv l \pmod{k} \) such that \( ap + b \) is squarefree, where \( (l,k) = 1 \) and \( a > 0 \). It is an explicitly defined rational multiple of the Artin constant.

In view of the analogy between the groups \( \mathbb{F}_p^* \) and \( E(\mathbb{F}_p) \), where \( E/\mathbb{F}_p \) is an elliptic curve, it is natural to also consider the squarefreeness of the elements of the sequence \( \#E(\mathbb{F}_p) = p + 1 - a_p \), as \( p \) goes to infinity. This problem may be interpreted as a stronger version of that of calculating the number of primes \( p \) for which the group \( E(\mathbb{F}_p) \) is cyclic, where \( E \) is a global elliptic curve defined over \( \mathbb{Q} \) and then reduced modulo primes \( p \). The problem of how often \( p + 1 - a_p \) is squarefree was first considered by A.C. Cojocaru in her PhD thesis [104], where she proved an unconditional asymptotic formula for these primes if \( E/\mathbb{Q} \) is with CM (see also [107]) and a conditional asymptotic formula if \( E/\mathbb{Q} \) is without CM.

The above topic is related to the question of how many ways, \( R(n) \) say, there are one can write a given number \( n \) as a sum of a prime and a squarefree number. Let \( B > 1 \) be fixed. In 1936 Walfisz [485] (see also [330, pp. 386-387]) showed that \( R(n) = c(n) \text{Li}(n) + O(n \log^{-B} n) \), where

\[
c(n) = A \prod_{q \mid n} \left(1 + \frac{1}{q^2 - q - 1}\right).
\]

The appearance of \( A \) in this context seems to be unrelated to the multiplicative order. It comes from the first sum below, which happens to be equal to the second
sum arising in primitive root theory:

\[ c(n) = \sum_{d=1, (d,n)=1}^{\infty} \frac{\mu(d)}{\varphi(d^2)} = \sum_{d=1, (d,n)=1}^{\infty} \frac{\mu(d)}{d \varphi(d)}. \]

For some material related to the result of Walfisz, see [150, 397].

2) Higher rank Artin. Note that \( g \) is a primitive root mod \( p \) if the subgroup generated by \( \bar{g} \), the reduction of \( g \) mod \( p \), equals \((\mathbb{Z}/p\mathbb{Z})^*\). If \( g_1, \ldots, g_r \) are rational numbers, one can wonder about

a) the density of primes \( p \leq x \) such that \( \langle \bar{g}_1, \ldots, \bar{g}_r \rangle \) is the full multiplicative group \((\mathbb{Z}/p\mathbb{Z})^*\);

b) the density of primes \( p \) such that each \( g_i, 1 \leq i \leq r \), is a primitive root modulo \( p \).

a) This was studied by Cangelmi and Pappalardi, see [65, 402]. The analogue of \( A \) in this setting is the \( r \)-rank Artin constant

\[ A_r = \prod_{q} \left(1 - \frac{1}{q^r(q-1)}\right). \]

Trivially \( A_1 = A \).

Let \( \kappa(p) \) denote the smallest integer \( r \) such that the first \( r \) primes generate \((\mathbb{Z}/p\mathbb{Z})^*\). Brown and Zassenhaus conjectured in [52] that \( \kappa(p) \leq [\log p] \) for almost all primes \( p \) and that \( \kappa(p) > \log p \) for infinitely many primes \( p \). The latter part of the assertion is true by the result of Graham and Ringrose [188] that the least quadratic non-residue exceeds \( c(\log p) \log \log \log p \) for infinitely many primes \( p \).

If \( U \) denotes the number of primes \( p \leq x \) for which \( g(p) \geq T \), then, by [25] we have \( UT \ll \sum_{p \leq x} g(p) \ll \pi(x) \log^2 x(\log \log x)^4 \). For any \( \epsilon > 0 \), we choose \( T = \log^2 x(\log \log x)^{4+\epsilon/2} \) so that \( U = o(\pi(x)) \) and since \( g(p) \leq T \) is a product of primes \( \leq T \), we infer that for almost all primes \( p \) we have the estimate \( \kappa(p) \leq \log^2 x(\log \log x)^{4+\epsilon/2} \leq (\log p)^2(\log \log p)^{4+\epsilon} \). Pappalardi [400] improved this by showing that \( \kappa(p) = O(\log^2 p/\log \log p) \) for almost all primes \( p \leq x \). Under GRH he showed in another paper [102] that the Brown-Zassenhaus conjecture is true. Moreover, he shows that there is a positive absolute constant \( B \) such that for every divergent function \( y = y(x) \leq \log x/(4 \log \log x) \) and for all primes \( p \leq x \) with at most \( O(\pi(x)B^{-y(x)}) \) exceptions we have \( \kappa(p) \leq [y(p)] \). In 1993, Konyagin and Pomerance [262] and Pappalardi [398] independently proved that for all \( \epsilon > 0 \) and for all primes \( p \leq x \), \( G(p) \leq x^\epsilon \) with at most \( O_\epsilon(1) \) exceptions.

b) This was studied by K. Matthews [324], who determined the density under GRH (formula (1.4)). (This formula contains a typo, one has to replace \( q > 2 \) by \( q \geq 2 \)).

The analogue of \( A \) in this setting is

\[ A_1' = \prod_{q} \left(1 - \frac{1}{q-1}\left(1 - \left(1 - \frac{1}{q}\right)^n\right)\right). \]

Trivially \( A_1' = A \). Pappalardi [404] studied the infinitude of this set of primes \( p \) assuming Schinzel’s Conjecture H. Schinzel [446], relying heavily on results from
Matthews paper, determined assuming GRH the density of primes $p$ such that two prescribed disjoint sets of odd primes $A$ and $B$ have the property that $(b/p) = 1$ for every $b \in B$ and every $a \in A$ is a primitive root modulo $p$. He used this to determine the density $D(p_k, p_l)$ of primes $p$ such that the $k$th-prime $p_k$ is for $p$ the least quadratic non-residue and $p_l$ the least prime primitive root modulo $p$.

The shortest route known to calculating the densities is provided by the average-character-sum method, see Moree and Stevenhagen [361]. In their setup Schinzel’s result follows very easily.

Again, this higher rank analogue of Artin’s conjecture can be formulated in the context of reductions of an elliptic curve $E/\mathbb{Q}$ with arithmetic rank $> 1$, as well as that of an elliptic curve $E/F_q[T]$. As mentioned before, the rational situation was studied by Gupta and Ram Murty in [203, 204], and the function field one by Hall and Voloch in [211].

3) Near-primitive roots. Fix an integer $t$. For the primes $p \equiv 1(\text{mod } t)$ we can ask for the subset of them such that $(\bar{g})$ generates a subgroup of index $t$ in $(\mathbb{Z}/p\mathbb{Z})^*$, see [117, 289, 292, 296, 326, 340, 342, 351, 355, 368, 483]. We let $N_{g,t}(x)$ denote the corresponding counting function. Assuming GRH the corresponding density, $\delta(g, t)$, can be shown to be

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

The first person to do so seems to have been H. Möller [326], followed a few years later by Wagstaff [483]. Since now $nt$ can be non-squarefree making the degree evaluation technically more involved, the resulting answer is less elegant than in the case $t = 1$. For $g > 0$ or $g$ not minus a square, the resulting density was given in Euler product form by Wagstaff [483]. For general $g$ the density has been given in Euler product form by Moree [355]. It turns out that the average-character-sum method [296] leads far more efficiently to this result. The latter method leads also very directly to an iff result for $\delta(g, t)$ to vanish. Lenstra [292] was the first to give these vanishing conditions, but he did this without proof. Since Wagstaff did not work out the Euler product form of the density for every $g$, his result did not make such a proof possible. In the paper by Moree cited above, [355], a proof along the lines of Wagstaff’s approach can be found.

Moree introduced a function $w_{g,t}(p) \in \{0, 1, 2\}$ for which he proved (see [340], for a rather easier reproof see [342]) under GRH that

$$N_{g,t}(x) = (h, t) \sum_{p \leq x, p \equiv 1(\text{mod } t)} w_{g,t}(p) \frac{\varphi((p - 1)/t)}{p - 1} + O\left(\frac{x \log \log x}{\log^2 x}\right).$$

This function $w_{g,t}(p)$ has the property that, under GRH, $w_{g,t}(p) = 0$ for all primes $p$ sufficiently large iff $N_{g,t}$ is finite. Since the definition of $w_{g,t}(p)$ involves nothing more than the Legendre symbol, it is then not difficult to arrive at the vanishing conditions.

To sum up, there are three different approaches to determine exactly when $\delta(g, t)$ vanishes:
1) completing Wagstaff’s work and bringing $\delta(g, t)$ into Euler product form \[355\];
2) using asymptotically exact heuristics for $N_{g,t}(x)$ \[340, 342\];
3) using the average-character-sum method \[296\].

There is no doubt though, that at present approach 3 yields the most elegant and short derivation of the vanishing conditions.

Unaware of the above results Solomon Golomb made in 2004 \[76\] the following near-primitive root conjecture (a review of near-primitive roots from the perspective of Golomb’s conjecture is given in Moree \[354\]. This perspective was abandoned in Moree \[355\], the final version).

**Conjecture 2.** For every squarefree integer $g > 1$, and for every positive integer $t$, the set $N_{g,t}$ is infinite. Moreover, the density of such primes equals a constant (expressible in terms of $g$ and $t$) times the corresponding density for the case $t = 1$ (Artin’s conjecture).

In a 2008 paper Franc and Ram Murty \[161\] made some progress towards establishing this conjecture. In particular they prove the conjecture in case $g$ is even and $t$ is odd, assuming GRH. In general though, this conjecture is false, since in case $g \equiv 1(\text{mod } 4)$, $t$ is odd and $g|t$, $N_{g,t}$ is finite. To see this note that in this case we have $(\frac{g}{p}) = 1$ for the primes $p \equiv 1(\text{mod } t)$ by the law of quadratic reciprocity and thus $r_p(g)$ must be even, contradicting the assumption $2 \nmid t$.

The author proposes the following conjecture (which on GRH can be shown to be true).

**Conjecture 3.** For every squarefree integer $g > 1$, and for every positive integer $t$, the set $N_{g,t}$ is finite iff $g \equiv 1(\text{mod } 4)$, $t$ is odd and $g|t$. In case $N(g, t)$ is infinite it has a natural density that equals a positive constant (expressible in terms of $g$ and $t$) times the corresponding density for the case $t = 1$.

Golomb apparently made his conjecture having in mind the problem of estimating the number of primes in the set $S$, defined as follows. Let $\Phi_n(x)$ denote the $n$-th cyclotomic polynomial. Let $S$ be the set of primes $p$ such that if $f(x)$ is any irreducible factor of $\Phi_p(x)$ over $\mathbb{F}_2$, then $f(x)$ does not divide any trinomial. Using the explicit evaluation of $\delta(g, t)$ and results from Golomb and Lee \[184\], one can then deduce that, on GRH, the set $S$ has a subset of density $> 0.95$, see \[354\].

Felix and Ram Murty \[155, 156\] are interested in the problem of proving estimates of the type

$$\sum_{p \leq x} f(r_p(g)) \sim A_f(g)\pi(x), \quad (22)$$

The case $f(x) = \log x$ and $g = 2$ was first studied by Bach et al. \[25\]. Fomenko \[159\] showed that \[22\] holds true in case $f(x) = \log x$, assuming GRH and Conjecture A of Hooley \[239\] p. 112. Felix and Ram Murty \[156\] managed to prove this result without assuming Conjecture A in case $f(x) = \log^\alpha x$, with $0 < \alpha < 1$. In fact they can deal with a wider class of functions including some arithmetic functions, e.g., $\omega$ and $\Omega$. In a sequel Felix \[155\] establishes \[22\] with $r_p(g)$ replaced by its higher rank analogue. When the rank is at least two, a much more precise version of \[22\] can be established (under GRH), namely with error term $O(x^\theta)$ and $\theta < 1$. 

\[38\]
Ram Murty and Simon Wong [381] showed that at least one of the following holds true:
1) $N_{2,2}$ is infinite.
2) There exist infinitely many primes $p$ such that $2^p - 1$ is composite.

In the same spirit, they announce that a variation of their argument gives that if $2$ is not a primitive root for infinitely many primes $p$, then $(2^p + 1)/3$ is composite for infinitely many primes $p$.

4) Primitive $\lambda$-roots. The definition of primitive roots was extended by Carmichael to that of primitive $\lambda$-roots for composite moduli $n$, which are integers with the maximal order modulo $n$ (which equals the exponent, $\lambda(n)$, of the group $(\mathbb{Z}/n\mathbb{Z})^*$).

We have $\lambda(n)\varphi(n)$. It is an exercise in elementary number theory to describe those $n$ for which $\lambda(n) = \varphi(n)/2$, see, e.g., Lee et al. [287]. Let $N_g(x)$ be the number of natural numbers up to $x$ for which $g$ is a primitive $\lambda$-root. One might wonder then, in analogy with Artin’s conjecture, whether $N_g(x) \sim B(g)x$ for some positive constant $B(g)$ depending on $g$, perhaps with some exceptional values of $g$. Li [303] provides results suggesting that $N_g(x)/x$ does not typically tend to a limit. Let $R(n)$ denote the number of residues modulo $n$ which are primitive $\lambda$-roots for $n$.

One has $R(n) \geq \varphi(\varphi(n))$. Müller and Schlage-Puchta [367] showed that the set of $n$ with $R(n) = \varphi(\varphi(n))$ has density zero. Li [303] showed that $(1/x) \sum_{n \leq x} R(n)/n$ does not tend to a limit as $x$ tends to infinity. In particular, one has

$$\lim \sup_{x \to \infty} \frac{1}{x} \sum_{n \leq x} \frac{R(n)}{n} > 0, \quad \lim \inf_{x \to \infty} \frac{1}{x} \sum_{n \leq x} \frac{R(n)}{n} = 0.$$

Let $E$ denote the set of integers $g$ which are a power higher than the first power or a square times a member of $\{\pm 1, \pm 2\}$. Li [302] showed that for $g \in E$ we have $N_g(x) = o(x)$, and that for every integer $g$ one has $\liminf_{x \to \infty} N_g(x)/x = 0$. Li and Pomerance [307] showed that, under GRH, for each integer $g$ not in $E$ one has $\limsup_{x \to \infty} N_g(x)/x > 0$. Furthermore, Li [304] showed that, for $y \geq \exp((\log x)^{3/4})$, one has

$$\frac{1}{y} \sum_{1 \leq g \leq y} N_g(y) \sim \sum_{n \leq x} \frac{R(n)}{n}, \quad \text{as } x \to \infty.$$ 

The range for $y$ was extended by Li and Pomerance [308]. See also [301, 304, 305, 367] for further results and [306] for a survey on primitive roots, with special focus on primitive $\lambda$-roots.

5) Squarefreeness. Pappalardi [403] studied the problem of determining how many primes $p \leq x$ there are such that $\text{ord}_p(g)$ is squarefree (and similarly $\text{ord}_m(g)$, where $m$ ranges over the integers $\leq x$ for which the latter order is defined). Using a simple characterisation of those $n$ for which Carmichael’s function $\lambda(n)$ is squarefree together with Mirsky’s result from §9.7.1, Pappalardi, Saidak and Shparlinski [405] have shown that the number of $n \leq x$ such that $\lambda(n)$ is squarefree is asymptotically equal to $cx \log^{A-1} x$, for some constant $c > 0$. Note that Artin’s constant appears in an unusual position in the formula! There are of course various generalisations.
possible, e.g., to ‘roughly’ squarefree values \[35\] and \(k\)th powerfree values \[36\].

6) Goldstein’s conjecture and follow up. Larry Goldstein formulated a conjecture in 1968 which implies Artin’s conjecture (announcement \[180\], detailed version \[181\]). For each prime \(q\), let \(L_q\) be a Galois extension over \(\mathbb{Q}\). For each integer \(k\) let \(L_k\) be the compositum of those \(L_p\) for which \(p\) divides \(k\), and let \(n(k)\) be the degree of \(L_k\) and \(d_k\) its discriminant; then the set of primes \(p\) that split completely in none of the \(L_q\) equals

\[
\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}
\]

if this series converges absolutely. This conjecture is known to be false, even for certain abelian \(L_q\) (Weinberg \[493\]). In 1973, Goldstein \[182\] proved a special case of his conjecture (assuming GRH) for families of abelian \(L_q\)satisfying certain conditions on their discriminants, degrees, and splitting of primes. An unconditional version of his result was established by Ram Murty \[371\].

**Theorem 8.** Suppose that for \(q\) sufficiently large, the extensions \(L_q\) are abelian over \(\mathbb{Q}\) and

1. \(\log |d_k| = O(n(k) \log k)\)
2. if a prime \(p\) splits completely in \(L_q\), then for \(q\) sufficiently large \(p \geq f_q\), where \(f_q\) is the conductor of \(L_q\);
3. \(\sum_{k \geq y} \frac{1}{n(k)} = o\left(\frac{1}{\log y}\right)\), as \(y \to \infty\),

then the set of primes which do not split completely in any \(L_q\) has a density \(\delta\) given by \((23)\).

In 1983, assuming GRH Ram Murty established a variant of Goldstein’s conjecture in a lattice theoretic setting and applied it to elliptic curves \[370\].

7) Brizolis’ conjecture. Brizolis conjectured that for every prime \(p > 3\) there exist an \(x\) and a primitive root \(g \pmod{p}\) such that \(x \equiv g^x \pmod{p}\). Let \(N(p)\) denote the number of \(1 \leq x \leq p - 1\) such that \(x\) is a primitive root mod \(p\) and \(x\) and \(p - 1\) are coprime. It is easy to see that if \(N(p) \geq 1\), then Brizolis’ conjecture is true for the prime \(p\). (Let \(y\) be the multiplicative inverse of \(x\) modulo \(p - 1\) and consider \(g = x^y\). Then \(g^x \equiv x^{xy} \equiv x \pmod{p}\) and \(g\) is a primitive root for \(p\).) Hausman \[220\] showed that \(N(p) \geq 1\) for every sufficiently large prime \(p\). Let \(\omega(n)\) denote the number of distinct prime divisors of \(n\) and \(d(n)\) the number of divisors of \(n\). Cobeli and Zaharescu \[94\] and, independently Wen Peng Zhang \[507\] using character sums and the Weil bounds proved that

\[
N(p) = \frac{\varphi(p-1)^2}{p-1} + O(\sqrt{p} 4^{\omega(p-1)} \log p),
\]

and used this to show that Brizolis’ conjecture is true for every prime \(p > 10^{50}\). The full Brizolis’ conjecture was settled by Campbell \[63\]. In a later paper \[298\] she and her coauthors using a numerically explicit “smoothened” version of the Pólya-Vinogradov inequality showed that for each prime \(p > 3\), there is a primitive root.
for $p$ in $[1, p-1]$ that is coprime to $p-1$. This led to a new proof of Brizolis conjecture requiring far less computer calculation.

Note that if $x \equiv g^x (\text{mod } p)$, then $x$ is 1-cycle under taking the discrete logarithm with respect to $g$. For small $k$, $k$-cycles of the discrete logarithm problem are studied in Holden and Moree [236] (for more experimental work in this direction see [233, 234]), see also Glebsky and Shparlinski [178]. Let $F(p)$ denote the number of pairs $(g, h)$ satisfying $g^h \equiv h (\text{mod } p)$ with $1 \leq g, h \leq p-1$. Let $G(p)$ denote the number of pairs $(g, h)$ satisfying $g^h \equiv h (\text{mod } p)$ with $1 \leq g, h \leq p-1$, where in addition we require $g$ to be a primitive root modulo $p$. Holden and Moree [236, Conjecture 8.3] conjectured that

$$\sum_{p \leq x} F(p) p^{-1} = (1 + o(1)) \pi(x) \quad \text{and} \quad \sum_{p \leq x} G(p) p^{-1} = (A + o(1)) \pi(x).$$

This conjecture with quantitative error estimates has meanwhile been established by Bourgain et al. [44]. A related conjecture by Holden and Moree [236] states that one should have $F(p) = (1 + o(1)) p$. Bourgain et al. [44] showed that $F(p) = p + O(p^{4/5+\epsilon})$ for a set of primes $p$ of relative density 1 and in a later paper, [45], $F(p) \geq p + O(p^{3/4+\epsilon})$ and $F(p) = O(p)$.

The above questions are all modulo $p$, we can also ask them modulo prime powers. A preliminary approach to these questions was made by Holden and Robinson [237] using $p$-adic methods, primarily Hensel’s lemma and $p$-adic interpolation.

8) $\omega(n) = \omega(n + 1)$ and Artin. Erdős conjectured that there are infinitely many integers $n$ such that $\Omega(n) = \Omega(n + 1)$, where $\Omega(n)$ denotes the total number of prime divisors of $n$ and a similar result for $\omega(n)$. The former conjecture was proved in 1984 by Heath-Brown [221], but the latter was only proved by Schlage-Puchta in 2003 [448]. Kan in 2004 [251], unaware of the latter result, proved the weaker result that not both the $\omega(n) = \omega(n + 1)$ conjecture and the qualitative form of Artin’s primitive conjecture can be false.

Heath-Brown actually proved that there are infinitely many integers $n$ such that $d(n) = d(n + 1)$ (thus solving a conjecture of Erdős and Mirsky) and remarks that his method can similarly prove that $\Omega(n) = \Omega(n + 1)$ infinitely often, where $d(n)$ denotes the number of positive divisors of $n$.

9) Artin over number fields. Over arbitrary number fields, there are two obvious ways in which Artin’s conjecture can be generalized. Fix a number field $K$ with ring of integers $\mathcal{O}_K$, and a nonzero element $\alpha \in \mathcal{O}_K$, which is not a root of unity. We expect the following generalization to hold: the set of primes $p$ of $K$ for which $\alpha$ generates the cyclic group $(\mathcal{O}_K/p\mathcal{O}_K)^\ast$ has a density inside the set of all primes of $K$. Moreover, the situation is highly similar to the rational case, as the set of primes $p$ of $K$ for which $(\mathcal{O}_K/p\mathcal{O}_K)^\ast$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\ast$ has density 1. In 1975 Cooke and Weinberger [112] proved that this generalization of Artin’s conjecture is indeed true and the density is given by the infinite sum in [9] with $\mathbb{Q}$ replaced by $K$, if an appropriate generalization of RH holds.
Roskam \cite{139} considers a generalization of Artin’s conjecture in a “rational” direction: the set of rational primes \( p \) for which the order of \( \alpha \) in \((\mathcal{O}_K/p\mathcal{O}_K)^*\) is equal to the exponent of this group has a density inside the set of all rational primes. He proves that, assuming that an appropriate generalization of RH is true, this conjecture holds for quadratic fields \( K \). A less general result in this direction he established in \cite{437} (but with a rather easier proof). Kitaoka and various of his pupils did a lot of work on Artin’s conjecture for units (rather than general elements) in number fields, cf. \cite{70, 245, 253, 254, 257, 258, 259, 260} (this being only a partial list of references).

10) Artin for matrices. Let \( A \) be a hyperbolic matrix in \( \text{SL}_2(\mathbb{Z}) \), that is a matrix with absolute trace greater than 2. We may define \( \text{ord}_n(A) \) to be the order of \( A \) in \( \text{SL}_2(\mathbb{Z}/n\mathbb{Z}) \). It can be shown that for a hyperbolic matrix in \( \text{SL}(2, \mathbb{Z}) \) there is a density-one sequence of integers \( n \) such that its order mod \( n \) is slightly larger than \( \sqrt{n} \). This is a crucial ingredient in an ergodicity theorem regarding eigenstates of quantized linear maps \( A \) of the torus ("cat maps"), see Kurlberg and Rudnick \cite{273}. Under an appropriate generalisation of RH it can be shown \cite{272} that for almost all \( n \) we have \( \text{ord}_n(A) \gg n^{1-\epsilon} \) for any \( \epsilon > 0 \). Call a matrix \( A \) exceptional if it is of finite order or if it is diagonalizable and a power \( A^r \) of \( A \) has all eigenvalues equal to powers of a single rational integer \( > 1 \), or equal to powers of a single unit \( \neq 1 \) of a real quadratic field. Corvaja et al. \cite{113} established that if \( A \) is not exceptional, then the quotient \( \text{ord}_n(A)/\log n \) tends to infinity with \( N \), with their proof ultimately relying on the Schmidt subspace theorem from Diophantine approximation. Their result is best possible since, for any exceptional matrix \( A \), there exist some \( c > 0 \) and arbitrarily large integers \( n \) for which \( \text{ord}_n(A) < c \log n \).

Since the eigenvalues of \( A \) are units in a quadratic number field, this problem is closely related to that discussed in part 9.

11) Artin for K-theory of number fields. (Written by W. Gajda.) For basic references concerning K-theory the reader should consult \cite{169} and \cite{170}. For a number field \( K \) we denote by \( \mathcal{O}_K \) the ring of algebraic integers. The class group of \( \mathcal{O}_K \) is isomorphic to the quotient \( K_0(\mathcal{O}_K)/\mathbb{Z} \), where \( K_0(R) \) denotes the Grothendieck of a commutative ring \( R \) with unity. The group of units \((\mathcal{O}_K)^*\) coincides with the group \( K_1(\mathcal{O}_K) \) defined by Bass in the sixties. In 1972 Quillen introduced groups \( K_n(R) \), for all integers \( n \geq 0 \), the so called higher algebraic K-theory groups of \( R \). In the case \( R = \mathcal{O}_K \) one can treat Quillen’s groups as higher dimensional analogs of the class group of \( \mathcal{O}_K \) - for \( n \) even, and of the group of units \((\mathcal{O}_K)^*\) - for \( n \) odd. The groups \( K_n(R) \) enjoy many very useful properties. In particular, they depend functorially on the ring \( R \). For a fixed \( n \), the reduction at a prime ideal \( \mathfrak{p} \) of \( \mathcal{O}_K \) induces a group homomorphism: \( K_n(\mathcal{O}_K) \rightarrow K_n(\mathcal{O}_K/\mathfrak{p}) \), which for \( n = 1 \) can be easily identified with the map \((\mathcal{O}_K)^* \rightarrow (\mathcal{O}_K/\mathfrak{p})^*\). Due to a classical result of Quillen \( K_n(\mathcal{O}_K) \) are finitely generated abelian groups. On the other side, \( K_n(\mathcal{O}_K/\mathfrak{p}) \) vanishes, for \( n > 0 \) and even, and is a finite cyclic group, if \( n > 0 \) and odd. The ranks of the groups \( K_n(\mathcal{O}_K) \) were determined by Borel. In particular, if \( \mathcal{O}_K = \mathbb{Z} \), then the group \( K_n(\mathcal{O}_K) \)
is of rank 1, if \( n = 0 \) or \( n = 4m + 1 \) for an integer \( m > 0 \), and is finite, otherwise. We expect that the following analog of the Artin conjecture holds for the \( K \)-groups of the integers: for a fixed \( n = 4m + 1 \) and \( m > 0 \), the set of primes \( p \) for which the homomorphism \( K_n(\mathbb{Z}) \rightarrow K_n(\mathbb{F}_p) \) is onto, has a natural positive density. Note that for \( n \) as above, due to another classical result of Quillen \( K_n(\mathbb{F}_p) \cong \mathbb{Z}/(p^{2m+1} - 1) \), and conjecturally \( K_n(\mathbb{Z}) \cong \mathbb{Z} \), at least up to 2-torsion. For some results supporting this conjecture and the discussion of the relation of the reduction map on the \( K \)-groups to deep questions in number theory, such as the Kummer-Vandiver conjecture, we refer the reader to the survey paper [170].

12) Griffin's dream. R. Griffin (a mathematical amateur) thought in 1957 that the decimal expansions of \( 1/p \) should have period length \( p - 1 \) for all primes of the form \( 10X^2 + 7 \). The first 16 primes \( p \) of the form \( 10X^2 + 7 \) have indeed decimal period \( p - 1 \), but this is not true for \( p = 7297 \), the 17th such prime. D. Lehmer [288] found in 1963 that 326 is a primitive root for the first 206 primes of the form \( 326X^2 + 3 \). More impressive examples in the same spirit can be given using recent results on prime producing quadratics by Moree [352] and K. Scholten [451]. Y. Gallot holds the record in which 206 is being replaced by 38639. Scholten [451] was the first to consider prime producing cubics and he found one having the property that the first 10011 primes \( p \) it produces are such that that 11045 is a primitive root modulo \( p \).

13) Artin and binomial coefficients. Interest in prime divisors of binomial coefficients dates back at least to Chebyshev. It is not difficult to see that unless \( k \) is fairly close to one of the ends of the range \( 0 \leq k \leq n \), then the coefficient \( \binom{n}{k} \) contains many prime factors and many of these occur with high multiplicity. Erdős made a number of conjectures quantifying these observations, one well-known conjecture being that the middle coefficient \( \binom{2n}{n} \) is not squarefree for any \( n > 4 \). Granville and Ramaré [190] proved this conjecture in 1996. The corresponding problem for \( q \)-binomial and, more generally, \( q \)-multinomial coefficients is much more complicated. Sander [443] showed how Artin’s primitive root conjecture implies the respective results.

14) Ulmer’s rank result. Let \( \mathbb{F}_q \) be the finite field of \( q \) elements of prime characteristic \( p \). If \( (n, q) = 1 \), then it can be shown that \( X^n - 1 \) factors into distinct irreducible factors over \( \mathbb{F}_q \). The quantity \( i_q(n) \) appears in various mathematical settings, for example in Ulmer’s study of elliptic curves with large rank over function fields [176], the study of the cycle structure of repeated exponentiation modulo a prime \( p \) [79] [455], see Moree and Solé [357] for further examples). Using
the Cauchy-Frobenius identity coupled with elementary group-theoretical considerations, Deaconescu [121] has shown that

\[ i_q(n) = \frac{1}{\text{ord}_q(n)} \sum_{d | \text{ord}_q(n)} \varphi\left(\frac{\text{ord}_q(n)}{d}\right)(n, q^d - 1). \]

Ulmer considers the parametric family of curves \( E_d : y^2 + xy = x^3 - t^d \) over the function field \( \mathbb{F}_q(t) \), where \( d \) is a positive integer. Ulmer [476] Theorem 9.2] showed that if \( d \) is a divisor of the sequence \( \{p^k + 1\} \), then the rank \( R_q(d) \) of \( E_d \) over \( \mathbb{F}_q(t) \) is given by \( R_q(d) = i_q(d) - \epsilon_q(d) \), with \( \epsilon_q(d) \) an explicit correction term that always satisfies \( 0 \leq \epsilon_q(d) \leq 4 \).

Using techniques from the study of Artin primitive root type problems (for example a version of the Chebotarev density theorem due to Lagarias and Odlyzko), Pomerance and Shparlinski [425] showed that the typical rank in Ulmer’s family \( R_q(d) \) tends to infinity as \( d \to \infty \). In particular, they proved that except for \( o_p(x) \) values of \( d \leq x \), one has \( R_q(d) \geq (\log d)^{1/3} \log \log \log d \). Further they established the existence of an absolute constant \( \alpha > 0 \) such that for all finite fields \( \mathbb{F}_q \) and all sufficiently large values of \( x \) (depending only on the characteristic \( p \) of \( \mathbb{F}_q \)), one has \( x^{-1} \sum_{d \leq x} R_q(d) \geq x^\alpha \). This shows that the family \( E_d \) is quite special, as Brumer [53] has shown that the average rank for all elliptic curves over a function field of positive characteristic is asymptotically bounded above by 2.3.  

15) **Primitive roots compared with quadratic non-residues.** Let \( n \) be a power \( p^h \) or \( 2p^h \), with \( p \) an odd prime. Write

\[ PR(n) = \{ g \in (\mathbb{Z}/n\mathbb{Z})^\times, \ g \text{ is a primitive root modulo } n \}, \]
\[ QNR(n) = \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times, \ a \text{ is a quadratic non-residue modulo } n \} \]

for the set of primitive roots and quadratic non-residues modulo \( n \), respectively. Obviously \( PR(n) \subseteq QNR(n) \). By methods from elementary number theory and combinatorics Gun et al. [200] classified those \( n \) for which

\[ \#(PR(n)) = \#(QNR(n)) - 2^\epsilon. \]

Modulo \( p \) the number of nonquadratic residues which are not primitive roots is obviously \( g(p) := (p - 1)/2 - \varphi(p - 1) \). The values assumed by \( g \) were investigated by Luca and Walsh [316] and by Robbins [430]. More recently, Gun et al. [199] applied character sum estimates to prove results on consecutive quadratic non-residues modulo \( p \) that are not primitive roots. They showed for example that given a fixed \( 0 < \epsilon < 1/2 \) and any positive integer \( N \), then for all primes \( p \geq \exp((2e^{-1})^{8N}) \) satisfying \( \varphi(p - 1)/(p - 1) \leq 1/2 - \epsilon \), we can find \( N \) consecutive quadratic non-residues modulo \( p \) that are not primitive roots. More recently Luca et al. [314] showed that in fact the same property holds starting with significantly smaller primes. These results are analogous to earlier results by A. Brauer [16] (quadratic residues, quadratic non-residues) and Szalay [472] (primitive roots).

16) **The Crandall-Collatz \( qx + 1 \) problem.** For positive odd numbers \( q \) and \( m \), let \( C_q(m) \) denote the largest odd factor of \( qm + 1 \). The sequences of iterates
\( C_q(m), \ C_q(C_q(m)), \ldots \) consists of the odd numbers in the orbit of \( m \) under the \( qx + 1 \) function. The \( 3x + 1 \) conjecture (unproven) asserts that for \( q = 3 \) such an orbit always contains the number 1, cf. Lagarias [277] or the book [278]. Crandall conjectured that for every odd number \( q > 3 \) there always exists an integer \( m \) such that 1 does not occur in the orbit of \( m \) under the \( qx + 1 \) function. A number \( q \) for which such an \( m \) exists we call a Crandall number. Crandall [115] showed that 5, 181 and 1093 are Crandall numbers. The proofs for 5 and 181 involve cycles: for \( q = 5 \), we have the cycle 13, 33, 83, 13, and for \( q = 181 \), we have the cycle 27, 611, 27. The proof for 1093 depends on the fact that it is a Wieferich prime, that is a prime \( p \) such that \( 2^{p-1} \equiv 1(\text{mod } p^2) \). It is conjectured that there are infinitely many, but presently only two of them are known: 1093 and 3511. We define a positive odd integer \( q \) to be a Wieferich number if \( q \) and \( (2^{\text{ord}_q(2)} - 1)/q \) are not coprime. These definitions are consistent in the sense that a Wieferich prime is a Wieferich number, and a prime Wieferich number is a Wieferich prime. Franco and Pomerance [162] showed that every Wieferich number is a Crandall number, and that the Wieferich numbers have relative density 1 in the odd numbers. The appearance of \( \text{ord}_q(2) \) in this setting is trivial: the odd number \( r \) is in the range of \( C_q \) iff \( 2^j r \equiv 1(\text{mod } q) \) for some integer \( j \), so that the residue classes modulo \( q \) are precisely those in the subgroup of \( (\mathbb{Z}/q\mathbb{Z})^\times \) generated by 2 modulo \( q \) (see also [263]). Also in some weaker versions of the \( 3x + 1 \) problem, the order of 2 modulo \( q \) makes its appearance, see, e.g., [66].

As a byproduct Franco and Pomerance [162] showed that \( N_m(x) = o(x) \) (see §9.7.17 for the definition of \( N_m(x) \)).

17) Counting integers with odd order. Let \( m \geq 1 \) be an arbitrary integer and let \( N_m(x) \) count the number of odd integers \( u \leq x \) such that \( m \nmid \text{ord}_u(2) \). In case \( m = q \) is an odd prime H. Müller [364] proved that

\[
\frac{x}{\log^{1/(q-1)} x} \ll N_q(x) \ll \frac{x}{\log^{1/q} x}.
\]

This was improved in Moree [350] to

\[
N_q(x) = c_q x \log^{q/(q^2-1)} x \left(1 + O\left(\frac{(\log \log x)^5}{\log x}\right)\right),
\]

with \( c_q > 0 \) a constant. The latter result was subsequently generalized by Müller [365] to the case where \( m = q^n \). Subsequently this result was generalized to arbitrary \( m \) see Moree [350]. For a nice survey of the material discussed under §9.7.16 and §9.7.17, see Müller [366].

18) Pseudorandom number generators. Of importance in computer science are pseudorandom number generators, an example being the power generator, where the sequence is given by \( u_{i+1} \equiv u_i^2(\text{mod } n) \). This generator is periodic, and for it to behave pseudorandom, the period must be large. Some light on this can be shed by techniques used in the study of Artin’s primitive root conjecture; see, e.g., [164, 273, 321]. Goubin, Mauduit and Sárközy [187] studied the pseudorandomness.
of sequences $e_1, \ldots, e_N$ with $e_n = \left(\frac{f(n)}{p}\right)$ if $p$ and $f(n)$ are coprime, and $e_n = 1$ otherwise, where $f(X) \in \mathbb{F}_p[X]$ has positive degree. In their considerations the order of $2(\text{mod } p)$ plays an important role (the larger it is the better).

The analogous problem of studying pseudoprime reductions of an elliptic curve over $\mathbb{Q}$ was considered by Cojocaru, Luca and Shparlinski in [109]. Some of their results were recently improved on by David and Wu [120].

19) **Non-primitive roots.** Let $E(M, N)$ denote the number of integers in the interval $[M + 1, M + N]$ which are not primitive roots modulo $p$ for any odd prime $p \leq \sqrt{N}$. Gallagher, in the fundamental paper [108] in which he introduced what is now called Gallagher’s large sieve, gave the estimate $E(M, N) = O(\sqrt{N} \log N)$. This was improved by Vaughan [479] to $E(M, N) = O(\sqrt{N} \log c N)$ for some explicit $c = 0.37 \ldots$. Note that the result is quite sharp as $E(M, N)$ includes the squares in the interval and so trivially $E(0, N) \gg \sqrt{N}$. A number field analogue of Gallagher’s result was established by Hinz [228]. In a later paper Hinz [230] obtained an analogue of Vaughan’s result with an explicit value of $c < 1$ depending on the field.

20) **Romanoff’s result and follow up.** In Bilharz’s [39] work on the Artin primitive root conjecture over $\mathbb{F}_q[T]$ the density

\[ \sum_{m=1, \ q|m}^{\infty} \frac{\mu(m)}{m \ \text{ord}_m(q)} \]  

appeared. The absolute convergence of this sum was proven by Romanoff [434]. A simpler proof was given by Erdős and Turán [148]. However, a much simpler proof of this was given by Erdős [141]. Romanoff’s result was strengthened and generalized by Landau [281] and more recently by Ram Murty et al. [377], who also established analogous results over number fields and for abelian varieties.

Romanoff proved that the integers of the form $p + 2k$ have positive lower density (for a nice reproof see Montgomery and Vaughan [330, pp. 98–99]). He raised the following question: does there exist an arithmetic progression consisting only of odd numbers, no term of which is of the form $p + 2k$? Erdős [140] found such an arithmetic progression by considering integers which are congruent to 172677 modulo 5592405($= (2^{24} - 1)/3$). Thus the density of numbers of the form $p + 2k$ is less than $1/2$, the trivial bound obtained from the odd integers. Put

\[ d = \lim \inf_{x \to \infty} \frac{\# \{p + 2k \leq x\}}{x/2} \text{ and } \overline{d} = \lim \sup_{x \to \infty} \frac{\# \{p + 2k \leq x\}}{x/2}. \]

Habsieger and Roblot [208] showed that $\overline{d} < 0.9819$. Pintz [420] showed that $d \geq 0.18734$. The first explicit lower bound for $\overline{d}$ was found by Chen and Sun [72].

A related conjecture is due to Erdős, who conjectured that 7, 15, 21, 45, 75 and 105 are the only integers $n$ for which $n - 2^k$ is a prime for every $k$ with $2 \leq 2^k < n$. Vaughan [479] gave an estimate for the number of integers $n \leq x$ of this form [479 (1.5)]. Assuming that 2 is a primitive root infinitely often, it is not difficult (see Hooley [239 pp. 113–115]) to show that the number of such integers $n \leq x$ is
O(x^{1-A+\epsilon}). Narkiewicz \cite{384} sharpened this estimate to \(O(x^{1-A/(\log 2)+\epsilon})\).

Ram Murty and Srinivasan \cite{379} considered a sum akin to (24). They showed that if

\[ S_a(x) := \sum_{p \leq x, \ p \nmid a} \frac{1}{\text{ord}_p(a)} = O(x^{1/4}) , \]

then Artin’s conjecture holds true. Unconditionally they showed that the latter sum is \(\ll \sqrt{x} \). Erdős and Ram Murty \cite{144} later improved on this by showing there exists \(\delta > 0\) such that \(S_a(x) \ll \sqrt{x} \log^{-1-\delta} x\). Felix \cite{154} showed that if \(x/\log x = o(y)\), then

\[ \frac{1}{y} \sum_{\alpha \leq y} S_a(x) = \log x + O(\log \log x) + O(x/y) , \]

showing that \(S_a(x)\) equals \(\log x\) on average. He established a similar result for \(S_a(x)\), but with \(\text{ord}_n(a)\) replaced by \(\varphi(\text{ord}_n(a))\), showing that this sum is \(\zeta(2)\zeta(3) \log x/\zeta(6)\) on average. The asymptotic he obtains involves a constant arising in the Titchmarsh divisor problem (cf. Problem 40).

21) \textit{Erdős-Kac type theorems for the multiplicative order.} An arithmetic function is said to have a \textit{normal order} \(F(n)\), iff for any \(\epsilon > 0\), for almost all \(n \leq x\), one has \((1-\epsilon)F(n) < f(n) < (1+\epsilon)F(n)\). In 1917 Hardy and Ramanujan \cite{212} showed that \(\omega(n)\) has normal order \(\log \log n\). In 1940, Erdős and Kac \cite{143} proved a more refined result: the quantity

\[ \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \]

is normally distributed, thus the normal order \(\log \log n\) serves as the mean, and \(\sqrt{\log \log n}\) as standard deviation. This result can be more precisely formulated as follows:

\[ \lim_{x \to \infty} \left( \frac{1}{x} \cdot \# \left\{ n \leq x : \alpha \leq \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \leq \beta \right\} \right) = G(\alpha, \beta) , \]

where \(G(a, b) := \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt\) denotes the Gaussian normal distribution. This celebrated result marked the birth of a whole new branch of number theory: probabilistic number theory. See Elliott \cite{133, 134} and Tenenbaum \cite{473} for books dealing with this topic.

Under GRH the following result was proved by Saidak in his PhD thesis and Ram Murty and Saidak \cite{378}. Let \(a \geq 2\) be an integer. We have

\[ \lim_{x \to \infty} \left( \frac{1}{x} \cdot \# \left\{ n \leq x : (a, n) = 1, \alpha \leq \frac{\omega(\text{ord}_n(a)) - \frac{1}{2}(\log \log n)^2}{\sqrt{\frac{1}{3}(\log \log n)^3}} \leq \beta \right\} \right) = G(\alpha, \beta) \frac{\varphi(a)}{a} . \]

Later Li and Pomerance \cite{307} gave a different proof, also requiring GRH. Erdős and Pomerance \cite{145} had earlier conjectured the latter result and proved that it is true with \(\text{ord}_n(a)\) replaced by \(\varphi(n)\). For analogues in the setting of elliptic curves, see, e.g., Cojocaru \cite{106} and Liu \cite{310, 311}, and in the context of Drinfeld modules see \cite{108, 269, 270, 271}.
In [269] Kuo and Liu give a short survey of Erdős-Kac type theorems and sketch the proof of the main result in their paper [270].

22) **Gauss periods.** In connection with a problem involving Gauss periods, Gao et al. [171] raised the question of determining the density of primes $p \equiv 1(\text{mod } k)$ such that $\frac{p-1}{\text{ord}_p(g)}$ and $\frac{p-1}{k}$ are coprime. For a given $g$ and $k$, von zur Gathen and Pappalardi [174] showed that, under GRH, this density exists and computed an Euler product for it. Gauss periods are of interest to perform fast arithmetic in finite fields [173].

23) **Golomb’s conjectures.** In 1984, Golomb [183] made four conjectures, which if true could be applied to construct so-called Costas arrays which were first considered by Costas [114] in attempting to construct sonar signal patterns. Independently, Gilbert [176] also wrote about them in the same year, publishing what is now known as the logarithmic Welch method of constructing Costas arrays. Costas arrays concern primitive elements in finite fields. For our purposes it suffices to formulate the first three of these conjectures in the case where the finite field is of prime order. A) If $p$ is odd, then there are two not necessarily distinct primitive roots $g_1$ and $g_2$ such that $g_1 + g_2 \equiv 1(\text{mod } p)$. B) If $p$ is odd, then there are two not necessarily distinct, primitive roots $g_1$ and $g_2$ such that $g_1 + g_2 \equiv -1(\text{mod } p)$. C) For all $p$ large enough, every $c$ with $p \nmid c$ can be written as $c \equiv g_1 + g_2$ with $g_1$ and $g_2$ primitive roots modulo $p$.

After work of various authors, it is now known that these conjectures are true; see S. Cohen and Mullen [100]. A more general form of Conjecture C is also known to be true [99]. A related question is to estimate the number of solutions $g_1, g_2$ for a fixed $c$ (representations of $c$) asymptotically as $p \to \infty$ [102, 511].

24) **Fibonacci primitive roots.** Various authors considered primitive roots that in addition are required to satisfy a polynomial equation. In this context, most frequently the **Fibonacci primitive roots** have been considered: a primitive root $g$ modulo a prime $p$ is called a Fibonacci primitive root if $g^2 \equiv g + 1(\text{mod } p)$. More generally, if $m > 1$, $A$ and $B$ are integers, then a primitive root $g$ modulo $m$ is called a generalized Lucas primitive root modulo $m$ with parameters $A$ and $B$ if $m$ divides $g^2 - Ag + B$, see, e.g., Mollin [327].

Shanks [456] conjectured that the density of Fibonacci primitive roots equals $27A/38$. Under GRH this was shown to be true by Sander [412] in 1990. However, this result was already established by Lenstra in 1977 [292, Theorem 8.1].

25) **$N(H, p)$.** For primes $p$ let $N(H, p)$ denote the number of primes $q \leq H$ which are primitive roots modulo $p$. Heuristically one expects that $N(H, p)$ should be well approximated by $\frac{\phi(p-1)}{p-1} \pi(H)$. Results in this direction were established by Elliott
and, more recently, Nongkynrih \textsuperscript{391}.

26) \textit{Primitive roots and groups}. There are many papers in the group theory literature based on the problem of recognizing a finite group by the set of its element orders. For a finite group the set of orders of all its elements is called a spectrum of this group. A finite group is called recognizable from its spectrum if all finite groups with the same spectrum are isomorphic to this group. Lyuchido and Mogkhaddamfar \textsuperscript{317} proved that for an odd prime \( p \) the projective special linear group \( L_p(2) \) is recognizable from its spectrum if \( 2 \) is a primitive root modulo \( p \).

Recall that \( \text{Aut}(C_n(p)) \) is the symplectic group of \( 2n \times 2n \) matrices over \( \mathbb{F}_p \). Thompson \textsuperscript{474} proved that if \( p \) is an odd prime which is a primitive root modulo the prime \( l \geq 5 \), then \( \text{Aut}(C_{l-1}/2(p)) \) is the Galois group of an extension of \( \mathbb{Q}(t) \).

Let \( p \) and \( r \) be odd primes. Abért and Babai \textsuperscript{1} considered the wreath product \( W(r, p) \) of the cyclic groups \( C_r \) and \( C_p \). They showed that the maximum size of the minimal generating set of \( W(r, p) \) equals \( 2 + (p - 1)/\text{ord}_p(g) \). They used this result to answer a question of Lubotzky.

Martin and Valette \textsuperscript{319} considered the solvable Baumslag-Solitar group \( BS_n = \{ s, b : aba^{-1} = b^n \} \) for \( n \geq 2 \). They showed for example that if the Artin conjecture holds for the integer \( n \), then the spectrum of the associated Markov operators contains the set \( \{ z \in \mathbb{C} : |z| = 1/2 \} \).

27) \textit{Least primitive root modulo} \( p \). Let \( g(p) \) denote the least primitive root modulo \( p \), and \( h(p) \) be the least positive primitive root modulo \( p^2 \). Using Gauss sums Vinogradov \textsuperscript{481} (see also Landau \textsuperscript{250}) showed in 1930 that \( g(p) < 2^{\omega(p-1)}p^{1/2} \log p \). This was improved to \( g(p) < 2^{\omega(p-1)+1} \sqrt{p} \) in 1942 by Hua \textsuperscript{243}. Erdős \textsuperscript{139} showed that \( g(p) = O(\sqrt{\log \log \log p}) \), and Erdős and Shapiro \textsuperscript{147} that \( g(p) = O(\omega(p-1)^c \sqrt{p}) \), for some absolute constant \( c \). Burgess \textsuperscript{55} using his celebrated character sum estimates proved that \( g(p) = O(p^{1/4+\epsilon}) \) and \( h(p) = O(p^{1/2+\epsilon}) \). The former estimate was achieved independently by Wang \textsuperscript{487}. S. Cohen et al. \textsuperscript{101} sharpened the latter estimate to \( h(p) = O(p^{1/4+\epsilon}) \). Elliott and Murata \textsuperscript{137} considered the least primitive root mod \( 2p^2 \). They also considered moments of \( g(p) \), that is sums of the form \( \pi(x)^{-1} \sum_{p \leq x} g(p)^\delta \) (in \textsuperscript{136}); in particular they showed that if \( \delta < 1/2 \) assuming GRH the latter sum tends to a constant depending on \( \delta \). Elliott \textsuperscript{130} has shown that for all but \( O(X^\epsilon) \) primes \( p \) up to \( X \), one has \( g(p) = O(\log^c p) \), with \( c_\epsilon \) a constant depending on \( \epsilon \). In the same paper he proved that \( g(p) < 475 \log^{1.6} p \) for infinitely many primes \( p \). The latter result was superseded in 1984 by Gupta and Murty \textsuperscript{202} who obtained the bound \( g(p) < 2250 \) for infinitely many primes \( p \). Subsequently this bound was reduced to \( g(p) \leq 7 \) for infinitely many primes \( p \) by Heath-Brown \textsuperscript{222}. Under GRH, Wang \textsuperscript{487} has shown that \( g(p) \ll (\log^2 p)\omega(p-1)^6 \). Utilizing a combinatorial sieve due to Iwaniec, Shoup \textsuperscript{458} improved this to \( g(p) \ll \omega(p-1)^4(\log(\omega(p-1)) + 1)^4 \log^2 p \). Towards a lower estimate for \( g(p) \), it is known that infinitely often \( g(p) \) can exceed \( c(\log p)(\log \log \log p) \) for a certain \( c > 0 \) \textsuperscript{188}. This improves dramatically on a result of Pillai \textsuperscript{419}, who showed that unconditionally \( g(p) = \Omega(\log \log p) \). Assuming
GRH one has \( g(p) > c(\log p)(\log \log p) \) for infinitely many primes \( p \) (see Montgomery \[328\], Theorem 13.5). An often studied quantity in the literature is \( p \), which is defined as the least quadratic non-residue modulo \( p \). For example in 1952, Ankeny \[10\] proved the important result that \( n_2(p) = O(\log^2 p) \) on GRH. This consequence of GRH has the important corollary of making Miller’s primality test polynomial time (cf. Bach \[20\]). Since clearly \( g(p) \geq n_2(p) \), any \( \Omega \)-result for \( n_2(p) \) will imply the same result for \( g(p) \).

Burgess and Elliott \[58\] have shown that

\[
\frac{1}{\pi(x)} \sum_{p \leq x} g(p) \ll \log^2 x (\log \log x)^4,
\]

improving on an earlier bound \( \log^4 x \) (with an unspecified \( A \)) of Burgess \[56\]. Cohen et al. \[101\] showed that in \((25)\) one can replace \( g(p) \) by \( h(p) \), thus improving on an earlier result of Burgess \[57\] to the effect that \( \pi(x)^{-1} \sum_{p \leq x} h(p) \ll \log^3 x (\log \log x)^6 \).

Murata \[369\] has shown that \( \pi(x)^{-1} \sum_{p \leq x} g(p) \ll \log x (\log \log x)^7 \), assuming the GRH, meanwhile the exponent 7 has been replaced by any number \( \gamma > 4 \) by Elliott and Murata \[136\].

Let \( D(i) \) be the density of primes \( p \) such that \( g(p) = i \). Elliott and Murata \[136\] proved under GRH that \( D(i) = \sum_M (-1)^{M-1} A_M \), where \( M \) runs over all the subsets of the set \( \{1, 2, \ldots, i\} \) containing \( i \), with \( A_M \) the density (under GRH) of primes \( p \) such that each \( a_i \in M \) is a primitive root modulo \( p \), as computed by K. Matthews \[324\]. This formula can be transformed using finite difference methods, into a form which allows one to prove that \( D(i) > 0 \) if \( i \) is not a power; see Buttsworth \[61, 62\]. Paszkiewicz and Schinzel \[410\] carried out extensive numerical work concerning \( D(i) \) for \( i \leq 32 \). Paszkiewicz did extensive computations to study whether or not \( g(p) = h(p) \). Litver and Yudina had computed in 1971 that \( g(p) = h(p) \) for \( p \in [2, 2^{32}] \) with the single exception of \( p = 40487 \). Paszkiewicz \[408\] showed that in the interval \([2^{32}, 10^{12}]\) there is one further such prime: \( p = 6692367337 \).

Let \( d > 1 \) be an integer. Linnik proved in 1944 the celebrated result that there is a constant \( c \) such that every reduced residue class modulo \( d \) contains a prime not exceeding \( d^c \). Subsequent proofs and improvements use, like Linnik, zero-free regions for \( L \)-series, zero density estimates for these and a quantitative version of the Deuring-Heilbronn phenomenon (for an introduction, see Stopple \[171\]). This also applies to Heath-Brown’s paper \[223\] in which he established \( c = 11/2 \). Recently T. Xylouris in his Diplomaarbeit (Bonn, 2009), established \( c = 5.2 \), see \[502\]. Elliott \[134\] gave a rather different proof in which as a ‘waystation’ (as he called it), he established the result that the least prime primitive root, \( q^*(p) \), to a prime modulus \( p \) does not exceed \( p^c \). In another paper Elliott \[131\] proved that \( g^*(p) < 475(\log p)^{8/5} \) infinitely often. Shoup \[458\], assuming GRH, gave a much sharper upper bound. G. Martin \[320\] showed that for all but \( O(Y^\epsilon) \) primes \( p \leq Y \) we have \( g^*(p) \ll \log^{C(\epsilon)} p \). Assuming GRH, Paszkiewicz and Schinzel \[409\] derived from the work of K.R. Matthews \[324\] a formula for the density \( E(q) \) of primes \( p \) for which \( g^*(p) = q \).
They computed $E(q)$ for the first 25 primes $q$. Bach [23] conjectured that

$$\limsup_{p \to \infty} \frac{g^*(p)}{(\log p)(\log \log p)^2} = e^\gamma.$$ 

Murata [369] showed that, under GRH, for any positive constant $D$ we have

$$|\{p \leq x : g^*(p) \geq D(\log p) \log \log p\}| \ll_D \frac{\pi(x)}{\log \log x}$$

and $g^*(p) = O(p^\epsilon)$ for almost all primes $p$.

A polynomial analogue of $g(p)$ also exists. There one can prove, as did Hsu [241], that there exists a $c > 0$ such that if $n \geq c \cdot \deg(P)/\log_q \deg(P)$, one can find at least one positive irreducible of degree $n$ which is a primitive root modulo $P$. Davenport [119] had proven much earlier that if $q$ (taken to be prime) is large enough with respect to $\deg(P)$, then there even exists a linear polynomial which is a primitive root.

Various authors [226, 227, 229, 230, 231, 488, 486] considered the least primitive root in number fields. For example, Hinz [225] generalized the Pólya-Vinogradov inequality to arbitrary algebraic number fields $K$. As an application he estimated the totally positive primitive root $\nu$ modulo a prime ideal $p$ of least norm and showed that it satisfies $N(\nu) \ll N(p)^{1/2+\epsilon}$. In a later paper [226] he improved this to $N(\nu) \ll N(p)^{1/4+\epsilon}$.

Dieulefait and Urroz [124] used results on $g(p)$ in order to study the malleability of RSA moduli. An encryption algorithm is malleable if it is possible for an adversary to transform a ciphertext into another ciphertext which decrypts to a related plaintext. That is, given an encryption of a plaintext $m$, it is possible to generate another ciphertext which decrypts to $f(m)$, for a known function $f$, without necessarily knowing or learning $m$.

These results on $g(p)$ immediately give an efficient search procedure for primitive roots, that is, lead to the construction a small set $S$ with at least one element that is a primitive root modulo $p$. Bach [23] gave a different search procedure, where the set $S$ has size $O(\log^4 p/(\log \log p)^3)$ and can also be constructed in polynomial time, assuming GRH. However, the set tends to have larger elements. (In writing this section I made grateful use of §2.2.4.3 in Narkiewicz’s book [388].)

28) Inverse primitive roots. Zhang [509] considered the distance between a primitive root $g$ with $1 \leq g \leq p - 1$ and its inverse, $\bar{g}$ (which is also a primitive root), with $1 \leq \bar{g} \leq p - 1$. For about 75% of the primitive roots $g$ modulo $p$ in $[1, p]$, one has that $|g - \bar{g}| \leq p/2$.

29) Consecutive primitive roots. Vegh, see, e.g., [480], wrote a series of papers on consecutive primitive roots and primitive roots in arithmetic progression. Mozingo [331], using elementary arguments, showed that the only positive integers $> 1$ having all their primitive roots consecutive are 2, 3, 4, 5 and 6.
30) **Average multiplicative order.** J. von zur Gathen et al. [172] defined $u(n)$ to be the average multiplicative order of the elements of $(\mathbb{Z}/n\mathbb{Z})^*$. Note that $u(n) \leq \lambda(n)$. They proved various results comparing $u(n)$ with $\lambda(n)$, see also [312, 313, 343].

31) **Smooth orders.** An integer is said to be “$y$-smooth” (or “$y$-friable”) if none of its prime factors exceed $y$. The distribution of smooth integers is by now very well understood; for a survey up to 1993 see Hildebrand and Tenenbaum [224]. A more recent survey is due to Granville [189]. Banks et al. [34] established some results on the smoothness of the order function, thus improving upon earlier results by Pomerance and Shparlinski [424].

32) **Distribution of $\varphi(p-1)/(p-1)$.** Trivially $\varphi(p-1)/(p-1) \leq 1/2$ if $p$ is odd. For any real numbers $x \geq 2$ and $u$, let

$$D(x, u) = \frac{1}{\pi(x)} \sum_{\varphi(p-1)/(p-1) \leq x} 1.$$  

Elliott [132] proved that the limit $\lim_{x \to \infty} D(x, u) = D(u)$ exists for all real numbers $u$. The function $D(u)$ turns out to be continuous and is strictly increasing on the interval $[0, 1/2]$. Schoenberg [150], see also Kac [250], had earlier considered the distribution problem for $\varphi(n)/n$ and proved the existence of the analogue of $D(u)$ and its continuity as a function of $u$. Li [301] considered the analogue of $D(x, u)$ with $R(n)/\varphi(n)$ as function, with $R(n)$ the number of primitive $\lambda$-roots in $[1, n]$. He showed for example that in this case there exists $u_0 > 0$ such that for every $u$ in $(0, u_0)$ the function $D(x, u)$ does not have a limit as $x \to \infty$.

In the stochastic model proposed by Esseen [149] the sum

$$\sum_{p \leq x} \left( \frac{\varphi(p-1)}{p-1} \right)^k$$

with $k \geq 1$ an integer played an important role. Without proof Esseen stated an asymptotic for this sum, namely that the latter sum is asymptotic to $A'_r \text{Li}(x)$ with $A'_r$ as in §9.7.2. A proof was given much earlier by Vaughan [479, Lemma 4.4]. An easier proof was given by Holden and Moree [236] (following a suggestion of Pomerance).

If in the latter sum we sum over integers $n \leq x$ we have (see [330, p. 42])

$$\sum_{n \leq x} \left( \frac{\varphi(n)}{n} \right)^k = x \prod_q \left( 1 - \frac{1}{q^k} (1 - \frac{1}{q}) \right) + O(x^\epsilon).$$

Vaughan [479] studied the average relative density of primitive roots mod $p$ versus non-primitive roots mod $p$,

$$\frac{1}{\pi(x)} \sum_{2 < p \leq x} \frac{\varphi(p-1)}{p-1 - \varphi(p-1)},$$

by relating it to the above ‘Esseen sums’.
33) **Cubic reciprocity primitive root criteria.** Chebyshev’s criterium we mentioned in the introduction only involves quadratic reciprocity. Fueter [166] formulated some criteria which also make use of cubic reciprocity. He proved for example that if \( p \) is a prime of the form \( p = 1 + 2^{2n}3^m+3 \), with \( n > 0 \) and \( m \geq 0 \), then 5 is a primitive root modulo \( p \) iff \( m \equiv n \pmod{2} \).

34) **Coding theory.** In coding theory sometimes the multiplicative order arises. See, e.g., [38, 123, 183, 206, 252, 293, 357, 421, 427, 431, 432] and cf. §9.4.2. For example Lenstra applied his methods from [292] to yield existence theorems, assuming GRH, for perfect, one-error-correcting arithmetical codes, cf. [185, 293].

35) **Hooley-Heath-Brown Hybrids.** There are various results which are hybrid between Hooley’s result and Heath-Brown’s unconditional result in the sense that under an assumption weaker than GRH a conclusion weaker than Hooley’s is established, but stronger than Heath-Brown’s. For example Nongkynrih [392] proved that if for every squarefree integer \( k \) the Dedekind zeta function \( \zeta_K(s) \) of the field \( K = \mathbb{Q}(\zeta_k, 2^{1/k}) \) is zero free in \( \text{Re}(s) > 1 - e^{-12A/5} - \delta \), then 2 is a primitive root for a positive proportion of primes. For other examples, see Cojocaru [103, 104] and Ram Murty [373].

36) **Polynomials representing primitive roots.** Let \( f \) be a polynomial over a finite field. Is there a primitive root in its image? Madden [318] proved that for almost all finite fields \( k \), every squarefree polynomial of degree \( l \) over \( k \) represents a primitive root in \( k \). Let \( f_1(x), \ldots, f_r(x) \) be polynomials modulo \( p \), which are squarefree and relatively prime in pairs. Carlitz [67] gave an asymptotic formula for the number of \( x \pmod{p} \) for which each of \( f_1(x), \ldots, f_r(x) \) is a primitive root. The best results to date in this direction are due to S. Cohen [98].

37) **Permutations and primitive roots.** Consider the permutation

\[
(1, 2)(1, 2, 3) \ldots (1, 2, \ldots, m)
\]

(multiplication of cycles from right to left), then (for a proof see [19]) the product is a single cycle containing all of 1, 2, \ldots, \( m \) iff 2\( m + 1 \) is a prime number having 2 as primitive root.

To a primitive root \( g \) modulo \( p \) we associate the permutation \( \sigma_g \) of \( X \) defined by \( \sigma_g(x) \equiv g^x(\pmod{p}) \). More precisely, \( \sigma_g(x) = y \), the unique element in \( \{1, 2, \ldots, p-1\} \) satisfying \( y \equiv g^x(\pmod{p}) \). For example, if \( p = 7 \), then \( \sigma_5 = (1 5 3 6)(2 4) \). Lewittes and Kolyvagin [300] determined the parity \( s(\sigma_g) \) of the permutation \( \sigma_g \). Assume \( p > 3 \) and put \( w = ((p - 1)/2)! \). Then

\[
s(\sigma_g) = \begin{cases} 
-wg^{(p-1)/4}(\pmod{2}) & \text{if } p \equiv 1(\pmod{4}) ; \\
-w(\pmod{2}) & \text{if } p \equiv 3(\pmod{4}) .
\end{cases}
\]

In case \( p \equiv 1(\pmod{4}) \), using Wilson’s theorem one sees that \( \pm w \) are precisely the two roots of \( X^2 + 1 \equiv 0(\pmod{p}) \). On the other hand, \( \pm g^{(p-1)/4} \) are also roots modulo
p. The above results allows one to equate these roots.

In case $p \equiv 3 \pmod{4}$, the congruence can be rewritten as $s(\sigma_g) \equiv h_{\mathbb{Q}(\sqrt{-p})}(\mod{4})$, using Mordell’s [332] result that $w \equiv (-1)^a(\mod{p})$, with $a = (1 + h_{\mathbb{Q}(\sqrt{-p})})/2$.

38) Perfect card shuffling. Consider an even number of cards numbered 0 to $2k - 1$, with 0 the top card. Then a perfect card shuffle takes a card in position $i$ and sends it to $2i(\mod{2k - 1})$. If the cards continue to be perfectly shuffled, the deck returns to the order it was in before the first shuffle. For example, if one takes a deck of 52 cards, cut it in half, and perfectly shuffles it (with the bottom card staying at the bottom), then it returns after 8 times to its starting order. Thus Shuf(52) = 8. In general let Shuf(2k) be the least number of perfect shuffles that will return a deck of 2k cards to its starting order. It is not difficult so show that Shuf(2k) = ord$_{2k-1}(2)$, cf. [436].

To wit, she that can card shuffle can do algebraic number theory, as the level (see §9.4.3 for the definition) of the cyclotomic number field $\mathbb{Q}(\zeta_{2k-1})$ can be determined using the parity of Shuf(2k). This level is 4 if Shuf(2k) is odd, and 2 otherwise.

39) Parabolic generators of $\Gamma(p)$. Frasch [163] has shown that $\Gamma(p)$, the principal congruence subgroup of the modular group $\Gamma$ modulo a prime $p$, can be generated as a free group by the generators $S^p = (1 \ 0 \ 1 \ 0)^p$ and $(p - 1)p(p + 1)/12$ other generators. Recall that $g(p)$ is the smallest primitive root modulo $p$ (cf. §9.7.27). Grosswald [196] has shown that if $g(p) < \sqrt{p} - 2$, then these $(p - 1)p(p + 1)/12$ generators can be chosen in such a way that they are all parabolic. In a later paper, [197], he showed that for all $p$ sufficiently large we have $g(p) < \sqrt{p} - 2$.

40) Pseudopowers. An $x$-pseudopower to base $g$ is a positive integer which is not a power of $g$, yet is so modulo $p$ for all primes $p \leq x$. Let $q_g(x)$ denote the least $x$-pseudopower to base $g$. Bach et al. [25] proved that if RH holds for Dedekind zeta functions, then there is a constant $A > 0$, depending only on $g$ such that $q_g(x) \geq \exp(A\sqrt{x}\log^{-2}x)$. Estimating $q_g(x)$ is closely related to determining the behaviour of the order on average. Using upper bounds of Baker and Harman [26] for the Brun-Titchmarsh inequality on average (see also the book by Harman [213]) and new bounds on exponential sums, Konyagin et al. [263] showed that $q_g(x) \leq e^{0.88715x}$ for $x$ sufficiently large and $|g| \leq x$. This improved upon the upper bound $q_g(x) \leq e^{(1+o(1))x}$ due to Bach et al. [25]. In the course of the proof the authors showed that $\prod_{p \leq x, p \nmid g} \text{ord}_p(g) \geq e^{0.58045x}$ for $x$ sufficiently large and for $g$ an integer with $2 \leq |g| \leq x$. Recently the result by Konyagin et al. was improved by Bourgain et al. [13] who showed that $q_g(x) \leq e^{0.86092x}$ for $x$ sufficiently large and $|g| \leq x$.

41) Ducci sequences. The Ducci-sequence generated by $X := (x_1, \ldots, x_n) \in \mathbb{Z}^n$ is the sequence $(X, D(X), D^2(X), \ldots)$ where $D : \mathbb{Z}^n \to \mathbb{Z}^n$ is defined by $D(x_1, \ldots, x_n) = (|x_1-x_2|, |x_2-x_3|, \ldots, |x_n-x_1|)$. Every Ducci sequence $(X, D(X), D^2(X), \ldots)$ gives rise to a cycle; there are integers $i$ and $j$ with $0 \leq i < j$ with $D^i(X) = D^j(X)$. When
in \( \mathbb{G} \) other than \( 1 \).

Shparlinski [165] showed that under GRH for any fixed \( 1 \leq D \leq 2 \), Ducci sequences, primitive polynomials and Artin’s primitive root conjecture. They proved for example that if \( p \) is a prime and 2 is a primitive root modulo \( p \), then Ducci-sequences of length \( p \) have only one period other than 1.

Breuer [48] introduced Ducci sequences over abelian groups. They are sequences \( U, D(u), D^2(u), \ldots \in \mathbb{G}^n \), where \( D(u_1, u_2, \ldots, u_n) = (u_1 + u_2, u_2 + u_3, \ldots, u_n + u_1) \).

In [49] he proved that in case \( G = (\mathbb{Z}/p^{10}) \) and \( p \nmid n \), the maximal period of a Ducci sequences, \( P_p(n) \), divides \( p^{t-1}(p^{\text{ord}_p(n)} - 1) \) and \( p^{t-1}n(p^{\text{ord}_p(n)/2} - 1) \) if \( \text{ord}_p(n) \) is even. Furthermore, he showed that \( P_p(2) = \text{ord}_p(2) \).

42) **Divisible trinomials.** Golomb and Lee [184] considered irreducible polynomials which divide trinomials in \( \mathbb{F}_2 \). In their considerations \( \text{ord}_p(2) \) played an important role. They proved for example that if \( \Phi_p(x) = \frac{x^p - 1}{x - 1} = f_1(x)f_2(x) \cdots f_r(x) \) is a product of \( r \) irreducible polynomials, \( r \) is even and \( p > 7r/2 \), then the \( f_i(x) \)’s divide no trinomials. Note that \( r = (p - 1)/\text{ord}_p(2) \). In this context Golomb made a conjecture on near-primitive roots that subsequently turned out to be false; see [355].

43) **Sidelnikov primes.** In the theory of pseudo-random sequences, there is some interest in finding prime powers \( q \), such that \( q - 1 \) has a large prime divisor \( r \) such that 2 is a primitive root modulo \( r \). Let \( P(x, y) \) be the number of primes \( p \in (x, 2x] \) such that \( p - 1 \) has a divisor \( r \geq y \) satisfying \( \text{ord}_r(2) = r - 1 \). Friedlander and Shparlinski [105] showed that under GRH for any fixed \( 1/2 \leq \alpha < 17/32 \),

\[
P(x, x^\alpha) \geq (A \log(17/32\alpha)/100 + o(1)) \frac{x}{\log x}.
\]

44) **Diffie-Hellman triples.** Let \( g \) be a primitive root modulo \( p \). Canetti et al. [64] proved that the triples \( (g^x, g^y, g^{xy}) \), \( x, y = 1, \ldots, p - 1 \), are uniformly distributed modulo \( p \) in the sense of H. Weyl. In cryptography it is often assumed that the triples \( (g^x, g^y, g^{xy}) \) cannot be distinguished from totally random triples in feasible computation time. The above result implies that this is in any case true for a constant fraction of the most significant bits, and for a constant fraction of the least significant bits.

45) **Carmichael numbers in number rings.** If \( a^n \neq a \pmod{n} \), for some integer \( a \), then \( n \) is composite. This is a rudimentary Compositeness Test. However, there are some \( n \) for which this test fails, no matter how we pick \( a \). A **Carmichael number** is a composite integer \( n \) such that \( a^n \equiv a \pmod{n} \) for all integers \( a \). The smallest such number is 561. It turns out that there are infinitely many Carmichael numbers, see [9]. Steele [465] defined a **Carmichael ideal** to be a composite ideal \( n \) such for \( \alpha \in \mathcal{O}_K \), we have \( \alpha^{N(n)} \equiv \alpha \pmod{n} \). Using Heath-Brown’s result that all primes, with the possible exception of at most two are primitive roots for infinitely many primes \( p \), Steele [465] showed that if the integer \( n \) is the product of at least three distinct primes, then there exist infinitely many cyclotomic extensions \( \mathbb{Q}(\zeta_q) \), such
that $n$ is not Carmichael in $\mathbb{Q}(\zeta_q)$.

46) **Common primitive root.** Let $\prod_{i=1}^{r} p_i^{\ell_i}$ be the canonical prime factorisation of an integer $n$. Finizio and Lewis [158] called an integer $m$ a common primitive root if $m$ is a primitive root modulo $p_i^{\ell_i}$ for $1 \leq i \leq r$.

47) **Mapping the discrete logarithm.** A functional graph is a directed graph such that each vertex must have exactly one edge directed out from it. If $S$ is a finite set and $f : S \rightarrow S$ a mapping, then one can associate a functional graph to the mapping $f$ by interpreting each element in $S$ as a vertex. The edges are defined such that an edge $(a,b)$ is in the graph iff $f(a) = b$. Cloutier and Holden [91] considered the functional graph associated to the mapping $x \rightarrow g^x$ modulo $p$, with $p$ a prime and $S = \{1, 2, \ldots, p-1\}$. They computed various statistics of this graph and compared them with those of a random mapping.

48) **Hilbert $p$-class field towers.** Furuta [167] and B. Schmidt [449] proved results relating the multiplicative order to sufficiency criteria for the existence of Hilbert $p$-class field towers of $\mathbb{Q}(\zeta_m)$. For example, Schmidt proved that if $m = kq$, where $k$ is an integer, and $q$ is a prime with $q \equiv 1 \pmod{p}$, $(k,q) = 1$ and $q^n \not\equiv -1 \pmod{k}$, for $n = 1, 2, \ldots$, and also such that $\varphi(k)/\text{ord}_q(q) \geq 8p + 12$, then $\mathbb{Q}(\zeta_m)$ has an infinite Hilbert $p$-class field tower. Shparlinski [460] used the latter result to show that for infinitely many $m$ there is an infinite Hilbert $p$-class field tower over $\mathbb{Q}(\zeta_m)$ for some $p \geq m^{0.3385 + o(1)}$. Furthermore, he used the result of Furuta [167] to show that for almost all positive integers $m$, $\mathbb{Q}(\zeta_m)$ has an infinite Hilbert $p$-class field tower with high rank Galois groups at each step, simultaneously for all primes $p$ to size up to about $(\log \log m)^{1+\varepsilon}$. As a consequence, Shparlinski inferred that for all $m \leq x$, with $x$ large enough, except possibly $O(x(\log \log x)^{-0.08})$ exceptions, the class number of $\mathbb{Q}(\zeta_m)$ is divisible by all primes $p \leq \log \log x/(10 \log \log \log x)$.

49) **Cunningham chains.** Let $p_1, \ldots, p_k$ be a chain of primes such that for $2 \leq j \leq k$ we have $p_j = 2p_{j-1} + 1$; that is we have

$$p_j = 2^{j-1}p_1 + 2^{j-1} - 1 = 2^{j-1}(p_1 + 1) - 1. \quad (26)$$

Such a chain of primes is known as a Cunningham Chain. A basic example is 2, 5, 11, 23, 47, while the longest one known is the Cunningham Chain with $k = 16$ and $p_1 = 810433818265726529159$, discovered by Carmody and Jobling in 2002. Let $k(p)$ be the length of the longest Cunningham Chain starting from $p$. One has $k(p) = 1$ for all primes $p \leq x$, except for $O(x \log^{-3} x)$ of them. (This follows by a standard upper bound for Sophie Germain primes coming from sieve theory.) By the first equality in (26) and Fermat’s little theorem we find $k(p) \leq \text{ord}_p(2)$. Conditionally one can do far better than this. Assuming that $\mathcal{P}(2)(x) \sim A\pi(x)$, which by Hooley’s result is true under GRH, Ford et al. [160] have shown that

$$\limsup_{p \to \infty} \frac{k(p)}{\log p} \leq \frac{1}{A}. \quad (27)$$
50) **Dynamical systems and Artin.** Let $k$ be an A-field. Denote by $P(k)$ the set of all places of $k$. Let $P_\infty(k)$ denote the set of Archimedean places if $k$ is a number field or the set of infinite places if $k$ is a function field of transcendence degree one over a finite field. Suppose one is given an element $\xi \in k^*$, and any set $S \subset P(k) \subseteq P_\infty(k)$ such that $\xi$ is integral for all $w \notin S \cup P_\infty(k)$. The dual group of the $S$-integers $R_S$, denoted by $X$, is a compact abelian group. Let $\alpha: X \to X$ be a continuous group endomorphism which is the dual of the monomorphism $\widehat{\alpha}: R_S \to R_S$ given by $\widehat{\alpha}(x) = \xi x$. Dynamical systems of the form $(X, \alpha) = (X(k, S), \alpha(k, S, \xi))$ are called $S$-integer dynamical systems. These were introduced in Chothi et al. [90]. The authors show, for example, that if the qualitative version of Artin’s conjecture holds, then there exist examples with uniformly distributed periodic points.

In [491] (building on an earlier paper [490]) Ward considers a family of isometric extensions of the full shift on $p$ symbols (with $p$ a prime) parametrized by a probability space. Using Heath-Brown’s work [222] on the Artin conjecture, he shows that for all but two primes $p$ the set of limit points of the growth rate of periodic points is infinite almost surely. This shows in particular that the dynamical zeta function is not algebraic almost surely.

51) **Converse theorems and Artin.** Associated to a newform $f(z)$ is a Dirichlet series $L_f(s)$ with functional equation and Euler product. Hecke showed that if the Dirichlet series $F(s)$ has a functional equation of a particular form, then $F(s) = L_f(s)$ for some holomorphic newform $f(z)$ on $\Gamma(1)$. Weil extended this result to $\Gamma_0(N)$ under an assumption on the twists of $F(s)$ by Dirichlet characters. Farmer and Wilson [152] take another approach by also making the assumption that $L_f(s)$ has an Euler factor at the prime 2:

$$L(s, f) = (1 - a_2 2^{-s} + 2^{k-1-2s}) \sum_{2 \nmid n} \frac{a_n}{n^s}.$$  

Their main result has various conditions, one being a weak form of the Artin conjecture, described in §10.36, that ensures that a certain subset of matrices of $\Gamma_0(N)$ actually is a generating set for $\Gamma_0(N)$.

52) **Finding $M$ from a string of $g$-ary digits of $1/M$.** It has been shown by Blum et al. [40] that given $k = 2L + 3$ successive digits of the $g$-ary expansion of $1/M$, one can find $M$ in polynomial time $L^{O(1)}$. On the other hand, under Artin’s conjecture, it is also shown in [40] that $k = L - 1$ digits are not enough to determine $M$ unambiguously. Konyagin and Shparlinski [264] proved that for any $\epsilon > 0$, given a string of $k = [(3/37 - \epsilon)\epsilon]L$ consecutive $g$-ary integers, there are at least $(1 + o(1))\pi(g^L)$ prime numbers $p < g^L$ such that the $g$-ary expansion of $1/p$ contains this string. Recently Bourgain et al. [44] showed that the $\frac{3}{37} = 0.0810\ldots$ can be replaced by $\frac{41}{504} = 0.0813\ldots$. 
53) \textit{Fermat quotients.} For a prime $p$ and and integer $u$ with $p \nmid u$, the Fermat quotient is defined by the condition

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p}, \quad 0 \leq q_p(u) \leq p - 1.$$ 

It has the property that $q_p(uv) \equiv q_p(u) + q_p(v) \pmod{p}$. It is expected that the map sending $u$ to $q_p(u)$ behaves very similarly to a random map on the set $\{0, \ldots, p - 1\}$. For results in this direction see \[396\]. Let $l_p$ be the smallest positive integer $a$ such that $p \nmid q_p(a)$. It might be true that $l_p \leq 3$. Bourgain et al. \[42\] have shown that $l_p \leq \log^{463/252+o(1)} p$ as $p$ tends to infinity. As a consequence, they derive a stronger version of Lenstra’s squarefree test. Shparlinski \[461\] shows that for every $p$ there exists $n \leq p^{3/4+o(1)}$ such that $q_p(n)$ is a primitive root modulo $p$.

54) \textit{Sums of squares of primitive roots modulo $p$.} Let $p \nmid c$ be an integer and let $M(p, c)$ be the number of solutions of the congruence $r^2 + s^2 \equiv c \pmod{p}$ with $1 \leq r, s \leq p - 1$ primitive roots. Zhang \[508\] shows that

$$M(p, c) = \frac{\phi^2(p-1)}{p} + O\left(\frac{\phi^2(p-1)}{(p-1)^2} \sqrt{p^{4\omega(p-1)}}\right).$$

55) $G(n)$. Let $G(n)$ be the least integer $G$ such that $\{y : 1 \leq y \leq G \text{ and } (y, n) = 1\}$ generates $(\mathbb{Z}/n\mathbb{Z})^*$. Any good upper bound for $G(n)$ would have implications for deterministic primality testing. Assuming GRH, Montgomery \[328\] showed that $G(n) = O(\log^2 n)$, which was made effective by Bach \[21\] who showed that $G(n) \leq 3 \log^2 n$ for $n \geq 2$. As to unconditional results: Bach and Huelsbergen \[24\] showed that $G(n) = O(\sqrt{n} \log(n) \log \log n)$, which was sharpened byBURTHE to $G(n) \leq n^{\alpha + \epsilon}$, where $\alpha = 1/(3\sqrt{e}) = 0.20217\ldots$. The proof is based on the formula $G(n) = \max\{\min\{a : \chi(a) \neq 0 \text{ and } \chi(a) \neq 1\}\}$, where $\chi$ runs over the non-principal Dirichlet characters modulo $n$. Norton \[393\] improved Burthe’s bound to $G(n) \leq n^{\beta + \epsilon}$, where $\beta = 1/(4\sqrt{e}) = 0.15163\ldots$. Bach and Huelsbergen \[24\] conjectured that

$$\limsup_{n \to \infty} \frac{G(n)}{\log n \log \log n} = \frac{1}{\log 2} \quad \text{and} \quad \frac{1}{x} \sum_{n \leq x} G(n) \sim (\log \log x) \log \log \log x.$$ 

Using zero density estimates Burthe \[60\] showed that $x^{-1} \sum_{n \leq x} G(n) = O(\log^{97} x)$.

Note that if $n$ is prime, $G(n)$ is bounded below by the least quadratic nonresidue of $n$, and above by the least primitive root of $n$. In this case $G(n) = \kappa(n)$, with $\kappa(n)$ defined as in Section §9.7.2.

56) \textit{Other Artin surveys.} For a much shorter introduction to Artin’s primitive root conjecture see Ram Murty \[372\]. Li and Pomerance have written a survey with special emphasis on $\lambda$-roots, see \[306\]. Cheng \[74\] wrote a survey on algorithms for finding primitive roots. Konyagin and Shparlinski \[264\] considered in their book various questions related to the distribution of integer powers $g^x$ for some integer $g > 1$ modulo a prime $p$. 

10. Open Problems

1) Remove the GRH assumption that is made in many results in this area.

2) The two papers of Holden and Moree $[235, 236]$ contain various open problems. Two of these have meanwhile been solved by Shparlinski; see §9.7.7.

3) Study the average behaviour of ranks in other families of elliptic curves than those considered by Ulmer (see §9.6.13), for example those appearing in Darmon $[118]$.

4) Let $g_1, \ldots, g_t$ denote the primitive roots modulo $p$. The Dence brothers $[122]$ considered symmetric functions in the primitive roots of primes. They considered for example $s_2(p) = \sum_{1 \leq i < j \leq t} g_i g_j$ and show that this quantity, when considered modulo $p$, assumes only values in $\{-1, 0, 1\}$. They wondered about the density $\delta(j)$ of primes for which, say $s_2(p) \equiv j \pmod{p}$. The author conjectures that $\delta(-1) = A/4$, $\delta(0) = 1 - A$ and $\delta(1) = 3A/4$. In general one has the following problem: given a symmetric function in the primitive roots, which values are assumed and with what frequency? For some partial progress see Moree and Hommersom $[356]$.

5) Guy $[207, \text{Section F9}]$ formulated some unsolved problems regarding primitive roots.

6) Find a lower bound, $b(p)$, say, such that $\mathrm{ord}_p(2) > b(p)$ for almost all $p$ (i.e. for all but $o(x/\log x)$ primes $p \leq x$), as $x$ tends to infinity. Erdős $[142]$ proved that one can take $b(p) = p^{1/2-\delta}$. This was later improved by Erdős and Ram Murty $[144]$ to $b(p) = p^{1/2+\epsilon(p)}$ for any function $\epsilon(p) \to 0$. They also proved that under the assumption of GRH for the Dedekind zeta function of $\mathbb{Q}(\zeta_d, 2^{1/d})$ one can take $b(p) = p/f(p)$ where $f(x)$ is any function that tends to infinity as $x \to \infty$. For related results see Indlekofer and Timofeev $[244]$ and Pappalardi $[401]$. For a subgroup $\Gamma$ of rank $r \geq 1$ of $\mathbb{Q}^*$, Erdős and Ram Murty $[144]$ and Pappalardi $[401]$ considered the problem of finding a lower bound $b(p)$, for almost all $p$, such that $|\Gamma_p| > b(p)$, where $\Gamma_p$ is the reduction mod $p$ of $\Gamma$. Again they proved that under GRH one can take $b(p) = p/f(p)$ where $f(x)$ tends to infinity. See Elsholtz $[138]$ for a related result. Unconditionally Pappalardi proved that for almost all primes $p$ one can take $b(p) = p^{\tau/r+1}\exp(\log^\tau p)$ for some $\tau \approx 0.15$. The analogous problems for subgroups of the group of rational points of CM elliptic curves were considered by Akbary $[3]$, and Akbary and Kumar Murty $[7]$. For an elliptic curve $E$ defined over $\mathbb{Q}$ and a subgroup $\Gamma$ of rank $r$ of the group of rational points of $E$, Akbary, Ghioca, and Kumar Murty $[6]$ proved that, under GRH, one can can take $b(p) = p/f(p)$ as long as $r > 18$ (for non-CM curves) or $r > 5$ (for CM curves). The problem remains open for lower ranks. Duke $[127]$ considered the problem of finding a lower bound, for almost all $p$, for the exponent of reduction modulo $p$ of an elliptic curve $E$ and proved (under GRH) that for almost all primes $p$, the group of rational points of and $E \mod p$ contains a cyclic subgroup of order at least $p/f(p)$. A related dynamical
interpretation for the size of reduction mod $p$ of the orbit of a point on a quasiprojective variety under the action of a monoid of endomorphisms of the variety proposed by Akbary and Ghioca [4]. Related questions in a more general context of algebraic groups and abelian varieties were considered by C. Matthews [323]. He mentioned further applications to nilpotent groups and to manifolds due to Milnor, Tits and Wolf.

In the paper of Erdős [142] mentioned above, he conjectured that if $c < 1$ one can take $b(p) = p^c$. If one could take $c = 0.8$ this would imply a conjecture of Skalba [163] to the extent that almost all primes occur as prime divisors of the numbers $2^a + 2^b + 1$. Under GRH it follows by a result of Pappalardi [401, Theorem 2.3] that we indeed can take $c = 0.8$. In the same paper Skalba conjectured that there are infinitely many primes $p$ such that $p$ does not divide any number of the form $2^a + 2^b + 1$. It is easy to see that this set includes all Mersenne primes. Skalba showed that if $\Omega(2^m - 1) < \log m / \log 3$, then there exists a prime divisor $q$ of $2^m - 1$ such that $q$ is not a divisor of $2^a + 2^b + 1$ for any positive integers $a$ and $b$. Luca and Stanica [315] conjecture that $\omega((a^n - 1)/(a - 1)) \geq (1 + o(1))(\log n)(\log \log n)$ for almost all integers $n$ and give heuristic arguments to support this. Their conjecture, if true, implies that the integers $m$ satisfying Skalba's condition $\Omega(2^m - 1) < \log m / \log 3$ are not typical. Skalba [163] conjectures that there are infinitely many primes $q$ such that $q$ does not divide any number of the form $2^a + 2^b + 1$.

7) Roskam [438] raised the following questions and demonstrated their applications to the study of divisors of general linear recurrences: let $f \in \mathbb{Z}[X]$ be an irreducible monic polynomial, $\alpha$ a root of $f$, and define $K = \mathbb{Q}(\alpha)$ with ring of integers $\mathcal{O}_K$. Furthermore, let $T$ be the set of primes that are inert in $K/\mathbb{Q}$, and define for each $h \geq 1$ the set $T_h$ of primes $p$ in $T$ for which the subgroup $\langle \alpha \rangle \subset (\mathcal{O}_K/p\mathcal{O}_K)^*$ has index $h$. Is it true for generic $\alpha$ that $T_h$ has a natural density $\delta(T_h)$? Is it true that $\sum_{h=1}^{\infty} \delta(T_h) = \delta(T)$? Earlier Brown and Zassenhaus had made a similar conjecture [52].

8) Let $q$ be an odd given prime power and $m$ a natural number. One can wonder whether there exists an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ such that $\mathbb{F}_{q^n}$ has an optimal normal basis over $\mathbb{F}_q$. A number theoretic question that arises in this context, see [32], is whether there is a prime $p$ such that $p \equiv 1 \pmod{m}$, and $q$ is a primitive root modulo $p$, and if yes to provide a small upper bound for the smallest such prime. The latter part of the question seems very difficult (it is already a very hard problem to find a bound for the smallest prime $p$ such that $p \equiv 1 \pmod{m}$, see, e.g., Heath-Brown [223]), but it should be possible to shed some light on the first part of the question.

9) For a given odd prime $l$ and prime power $q$, Ballot [29] has computed the Dirichlet density of primes $P$ of $\mathbb{F}_q[X]$ such that $l$ divides the order of $X(\pmod{P})$, by an elementary method using neither Kummer theory, nor the Chebotarev Density Theorem. In an earlier paper Ballot [28] considered this problem for the case $l = 2$. Can one likewise compute the Dirichlet density of primes $P$ such that the order of
X (mod P) is in a prescribed arithmetic progression? Indeed, in this setting one can wonder whether the Dirichlet density is the ‘good density’ to consider. For a lively discussion of this problem see Ballot [30].

10) Let K be a number field, F/K a Galois extension and C a union of conjugacy classes of Gal(F/K). Furthermore, let \( \alpha \neq 0 \) be an algebraic integer in a number field K which is not a root of unity. In [512], Ziegler was interested in the set \( P(\alpha, K, F, C, a, d) \) of primes \( p \) of K such that \( (p, F/K) \in C \), \( p \nmid \alpha \), and \( \text{ord}_p(\alpha) \equiv a(\text{mod} \, d) \), where \( (p, F/K) \) denotes the Frobenius automorphism of \( p \), and \( \text{ord}_p(\alpha) \) denotes the order of the algebraic integer \( \alpha \) in \( O/pO \), \( O \) being the ring of integers of K. Ziegler [512] showed assuming GRH that this set has a natural density that can be given as a double sum involving field degrees and Galois intersection coefficients. In the case \( K = \mathbb{Q} \) his result simplifies to results proven by Moree [347]. In the sequel to the latter paper, [348], Moree showed that there is a ‘generic’ density, and that almost always the density equals the generic density. Do similar results hold for the more general case considered by Ziegler as well?

11) Moree [351] gave an asymptotically exact heuristic for the number of primes \( p \leq x \) dividing a sequence of the form \( \{a^k + b^k\}_{k=1}^\infty \). These numbers satisfy a linear recurrence of degree 2. Is it possible to derive an asymptotically exact heuristic for the number of primes \( p \leq x \) dividing a linear recurrence of degree 2 consisting of integers only?

12) Let \( g \) be a primitive root modulo \( p \). How large is the smallest \( N \) such that any residue class modulo \( p \) is representable in the form \( g^x \mod p \) with \( 1 \leq x, y < N \)? This question is attributed to Odlyzko, who conjectured that one can take \( N \) as small as \( p^{1/2+\epsilon} \), for any fixed \( \epsilon \) and \( p \) large enough in terms of \( \epsilon \). Rudnick and Zaharescu [140] proved that one can take \( N = c_0 p^{3/4} \log p \), and this was sharpened by Cuauhtémoc Garcia [116] to \( N = 2^{5/4} p^{3/4} \). Using properties of Sidon sets the latter estimate was improved to \( N = (\sqrt{2} + \epsilon) p^{3/4} \) by Cilleruelo [83] (with \( p > p(\epsilon) \)) and more recently by Cilleruelo and Zumalacárregui [84] to \( N = \sqrt{2} p^{3/4} \) for every prime \( p \). For related papers on the distribution of small powers of a primitive root see [92, 329, 477].

13) Grosswald [197] wrote that an inspection of tabulated values of \( g(p) \), the smallest positive primitive root modulo \( p \), strongly suggests that \( g(p) < \sqrt{p} - 2 \) for all primes \( p > 409 \). He proved that \( g(p) < p^{0.499} \) if \( p - 1 \geq e^{24} \). Can one lower this lowerbound? (Andrew Booker, personal communication, suggested the answer is yes and even substantially so.) For an application of this bound see §9.7.39.

14) Cat maps are maps of the unit torus given by \( 2 \times 2 \) matrices with integer entries, unit determinant, and real eigenvalues. The chaotic nature of these maps is traditionally depicted by showing what the map does to the face of a cat (after several iterations). The cat map models chaotic components of phase space in Hamiltonian
systems. In the analysis of its periodic orbits the order of the cat map modulo \( p \) plays an important role. Keating \cite{255} studied these aspects using heuristic arguments. Meanwhile a much more rigorous treatment using for example the methods in Kurlberg’s paper \cite{272} is possible. As a working title for this project the author proposes: Cat maps: the dogged approach. (See also §9.7.10 and \cite{128, 412}.)

15) In connection with a question related to codes, Rodier \cite{431} was interested in computing the density of primes \( p \equiv 7 (\text{mod } 8) \) such that the subgroup in \((\mathbb{Z}/p\mathbb{Z})^*\) generated by 2 is of index 2. He argued that assuming GRH the density is \( A/2 \). Recently, Peter Malicky independently in connection with work on the periodic orbits of a certain 2-dimensional dynamical system asked about the infinitude of this set of primes. More generally one might ask for an explicit evaluation of the density of primes \( p \equiv a (\text{mod } f) \) such that the subgroup in \((\mathbb{Z}/p\mathbb{Z})^*\) generated by \( g \) is of index \( t \).

16) Brauer \cite{47} showed that the infinitely many primes \( p \equiv 9 (\text{mod } 16) \) which can be represented as \( 65x^2 + 256xy + 256y^2 \) are all non-divisors of the sequence \( \{2^k + 1\}_{k=1}^\infty \). Can this be generalized?

17) Transposition invariant words. In the context of a problem of words invariant under certain transpositions, Lepistő et al. \cite{297} prove that there are infinitely many primes \( p \) such that there is a primitive root mod \( p \) that divides \( p+1 \). They conjectured that this set of primes has a density \( B \geq 0.65 \) that should be exactly computable assuming GRH.

18) Nagata \cite{383} raised a question on \( \mathbb{Z}[\sqrt{14}] \). A positive answer would give a proof different from Harper’s \cite{214} that \( \mathbb{Z}[\sqrt{14}] \) is Euclidean.

19) Granville and Soundararajan \cite{191} studied a conjecture of Erdős, that every odd positive integer can be written as the sum of a squarefree number and a power of 2. They showed that this is connected with the behaviour of \( \text{ord}_p(2) \) and \( \text{ord}_p(2) \) and made various conjectures on these orders. They showed for example that if \( \sum_{p^2 \mid \lfloor p-1 \rfloor} 1/\text{ord}_p(2) < \infty \), then there exists an integer \( k \) such that almost every odd integer can be written as the sum of a squarefree number plus no more than \( k \) distinct powers of 2. They conjectured that there exists a constant \( \delta > 0 \) such that, for any finite set of primes \( \{p_1, p_2, \ldots, p_m\} \) and any choice of integers \( a_1, a_2, \ldots, a_m \), the proportion of positive integers which belongs to at least one of the congruence classes \( a_i \pmod{\text{ord}_p(2)} \), is \( < 1 - \delta \). They showed that \( \sum_p 1/\text{ord}_p(2) < \infty \) if this conjecture is true. In case the latter sum is \( < 1 \), they inferred that all but \( O(x/\log x) \) of the odd integers \( n \leq x \) can be written as a sum of a squarefree number and a power of 2. They also asked what the true order of magnitude is of

\[
\prod_{p \leq x} \left(1 - \frac{1}{\text{ord}_p(2)}\right).
\]
20) Elliott and Murata [137] conjectured that the following limits all exist and are finite:
\[
\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} g(p) \quad \text{and} \quad \lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} g(2p^2),
\]
and likewise with \( g \) replaced by \( g^\ast \) (recall that \( g^\ast(p) \) is the smallest prime primitive root modulo \( p \)). Bach [23] conjectured that
\[
\lim_{p \to \infty} \sup g^\ast(p) \frac{(\log p)(\log \log p)^2}{(\log p)(\log \log p)^2} = e^\gamma.
\]

21) Schinzel-Wójcik problem. Given any rational \( a, b \in \mathbb{Q}\setminus\{0, \pm1\} \), Schinzel and Wójcik [447] proved that there exist infinitely many primes \( p \) such that \( \nu_p(a) = \nu_p(b) = 0 \) and \( \text{ord}_p(a) = \text{ord}_p(b) \). The first condition ensures that the orders in the second one are defined and is satisfied for all but finitely many primes. More generally, given \( a_1, \ldots, a_s \in \mathbb{Q}\setminus\{0, \pm1\} \), the Schinzel-Wójcik problem is to determine whether there exist infinitely many primes \( p \) for which the order modulo \( p \) of each \( a_i \) is the same. Pappalardi and Susa [407] proved assuming GRH that the primes with this property have a density, and in the special case where each \( a_i \) is a power of a fixed rational number, they showed unconditionally that such a density is positive. In the case where all the \( a_i \)'s are prime, they expressed the density as an infinite product.

22) Y. Gallot found a quadratic polynomial \( f \) and an integer \( g \) such that the first (distinct) 38639 primes \( p \) produced by \( f \) are such that \( g \) is a primitive root modulo \( p \). Can this be improved (cf. §9.7.11)?

23) K. Szymiczek asked the following question: Do there exist infinitely many natural numbers \( n \) such that \((2^n - 3, 3^n - 2) = 1\)? In this direction Skalba [464], using ideas from a paper of Erdős [142], proved that the number of primes \( p < x \) dividing both \( 2^n - 3 \) and \( 3^n - 2 \) is \( O(x \log^{-1.0243} x) \). Ballot and Luca [33] considered the number of primes \( p \leq x \) such that \( p \) divides both \( a^n - b \) and \( c^n - d \).

24) Does the unconditional bound as established by Vinogradov, see (12), hold in greater generality?

25) Let \( q \) be an odd prime power. For each integer \( a \) with \((a, q) = 1\), is there a pair of primitive roots \( g_1 \) and \( g_2 \) modulo \( q \) such that \( a^2 \equiv g_1 g_2 \pmod{q} \)? Zhang [510] proved that if \( q \) is an odd prime and \((\frac{a}{q}) = 1\), then the answer is yes.

26) Prove or disprove the conjecture of Bach et al. [25] to the effect that \( q_g(x) \), the least \( x \)-pseudopower to base \( g \), should be about \( \exp(c_g x/\log x) \), where \( c_g > 0 \) (see §9.7.40).

27) Let \( G(n) \) be the smallest integer \( k \) such that the primes \( p \leq k \) generate the multiplicative group modulo \( n \). Prove or disprove the conjectures formulated by
Bach and Huelsbergen [24], see §9.7.55.

28) V.I. Arnold’s conjectures. In a series of papers, Arnold [12, 13, 14, 15, 16, 17, 18] considered dynamical systems related to linear transformations in finite fields and residue rings and made a series of conjectures. Of these many were confirmed, several refuted, and Shparlinski [459] observed that several required adjustments. For example, in [16] Arnold considered the quantity

\[ T_g(L) = \frac{1}{L} \sum_{l=1, (g,l)=1}^{L} \text{ord}_l(g), \]

where the sum is over the integers \( l \) coprime with \( g \) and suggested it grows asymptotically like \( c(g)L/\log L \), with \( c(g) > 0 \) a constant. Under GRH Shparlinski showed, however, that

\[ T_g(L) \geq \frac{L}{\log L} \exp(C(g)(\log \log L)^{3/2}), \]

for some constant \( C(g) > 0 \). Shparlinski observed that it should be possible to show under GRH that

\[ T_g(L) \geq \frac{L}{\log L} \exp((\log \log \log L)^{2+o(1)}). \]

Some of Shparlinski’s other results in [459] have recently been improved by Chang [69].

Since \( \text{ord}_l(g) \leq \lambda(l) \), with \( \lambda \) the Carmichael function, and on GRH there is a set of positive upper density of numbers coprime to \( g \) such that equality holds as Li and Pomerance [307] showed, it is natural to compare \( T_g(L) \) with \( L^{-1} \sum_{l=1}^{L} \lambda(l) \). Erdős et al. [146] proved that

\[ \frac{1}{x} \sum_{n \leq x} \lambda(n) = \frac{x}{\log x} \exp \left( B \frac{\log x}{\log \log \log x} (1 + o(1)) \right), \quad (27) \]

where

\[ B = e^{-\gamma} \prod_q \left(1 - \frac{1}{(q-1)^2(q+1)}\right) = 0.3453720641 \ldots \]

Kurlberg and Pomerance [274] showed that under GRH actually

\[ T_g(x) = \frac{x}{\log x} \exp \left( B \frac{\log x}{\log \log \log x} (1 + o(1)) \right), \]

as \( x \) tends to infinity, uniformly in \( g \) with \( 1 < |g| \leq \log x \). On comparing this result with (27) we see that the mean values of \( \lambda(n) \) and \( \text{ord}_n(g) \) are of a similar order of magnitude. Further, in the same paper Kurlberg and Pomerance established an asymptotic for

\[ \frac{1}{\pi(x)} \sum_{p \leq x} \text{ord}_p(g). \]
Earlier Stephens \[167\] showed that on GRH, the limit
\[
\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} \frac{\text{ord}_p(g)}{p - 1},
\]
exists and equals the Stephens constant \(S\) time a rational correction factor \(c_g\) depending on \(g\) (caution: his \(c_g\) must be adjusted in certain cases as noted by Moree and Stevenhagen \[359\]).

29) (Erdős, \[140\]). Is it true that 7, 15, 21, 45, 75 and 105 are the only integers \(n\) for which \(n - 2^k\) is a prime for every \(k\) with \(2 \leq 2^k < n\)? (See §9.7.20)

30) Are there Crandall numbers that are not Wieferich numbers other than 5 and 181? Are there infinitely many Crandall numbers that are not Wieferich numbers? (See §9.7.16 for definitions and references.)

31) Show that
\[
\sum_{n \leq x, (n,a) = 1} \frac{1}{\text{ord}_n(a)} = O(x^{1/4}).
\]

Then Artin’s primitive root conjecture follows by Ram Murty and Srinivasan \[379\], who conjectured that actually \(O(x^{1/4})\) should hold true. Felix \[154\] showed that the above sum is \(\log x\) on average.

32) Very odd sequences. Let \(V(x)\) denote the number of binary integers \(n = pq \leq 2x - 1\) with \(p < q\) such that \(\text{ord}_p(2) = (p - 1)/2\), \(\text{ord}_q(2) = (q - 1)/2\) and \((\text{ord}_p(2), \text{ord}_q(2)) = 1\). The author is inclined to believe that \(V(x)\) counts a positive fraction of all binary integers \(n \leq 2x - 1\), that is
\[
V(x) \sim c_0 \frac{x \log \log x}{\log x},
\]
for some positive constant \(c_0\). If true, this has some consequence for the theory of very odd sequences (introduced by J. Pelikán in 1973 \[111\]). For a given number \(n\) fix integers \(a_i\) with \(a_i \in \{0, 1\}\) for \(1 \leq i \leq n\). Put \(A_k = \sum_{i=1}^{n-k} a_ia_{i+k}\) for \(0 \leq k \leq n - 1\). We say that \(a_1 \ldots a_n\) is a very odd sequence if \(A_k\) is odd for \(1 \leq k \leq n\). By \(S(n)\) we denote the number of very odd sequences of length \(n\) and by \(N_k(x)\) the number of integers \(m \leq x\) such that \(S(m) = k\). Then if the above conjecture holds true we have, as \(x\) tends to infinity,
\[
N_{16}(x) \sim V(x) \sim c_0 \frac{x \log \log x}{\log x}.
\]
See Moree and Solé \[359\] for further information.

33) Cherednik’s heuristic. The heuristic considerations sketched in this survey begin with the behaviour of the sum \(\sum_{p \leq x} \varphi(p-1)/(p-1)\). Cherednik \[75\] proposed to
work instead with
\[ \frac{\sum_{p \leq x} \varphi(p - 1)}{\sum_{p \leq x} p - 1}. \]

From Pillai's work \[418\] it follows that the latter ratio has \( A \) as a limit. One can try to redo the asymptotically exact heuristics of the author in this spirit. Some numerical work, see \[75\], suggests that perhaps the Cherednik variation of the heuristics tends to be numerically closer to the actual primitive root counting function than the standard heuristics. Try to investigate and understand this.

34) **Least primitive root (mod \( p \)) versus least primitive root (mod \( p^2 \)).** Paszkiewicz \[408\] conjectures that for most primes \( p \) we have \( g(p) = h(p) \). Quantify this: do there exist infinitely many primes \( p \) for which \( g(p) \neq h(p) \)? (Presently only two are known, see also §9.7.27).

35) **Primitive roots in image of polynomial mapping.** Let \( f \) be a polynomial over a finite field. Is there a primitive root in its image? (See §9.7.36.)

36) **Farmer-Wilson variant of the Artin conjecture.** This conjecture states that if \((d, bM) = 1\), then there exist integers \( k \) and \( n \) such that \( b \equiv 2^n (\text{mod } d + kM) \).

Note that this follows from Artin’s conjecture, for if \( p = d + kM \) is prime and \( 2 \) a primitive root modulo \( p \) we are done. Since we do not require \( d + kM \) to be prime, nor \( 2 \) to be a primitive root modulo \( d + kM \), the above conjecture is actually much weaker than Artin’s. (See also §9.7.51.)

37) Let \( M \in \mathbb{F}_q[T] \) be a fixed polynomial and \( k \geq 2 \) be an integer. Determine the density of the set of all monic irreducible polynomials \( P \) for which \( P + M \) is a \( k \)-free polynomial. This is the polynomial variant of problems discussed in §9.7.1 and was earlier considered by Wei-Chen Yao \[503\], but according to MR1841909 (2002d:11144) his paper contains mistakes.

38) Let \( p \equiv 1(\text{mod } n) \). Put \( s_n(p) = \sum \{g/p\} \), where the sum is over the subgroup of \((\mathbb{Z}/p\mathbb{Z})^*\) of order \( n \), and \( \{ \} \) denotes the fractional part. Hadano et al. \[209\] raise 7 conjectures related to this quantity.

39) **Divisors of \( a^{f(n)} - 1 \).** From Fermat’s little theorem, we know that the set of primes which divide \( a^n - 1 \) for some \( n \) is precisely the set of primes not dividing \( a \). Ballot and Luca \[32\] investigated what happens if we replace the exponent \( n \) here by a different polynomial expression in \( n \). Let \( a \) be an integer with \(|a| > 1\) and \( f(X) \in \mathbb{Q}[X] \) a nonconstant, integer-valued polynomial with positive leading term. Suppose that there are infinitely many primes \( q \) for which \( f \) does not possess a root modulo \( q \), then Ballot and Luca showed that almost all primes \( p \) do not divide any number of the form \( a^{f(n)} - 1 \). Their result was sharpened by Pollack \[422\] who also gave a conjectural asymptotic for the number of primes dividing the sequence \( a^{f(n)} - 1 \), under the further assumption that the set of primes \( q \) for which \( f \) does
not possess a root modulo \( q \), has positive Dirichlet density.

40) **Generalized Titchmarsh divisor problem.** Let \( \tau(n) \) denote the number of divisors of the positive integer \( n \). In 1931, Titchmarsh [175] established the following estimate, assuming GRH,

\[
\sum_{a<p \leq x} \tau(p-a) = x \prod_{q \mid a} \left( 1 - \frac{1}{q} \right) \prod_{q \nmid a} \left( 1 + \frac{1}{q(q-1)} \right) + O\left( \frac{x \log \log x}{\log x} \right).
\]

In 1961, Linnik [309] established the above asymptotic unconditionally by using his dispersion method. Later Rodriguez [433] and independently Halberstam [210], by a straightforward application of the Bombieri-Vinogradov theorem, proved unconditionally the Titchmarsh conjectural asymptotic formula. In the special case \( a = 1 \) it is a trivial observation that

\[
\sum_{p \leq x} \tau(p-1) = \sum_{1 \leq m \leq x-1} \pi(x; m, 1) = \sum_{m \geq 1} \pi(x; m, 1).
\]

Essentially we are counting each prime number \( p \leq x \) for each occurrence of \( m \) such that \( p \) splits completely in \( \mathbb{Q}(\zeta_m) \).

Let \( \mathfrak{F} = \{ F_m : m \geq 1 \} \) be a family of finite Galois extensions of \( \mathbb{Q} \). For each \( m \), let \( D_m \) be a union of conjugacy classes of \( \text{Gal}(F_m/\mathbb{Q}) \) and let \( \tau_{\mathfrak{F}}(p) \) be the number of \( m \geq 1 \) such that \( p \) is unramified in \( F_m/\mathbb{Q} \) and the Artin symbol \( \sigma_p \) belongs to \( D_m \). Suppose that \( \tau_{\mathfrak{F}}(p) < \infty \) for each prime \( p \). Then we have the following problem: **Generalized Titchmarsh divisor problem:**

Determine the behaviour of \( \sum_{p \leq x} \tau_{\mathfrak{F}}(p) \) as \( x \) tends to infinity.

In the above generality, the problem is too unwieldy unless some constraint on the sizes of \( D_m \) are imposed. Let \( A \) be an abelian variety defined over \( \mathbb{Q} \) and for each \( m \geq 1 \), let \( A[m] \) be the set of torsion points of \( A \) of order dividing \( m \). Let \( F_m = \mathbb{Q}(A[m]) \) and \( D_m = \{ Id \} \). Therefore \( \tau_{\mathfrak{F}}(p) \) is the number of \( m \geq 1 \) such that \( p \) splits completely in \( \mathbb{Q}(A[m]) \). In this setup the problem specializes to the Titchmarsh divisor problem for Abelian varieties and it is analogous to the classical case for \( \tau(p-1) \). Akbary and Ghioca [5] believe that in this case

\[
\sum_{p \leq x} \tau_{\mathfrak{F}}(p) = \text{Li}(x) \sum_{n=1}^{\infty} \frac{1}{[\mathbb{Q}(A[m]) : \mathbb{Q}]} + o\left( \frac{x}{\log x} \right)
\]

and under GRH prove a special case. In case \( A = E \) is a CM elliptic curve, they unconditionally prove [28].

We note that Felix [154] gives an estimate for \( \sum_{p \leq x, p \equiv a(\mod k)} \tau((p-a)/k) \) and applies it to a question related to Artin’s primitive root conjecture (see §9.7.3).

**Remark.** If the reader has not suffered an overdose of primitive roots after reading this survey, (s)he is recommended to consume them at industrial strength [126].
11. ACKNOWLEDGEMENT

The basis for this paper was a survey lecture I gave at Oberwolfach concerning Artin’s primitive root problem. I am grateful for the privilege of having visited Oberwolfach several times and would like to than Z. Rudnick for inviting me to give the lecture on which this survey is based. MathSciNet turned out to be an extremely helpful tool in writing this survey. For close to 20 years now I regularly communicated with Peter Stevenhagen concerning Artin type problems. I am very grateful for his tremendous help. Hendrik Lenstra pointed out various inaccuracies in an earlier version. S.D. Cohen kindly updated me on the status of Golomb’s conjectures. W. Narkiewicz and Ana Zumalacárregui provided me with some helpful information concerning problems 29, respectively 12. Kate Petersen fine-tuned the description I gave of her work. Further thanks are due to Joachim von zur Gathen and the referee. Many (language) comments were provided by Julie Rowlett; a native English speaker. I am very grateful for her willingness to invest so much time in this. Comments of A. Akbary, A. Felix and P. Kurlberg on an earlier version are taken into account. Akbary kindly rewrote my initial version of Problems 6 and 40 a bit.

An earlier and rather shorter version of this paper (with the same title) is available from the arXiv [344] (its aim was to describe the status quo up to 2004). Many thanks are due to Alina Cojocaru for her contributions on elliptic Artin to the survey and for her comments and suggested corrections to the rest of survey. Wojciech Gajda kindly wrote a section on Artin and K-theory. Hester Graves carefully studied the literature on Artin and Euclidean domains and kindly reported on that, using my initial version of this as a starting point. Last but not least I thank Francesco Pappalardi and Carl Pomerance for urging me to publish this survey. Special thanks are due to Carl for his support and many helpful comments.

References


[150] T. Estermann, On the representations of a number as the sum of a prime and a quadratfrei number, J. London Math. Soc. 6 (1931), 219–221.


[218] H. Hasse, Über die Dichte die Dichte der Primzahlen \( p \), für die eine vorgegebene ganzrationale Zahl \( a \neq 0 \) von durch eine vorgegebene Primzahl \( l \neq 2 \) teilbarer bzw. unteilbarer Ordnung mod. \( p \) ist, \textit{Math. Ann.} \textbf{162} (1965/1966), 74–76.


L.J. Mordell, The congruence $(p - 1/2)! \equiv \pm 1 (\text{mod } p)$, *Amer. Math. Monthly* 68 (1961), 145-146.


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


P. Moree, On the distribution of the order and index of $g(\text{mod } p)$ over residue classes I, *J. Number Theory* 114 (2005), 238–271.


[351] P. Moree, Asymptotically exact heuristics for prime divisors of \( \{a^k + b^k\}_{k=1}^\infty \), \textit{J. Integer Seq.} \textbf{9} (2006), no. 2, Article 06.2.8, 15 pp. (electronic).


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


[365] H. Müller, On the distribution of the orders of \( 2 \pmod{u} \) for odd \( u \), \textit{Arch. Math. (Basel)} \textbf{84} (2005), 412–420.


83


[401] F. Pappalardi, On the order of finitely generated subgroups of $\mathbb{Q}^*(\text{mod } p)$ and divisors of $p – 1$, *J. Number Theory* **57** (1996), 207–222.


[456] D. Shanks, Fibonacci primitive roots, Fibonacci Quart. 10 (1972), 163–168.


86

[464] M. Skalba, Primes dividing both $2^n - 3$ and $3^n - 2$ are rare, Arch. Math. (Basel) 84 (2005), 485–495.

**PIETER MOREE**

**MAX-PLANCK-INSTITUT FÜR MATHEMATIK,**

**VIVATSGASSE 7**

**D-53111 BONN, DEUTSCHLAND**

*e-mail address:* moree@mpim-bonn.mpg.de