PRIME DENSITIES FOR SECOND ORDER TORSION SEQUENCES

PETER STEVENHAGEN

Abstract. The set of primes $\pi_X$ dividing the terms of a second order linear recurrent integer sequence $X$ has a natural description in terms of the initial quotient $q$ of $X$ and the root quotient $r$ of the underlying recurrence. We call $X$ torsion if the residue class of $q$ in the group associated to $r$ is torsion. We prove that for such $X$, the set $\pi_X$ has positive rational density in the set of all primes. We compute the density explicitly for a ‘generic’ class of examples.

1. Introduction

An integer sequence $X = \{x_n\}_{n=0}^\infty$ is said to satisfy a second order linear recurrence if there exist integers $a$ and $b$ such that we have

$$x_{n+2} = ax_{n+1} + bx_n$$

for all $n \geq 0$.

The set $\pi_X$ of prime divisors of $X$ is the set of prime numbers that divide some term of the sequence $X$. As the bibliography of [1] shows, determining the ‘size’ of $\pi_X$ is a natural and well-studied question. It is our aim to prove that for a natural class of second order recurrent sequences $X$, the torsion sequences, the set $\pi_X$ has a positive natural density inside the set of all primes, and that this density is a rational number.

We first show, in Proposition 2.2, that $\pi_X$ is most conveniently described in terms of two parameters: the root quotient $r$ of the defining recurrence and the initial quotient $q$ of the sequence. This characterization, which does not refer to integer sequences, greatly clarifies the group structure introduced in [6, 7] on the set of equivalence classes of sequences satisfying a given second order recurrence.

The problem of determining the density $\delta_X$ of $\pi_X$ comes down to a basic but non-trivial number theoretic question in terms of $q$ and $r$ that resembles the question underlying Artin’s primitive root conjecture. In this paper, we show that $\delta_X$ exists in the frequently occurring case where $q$ is a torsion element in the group $S(r)$ of equivalence classes of

1991 Mathematics Subject Classification. Primary 11B37; Secondary 11R45.

Key words and phrases. Second order linear recurrence, Chebotarev density theorem.

Typeset by A\LaTeX
version January 11, 2007
sequences with root quotient $r$ that we define in 2.4. In special cases, this had been proved earlier by Hasse [2, 3] and Lagarias [5], and it is their method that we generalize. Even though $\delta_X$ can be computed from the basic parameters $q$ and $r$ in every particular torsion case, a general formula has to distinguish more cases than one wants to write down. In section 5, we establish the following general fact.

**Main Theorem.** Let $X$ be a second order torsion sequence. Then the density $\delta_X$ of its set of prime divisors in the set of all prime numbers is positive and rational.

This proves the ‘main conjecture’ of [12, p. 362]. Our general formalism also shows how to compute explicit densities. By way of example, we treat in Theorem 5,* the case of the Lucas sequences $X = \{\text{Tr}(\alpha^n)\}_{n=1}^\infty$ obtained by taking the traces of the powers of a ‘generic’ quadratic integer. The example of the ‘classical’ Lucas sequence associated to the fundamental unit of a quadratic number field, which is slightly easier than the generic case, has already been treated in [9].

For non-torsion second order sequences, one has to apply different techniques in order to prove that $\delta_X$ exists. They are related to Hooley’s proof of Artin’s conjecture on primitive roots modulo $p$ and all results are conditional as they require the assumption of the generalized Riemann hypothesis. The densities obtained are rational multiples of the Artin-type constant $S = \prod_{p \text{ prime}}(1 - \frac{p^2 - 1}{p^3 - 1})$. The case where $q$ and $r$ are rational is treated in full generality in [10]. For the treatment of a non-rational non-torsion example, see [11].

2. Root quotients and initial quotients

Let $X = \{x_n\}_{n=0}^\infty$ be an integer sequence satisfying the second order recurrence $x_{n+2} = ax_{n+1} + bx_n$, and let $f = T^2 - aT - b \in \mathbb{Z}[T]$ be the corresponding characteristic polynomial. For $b = 0$ the sequence is actually a first order recurrent sequence with general term $x_n = a^n x_0$. In this case $\pi_X$ is trivially determined, and we will assume from now on that $X$ does not satisfy a first order recurrence. We also assume that $a$ does not vanish, since a second order sequence satisfying a recurrence of the form $x_{n+2} = bx_n$ is simply a ‘union’ of two first order sequences.

Let $f = (T - \alpha)(T - \tilde{\alpha}) \in \overline{\mathbb{Q}}[T]$ be the factorization of $f$ over an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. As we have $\alpha\tilde{\alpha} = -b \neq 0$, we may define the root quotient of our recurrence as

$$r = r(f) = \alpha/\tilde{\alpha} \in \overline{\mathbb{Q}}^*.$$  

Note that $r$ is determined only up to inversion, and that it is either a non-zero rational number or an element of norm 1 in a quadratic number field. The relation $\tilde{\alpha}(r+1) = a \neq 0$ shows that we always have $\mathbb{Q}(r) = \mathbb{Q}(\alpha)$, and that the value $r = -1$, which corresponds to recurrences of the form $x_{n+2} = bx_n$, is by assumption excluded as a root quotient.
For a second order recurrence with root quotient $r = 1$, we have $\alpha = \tilde{\alpha} \in \mathbb{Z}$ and $x_n = (x_0 + cn)\alpha^n$ for some rational number $c$. We have $c \neq 0$ as $X$ is not first order, and all primes $p$ for which the rational number $c$ is invertible modulo $p$ divide $X$. It follows that in this inseparable case, $\pi_X$ consists of all but finitely many primes.

In the separable case $r \neq 1$, we can write the general term of $X$ as $x_n = c\alpha^n + \tilde{c}\tilde{\alpha}^n$ with $c = \frac{x_1 - \tilde{\alpha}x_0}{\alpha - \tilde{\alpha}}$ and $\tilde{c} = \frac{x_1 - \alpha x_0}{\tilde{\alpha} - \alpha}$.

By assumption $\tilde{c}c$ does not vanish, and we define the initial quotient $q(X)$ of $X$ as

$$q = q(X) = \frac{x_1 - \alpha x_0}{x_1 - \tilde{\alpha}x_0} = -\frac{\tilde{c}}{c} \in \mathbb{Q}(\alpha)^* = \mathbb{Q}(r)^*.$$

Just like the root quotient, the initial quotient is determined only up to inversion, and it is either a non-zero rational number or an element of norm 1 in a quadratic number field. It is not defined for inseparable recurrences.

Let $p$ be a prime number, $\mathbb{Z}(p) = \{x \in \mathbb{Q} : \text{ord}_p(x) > 0\}$ the ring of $p$-integral rational numbers, and $\mathbb{Z}_p$ the integral closure of $\mathbb{Z}(p)$ in $\mathbb{Q}$. Then $\mathbb{Z}_p$ is the ring of $p$-integral algebraic numbers, and its unit group $\mathbb{Z}_p^*$ consists of the $p$-units in $\mathbb{Q}$. An algebraic number $x \neq 0$ is a $p$-unit if and only if no prime ideal lying over $p$ occurs in the ideal factorization of $(x)$ in the number field $\mathbb{Q}(x)$. In particular, any element $x \in \mathbb{Q}^*$ is a $p$-unit for almost all prime numbers $p$.

2.1. Definition. Given two non-zero elements $x, y \in \mathbb{Q}^*$, we let $D(x, y)$ be the set of rational prime numbers satisfying the following two conditions:

- both $x$ and $y$ are $p$-units;
- the subgroup of $(\mathbb{Z}(p)/p\mathbb{Z}(p))^*$ generated by $(y \mod p)$ contains $(x \mod p)$.

There are other, equivalent ways to define the set $D(x, y)$. If $x$ and $y$ are contained in a number field with ring of integers $\mathcal{O}$, one can replace $(\mathbb{Z}(p)/p\mathbb{Z}(p))^*$ by $(\mathcal{O}/p\mathcal{O})^*$ in the second condition and thus avoid any reference to the large ring $\mathbb{Z}_p$. Still another way to phrase the second condition is to say that there exists an integer $k \in \mathbb{Z}$ such that $xy^k$ is, in Hasse’s terminology, a ‘one-unit’ at all primes over $p$.

Note that $D(x, y)$ is left unchanged if we replace either $x$ or $y$ by its inverse. This enables us to take for $x$ and $y$ initial quotients and root quotients as defined above, and to characterize the set of prime divisors of a second order recurrent sequence as follows.

2.2. Proposition. Let $X$ be a second order recurrent sequence with root quotient $r \neq 1$ and initial quotient $q$. Then we have an equivalence

$$p \in \pi_X \iff p \in D(q, r).$$
for almost all prime numbers $p$.

**Proof.** Write $X = \{x_n\}_{n=0}^\infty$ with $x_n = c\alpha^n + \tilde{c}\alpha^n$ as above, and let $p$ be a prime number for which $c$, $\tilde{c}$ and $b = a\tilde{\alpha}$ are $p$-units. Then we have

$$p \text{ divides } x_n \iff \tilde{c}/c = (\alpha/\tilde{\alpha})^n \in \mathbb{Z}(p)/p\mathbb{Z}(p) \iff q = r^n \in (\mathbb{Z}(p)/p\mathbb{Z}(p))^*.$$

As every $p$-unit has finite order in $(\mathbb{Z}(p)/p\mathbb{Z}(p))^*$, the set of exponents $n$ for which we have $q = r^n \in (\mathbb{Z}(p)/p\mathbb{Z}(p))^*$ contains infinitely many positive elements if it is non-empty. We conclude that for all but the finitely many primes excluded above, we have $p \in D(q, r)$ if and only if $p$ divides some term of the sequence $X$.

We next show that all pairs $(q, r)$ of algebraic numbers that are either rational or quadratic of norm 1 actually come from a second order sequence.

2.3. **Proposition.** Let $q$ and $r \neq 1$ be non-zero algebraic numbers, and suppose that either both $q$ and $r$ are rational, or $q$ and $r$ are elements of norm 1 in the same quadratic number field. Then there exists a second order integer sequence with root quotient $q$ and initial quotient $r$.

**Proof.** If $q$ and $r$ are rational, this is immediate: write $r = \alpha/\tilde{\alpha}$ for integers $\alpha, \tilde{\alpha} \in \mathbb{Z}$, then solve the homogeneous linear equation $x_1 - \alpha x_0 = q(x_1 - \tilde{\alpha} x_0)$ for integers $x_0, x_1 \in \mathbb{Z}$ not both equal to 0.

If $q$ and $r$ are non-rational elements of norm 1 in a quadratic number field $K$, we can find $\alpha \in K^*$ with conjugate $\tilde{\alpha}$ satisfying $\alpha/\tilde{\alpha} = r$ by Hilbert’s theorem 90. Note that we have $K = \mathbb{Q}(\alpha)$. Multiplying $\alpha$ when necessary by a rational integer, we can take $\alpha$ to be integral. In the same way, the element $q \in \mathbb{Q}(\alpha)^*$ of norm 1 can be written as $q = (x_1 - \alpha x_0)/(x_1 - \tilde{\alpha} x_0)$ for integers $x_0, x_1 \in \mathbb{Z}$. The second order sequence with characteristic polynomial $(T - \alpha)(T - \tilde{\alpha}) \in \mathbb{Z}[T]$ and initial values $x_0, x_1$ now has root quotient $q$ and initial quotient $r$. \hfill $\Box$

Propositions 2.2 and 2.3 show that the study of $\pi_X$ for second order sequences $X$ and the study of the sets $D(q, r)$ with $q$ and $r \neq 1$ as in 2.3 are essentially the same problem. One may argue that $D(q, r)$ is the natural set of primes to look at and in fact, much clarity is gained if one suppresses all references to second order sequences and simply studies the sets $D(q, r)$ for those $q$ and $r$ that are allowed by Proposition 2.3. One may even extend such a study to arbitrary algebraic numbers $q$ and $r$, but this falls beyond the scope of the present paper.

The set $D(q, r)$ associated to a second order sequence $X$ is invariant under a few trivial modifications of the sequence $X$ that change $\pi_X$ by finitely many primes. These are:

(a) multiplication $x_n \mapsto ax_n$ of all terms of the sequence by some constant $a \in \mathbb{Q}^*$;
(b) multiplication $x_n \mapsto a^n x_n$ of the $n$-th term of the sequence by the $n$-th power of some non-zero constant $a \in \mathbb{Q}^*$;

(c) the shifting $x_n \mapsto x_{n+k}$ of the sequence over $k$ places.

Note that the second modification changes the recurrence, albeit in a simple way, and that the third modification uses for $k < 0$ some terms of negative index of the sequence. These are defined by the obvious extension of the recurrence to negative indices. If one prefers to restrict to integer sequences, one should avoid values of $k < 0$ in (c) that introduce non-integral terms in the sequence. Similarly, one should restrict in (a) and (b) to those $a \in \mathbb{Q}^*$ for which the resulting sequence is again integral.

The modifications in (a) and (b) leave $q$ and $r$ invariant, whereas those in (c) change $q$ by the $k$-th power of $r$. This does not change $D(q, r)$, and in each case it is clear—by Proposition 2.2 or by direct inspection—that $\pi_X$ only changes by finitely many primes.

The observation that $\pi_X$ does not change in an essential way under modifications of type (a) and (c) has given rise to an equivalence relation on second order sequences due to Laxton [6]. He defines a product of second order sequences satisfying the same recurrence based on their ‘standard representation’, shows that it is well-defined on equivalence classes, and finally checks that this multiplication gives rise to a group structure. All this is mildly cumbersome, but fortunately both the definition and the basic properties of this group are immediate in terms of the invariants $q$ and $r$. As we do not take the recurrence itself but only its root quotient as a basic invariant, we will call two second order sequences equivalent if one can be transformed into the other by repeated application of the three types of modifications above. This means that two second order sequences with invariants $(q_1, r_1)$ and $(q_2, r_2)$ are equivalent if and only if we have $r_1 = r_2 = r$ and $q_1/q_2 = r^k$ for some $k \in \mathbb{Z}$. For sequences satisfying the same recurrence, our notion of equivalence reduces to the one given in [6]. We can formalize it in the following way.

2.4. Definition. If $r \neq \pm 1$ is an algebraic number that is either rational or contained in the group $K_N^*$ of elements of norm 1 in a quadratic number field $K$, we set

$$S(r) = \begin{cases} \mathbb{Q}^*/\langle r \rangle & \text{if } r \text{ is rational;} \\ K_N^*/\langle r \rangle & \text{if } r \text{ is in } K_N^*. \end{cases}$$

We define the equivalence class $[q, r]$ of a second order recurrent sequence with root quotient $r \neq \pm 1$ and initial quotient $q$ to be the residue class $\overline{q} \in S(r)$.

We leave it to the reader to check that the multiplication of equivalence classes of sequences as found in [1] and [6] is the obvious multiplication

$$[q_1, r] \cdot [q_2, r] = [q_1 q_2, r]$$

of initial quotients in the sequence group $S(r)$. For any sequence $X$ in the class $[q, r]$, the symmetric difference of the sets $\pi_X$ and $D(q, r)$ is finite, so they are ‘the same’ for density purposes.
The determination of the set $D(q, r)$, either in the general setting of 2.1 or for $q$ and $r$ coming from a second order sequence, is immediate only for a couple of special values of $q$ and $r$.

If $q \in \overline{\mathbb{Q}}^*$ is arbitrary and $r$ is any root of unity, there are only finitely many elements of the form $q - r^n$; the set $D(q, r)$ in 2.1 is then either finite or, if $q$ is a power of $r$, the set of all primes. Second order sequences for which the root quotient is a root of unity are often said to be degenerate. If $r \neq \pm 1$ is a root of unity occurring as the root quotient of a second order sequence $X$, then $r$ is of order $m \in \{3, 4, 6\}$. In this situation, we can view $X$ as a ‘union’ of $m$ first order sequences and, unless one of these sequences is the zero sequence, we find that $\pi_X$ is finite. The same is true for sequences with root quotient $r = -1$; we chose to exclude this case in 2.4 since it is the only case where $\mathbb{Q}(r)$ does not determine $\mathbb{Q}(\alpha)$, and it would have introduced special cases in most of our statements.

If $r \in \overline{\mathbb{Q}}^*$ is arbitrary and $q$ is a power of $r$, then $[q, r]$ is the unit element in $S(r)$ and almost all primes are in $D(q, r)$. The corresponding sequences are those equivalent to a Fibonacci-type sequence with general term

$$x_n = \frac{\alpha^n - \tilde{\alpha}^n}{\alpha - \tilde{\alpha}}.$$  

In all cases where $r$ is not a root of unity and $[q, r] \in S(r)$ is not the unit element, the determination of $D(q, r)$ is not a trivial matter.

3. Torsion sequences

A second order recurrent sequence with root quotient $r$ and initial quotient $q$ is said to be torsion if $[q, r]$ is an element of finite order in $S(r)$. Before studying the sets $D(q, r)$ coming from torsion sequences, we describe the torsion subgroup $S(r)^{tor} \subset S(r)$. We will assume that $r$ is not a root of unity, and write $K = \mathbb{Q}(r)$. In order to avoid unnecessary distinctions between the rational case $K = \mathbb{Q}$ and the irreducible or quadratic case in which $K = \mathbb{Q}(r)$ is quadratic, we extend the notation $K_N^*$ for the norm-1-subgroup of a quadratic field $K$ from 2.4 and take $K_N^* = \mathbb{Q}^*$ in the rational case.

Since $r \in K_N^*$ is not contained in the group $\mu_K$ of roots of unity in $K$, the torsion subgroup $S(r)^{tor}$ of $S(r) = K_N^*/\langle r \rangle$ fits in an exact sequence of groups

$$(3.1) \quad 1 \longrightarrow \mu_K \longrightarrow S(r)^{tor} \longrightarrow (K_N^*/\mu_K \cdot \langle r \rangle)^{tor} \longrightarrow 1.$$  

As $K^*/\mu_K$ is a free abelian group on countably many generators, $(K^*/\mu_K \cdot \langle r \rangle)^{tor}$ is a finite cyclic group. Its order is the largest integer $k$ for which $r$ is ‘up to roots of unity’ a $k$-th power in $K^*$. If $K$ is real quadratic and $(K^*/\mu_K \cdot \langle r \rangle)^{tor}$ is generated by an element of norm $-1$, then $(K_N^*/\mu_K \cdot \langle r \rangle)^{tor}$ is the subgroup of index 2 in $(K^*/\mu_K \cdot \langle r \rangle)^{tor}$. In all other cases these groups are equal.
We call the order of \((K_N^*/\mu_K \cdot \langle r \rangle)^{tor}\) the exponent of our root quotient \(r\). If \(x \in K_N^*\) is the lift of a generator of this cyclic group and \(\zeta\) generates \(\mu_K\), we have

\[
S(r)^{tor} = \langle \zeta, x \rangle / \langle r \rangle
\]

The following ‘structure theorem’ for torsion groups of second order recurrences, which corrects the results of [7], is now immediate.

**3.3. Theorem.** Let \(e\) be the exponent of \(r\). Then the torsion subgroup \(S(r)^{tor}\) is an extension of a cyclic group of order \(e\) by \(\mu_K\). Conversely, every abelian extension of a cyclic group by a cyclic group of order 2, 4, or 6 can be realized as the torsion subgroup of \(S(r)\) for some root quotient \(r\).

**Proof.** The first statement is clear from (3.1). If \(\zeta\) is a root of unity of order 2, 4, or 6, one takes \(K = \mathbb{Q}(\zeta)\) and picks \(r_0 \in K_N^*\) of exponent 1. Putting \(r = \zeta^k r_0^e\) yields a group \(S(r)\) of which the torsion group is an extension of a cyclic group of order \(e\) by \(\langle \zeta \rangle\). Varying \(k\) yields the possible extension types. □

If \(r = x^e\) is an \(e\)-th power in \(K_N^*\), with \(e\) the exponent of \(r\), the group \(S(r)^{tor}\) is said to be of split type. Otherwise it is of non-split type. In the split case, we have an isomorphism

\[
S(r)^{tor} \cong \mu_K \times \langle x \rangle \cong \mu_K \times \mathbb{Z}/e\mathbb{Z}.
\]

If \(K = \mathbb{Q}(r)\) is not the quadratic field of discriminant \(-3\) or \(-4\), we have \(\mu_K = \langle -1 \rangle\) and there is a single non-split case. It occurs when \(e\) is even, \(-r = x^e\) is an \(e\)-th power and \(S(r)^{tor} \cong \langle x \rangle \cong \mathbb{Z}/2e\mathbb{Z}\) is cyclic of order \(2e\). In the two special cases where \(\mu_K\) has order 4 or 6, there are more non-split extensions.

If \([q, r]\) is an arbitrary element of \(S(r)\), we can characterize almost all \(p \in D(q, r)\) in terms of the orders \(f_p(q)\) and \(f_p(r)\) of \(q\) and \(r\) in the group \((\mathbb{Z}/p\mathbb{Z})^*\) occurring in 2.1. For rational \(p\)-units \(q, r \in \mathbb{Q}^*\), this is immediate: the images of \(q\) and \(r\) in \((\mathbb{Z}/p\mathbb{Z})^*\) lie in the cyclic subgroup \(F_p^* \subset (\mathbb{Z}/p\mathbb{Z})^*\), and we have \(q = r^n \in F_p^*\) if and only if \(f_p(q)\) divides \(f_p(r)\). If \(K = \mathbb{Q}(r)\) is a quadratic field with ring of integers \(\mathcal{O}\), then the images of \(q, r \in K_N^*\) in \((\mathbb{Z}/p\mathbb{Z})^*\) lie in the kernel of the norm map \(N : (\mathcal{O}/p\mathcal{O})^* \longrightarrow F_p^*\). This is a cyclic subgroup of \((\mathbb{Z}/p\mathbb{Z})^*\) whenever \(p\) is unramified in \(K/\mathbb{Q}\). We therefore set

\[
\kappa_p = \begin{cases} \mathbb{F}_p^* & \text{for } K = \mathbb{Q}; \\ \text{ker}[N : (\mathcal{O}/p\mathcal{O})^* \longrightarrow F_p^*] & \text{when } K \text{ is quadratic.} \end{cases}
\]

In either case, \(\kappa_p\) is cyclic of order \(p - (\Delta_p)\) for all \(p\) coprime to the discriminant \(\Delta\) of \(K = \mathbb{Q}(r)\). If \(q, r\), and \(\Delta\) are \(p\)-units, we have

\[
p \in D(q, r) \iff q \in \langle r \rangle \subset \kappa_p \iff f_p(q) \text{ divides } f_p(r).
\]
All classical observations about ‘ranks of apparition’ of primes dividing second order sequences and the periodicity properties of the indices \( n \) for which \( p \) divides \( x_n \) are translations of elementary group theoretic statements about \( \kappa_p \).

The special importance of torsion classes \([q,r]\) arises from the fact that the primes in the corresponding set \( D(q,r) \) can be characterized in terms of divisibility conditions on the order of a single element \( x \in K^* \) modulo \( p \). For the \( m \)-torsion class \([\zeta_m,r] \in S(r)\) arising from a primitive \( m \)-th root of unity \( \zeta_m \in K \), this is immediate from (3.5): the order \( f_p(\zeta_m) \) equals \( m \) for all primes \( p \nmid m \), and we find

\[
p \in D(\zeta_m,r) \iff m \text{ divides } f_p(r)
\]

whenever \( m \) and \( r \) are \( p \)-units. Similarly, if \( r = q^m \) is the \( m \)-th power of \( q \), then \([q,q^m]\) has order \( m \) in \( S(q^m) \), and we have \( f_p(q^m) | f_p(q) \), with equality if and only if \( f_p(q) \) is coprime to \( m \). In view of (3.5), this yields

\[
p \in D(q,q^m) \iff f_p(q) \text{ is coprime to } m
\]

whenever \( q \) is a \( p \)-unit. For general torsion classes of order \( m \), we have the following result.

3.6. **Main lemma.** Let \([q,r] \in S(r) \) have order \( m \), and write \( q^m = r^n \). Let \( p \) be a prime number for which \( q, r, m \) and \( \Delta \) are \( p \)-units. Then we have \( p \in D(q,r) \) if and only if the following conditions hold for each prime divisor \( \ell \) of \( m \):

1. for \( \text{ord}_\ell(m) > \text{ord}_\ell(n) \) we have \( \ell \nmid f_p(q^n) \);
2. for \( \text{ord}_\ell(m) \leq \text{ord}_\ell(n) \) we have \( \ell | f_p(r^{m/\ell}) \).

**Proof.** By (3.5), a prime \( p \) for which \( q, r, m \) and \( \Delta \) are \( p \)-units is in \( D(q,r) \) if and only if we have an inclusion \( \langle q \rangle \subset \langle r \rangle \) of subgroups of the cyclic group \( \kappa_p \). Such an inclusion holds if and only if for every prime number \( \ell \), there is an inclusion \( \langle q \rangle_\ell \subset \langle r \rangle_\ell \) of the corresponding \( \ell \)-Sylow subgroups. This only yields conditions for the primes \( \ell | m \), since for other \( \ell \) we trivially have \( \langle q \rangle_\ell = \langle q^m \rangle_\ell = \langle r^n \rangle_\ell \subset \langle r \rangle_\ell \).

Let \( \ell | m \) be a prime for which we have \( \text{ord}_\ell(m) > \text{ord}_\ell(n) \), and put \( g = \gcd(m,n) \). As \( q \) has order \( m \) in \( S(r) \), the quotient \( q^m/g / r^n/g \) is some primitive \( g \)-th root of unity \( \zeta_g \in \mathbb{Q}(r)^* \). By assumption \( n/g \) is coprime to \( \ell \), so we find that \( \langle r \rangle_\ell = \langle r^{n/g} \rangle_\ell = \langle \zeta_g^{-1} q^m/g \rangle_\ell \) contains \( \langle q \rangle_\ell \) if and only if we have an equality

\[
\langle \zeta_g^{-1} q^m/g \rangle_\ell = \langle \zeta_g, q \rangle_\ell.
\]

For \( x = \text{ord}_\ell(f_p(q)) > \text{ord}_\ell(g) \) the right hand side has order \( \ell^x \), and since \( \ell \) divides \( m/g \) the left hand side is annihilated by \( \ell^{x-1} \). In the opposite case \( \text{ord}_\ell(f_p(q)) \leq \text{ord}_\ell(g) =
\(\text{ord}_\ell(n) = y\) both groups have order \(\ell^y\), so they coincide. Phrasing the last inequality as 
\(\text{ord}_\ell(f_p(q^n)) = 0\), we arrive at condition (1) for \(p\) to be in \(D(q, r)\).

Suppose now that \(\ell|m\) is a prime for which we have \(\text{ord}_\ell(m) \leq \text{ord}_\ell(n)\). Then \(m/g\) is coprime to \(\ell\), and \(\langle q \rangle_{\ell} = \langle q^{m/g} \rangle_{\ell} = \langle \zeta_g r^{m/g} \rangle_{\ell}\) is contained in \(\langle r \rangle_{\ell}\) if and only if we have \(\langle \zeta_g \rangle_{\ell} \subset \langle r \rangle_{\ell}\). As we have \(\text{ord}_\ell(g) = \text{ord}_\ell(m)\) by assumption, the resulting condition 
\(\text{ord}_\ell(g) \leq \text{ord}_\ell(f_q(r))\) can be rewritten as \(\text{ord}_\ell(f_q(r^{m/\ell})) > 0\). This yields condition (2) for \(p\) to be in \(D(q, r)\).

If \(m\) and \(n\) are as in 3.6, the proof shows that \(K = \mathbb{Q}(r)\) contains a primitive \(g\)-th root of unity, with \(g = \gcd(m, n)\). As \(K\) is at most quadratic, only \(g \in \{1, 2, 3, 4, 6\}\) can occur, and case (2) will not arise for a prime \(\ell > 3\).

4. The basic density problem

From the Main Lemma 3.6, we see that the essential step in finding the density of \(D(q, r)\) for a torsion sequence \([q, r]\) consists in finding, for \(\ell\) a prime number and \(x\) an element that is rational if \(r\) is rational and quadratic of norm 1 if \(r\) is quadratic, the density of the set of primes \(p\) for which the order \(f_p(x)\) of \(x\) in \((\mathbb{Z}/p\mathbb{Z})^*\) is coprime to \(\ell\). Note that we have \(\mathbb{Q}(x) = \mathbb{Q}(r)\), and that the subgroup generated by \((x \mod p)\) lies in the group \(\kappa_p\) we defined in (3.4). As \(r\) is not a root of unity and condition (1) in 3.6 is never met for a root of unity \(q\), we may and do assume that \(x\) is not a root of unity. The main result of this section is the following.

4.1. Theorem. Let \(\ell\) be a prime number, and \(x\) an algebraic number that is either rational or quadratic of norm 1, and not a root of unity. Then the set of prime numbers \(p\) for which the order of \(x\) in \((\mathbb{Z}/p\mathbb{Z})^*\) is coprime to \(\ell\) has positive rational density.

The proof is an application of the Chebotarev density theorem to an infinite tower of number fields contained in the normal extension

\[
\Omega_{\ell} = K(\zeta_{\ell^\infty}, \sqrt[r]{x}) = \bigcup_{k \geq 1} K(\zeta_{\ell^k}, \sqrt[\ell^k]{x})
\]

of \(\mathbb{Q}\) obtained by adjoining to \(K = \mathbb{Q}(x)\) all \(\ell\)-power roots of unity and all \(\ell\)-power roots of \(x\). As \(x\) is not a root of unity, \(x\) is not an \(\ell\)-th power in \(K\) for \(k\) sufficiently large. Moreover the number field \(K(\sqrt[\ell^k]{x})\) obtained by adjoining some \(\ell^k\)-th root of \(x\) to \(K\) is not normal for large \(k\), so we find that \(x\) is not an \(\ell\)-th power in the \(\ell\)-power cyclotomic extension \(K(\zeta_{\ell^\infty})\) of \(K\) for large \(k\). It follows that \(\Omega_{\ell}\) is a \(\mathbb{Z}/\ell\)-extension of \(K(\zeta_{\ell^\infty})\).

The proof of 4.1 distinguishes 3 cases, which are found in Theorems 4.3, 4.4 and 4.5. As we are dealing with a density statement, we will without further notice restrict to primes \(p\) for which \(x, \ell\) and the discriminant of \(K\) are all \(p\)-units. Such \(p\) are unramified in \(\Omega_{\ell}/\mathbb{Q}\).
We start with the easiest case, in which the prime \( p \) is split in \( K/\mathbb{Q} \). For \( K = \mathbb{Q} \) this is the only case, and it is for this case that Hasse formulated his method. For split \( p \), the group \( \kappa_p \) from (3.4) is a cyclic group of order \( p - 1 \). The reader may wish to identify \( \kappa_p \) with \( \mathbb{F}_p^* \), even though the isomorphism is non-canonical in the quadratic case. Let \( k \geq 0 \) be the number of factors \( \ell \) in \( p - 1 \). Then the order \( f_p(x) \) of \( x \) in \( \kappa_p \) is coprime to \( \ell \) if and only if \( x \) is contained in the subgroup \( \kappa_p^{\ell^k} \) of \( \ell^k \)-th powers in \( \kappa_p \). The condition that \( p - 1 \) has exactly \( k \) factors \( \ell \) and that \( x \) is an \( \ell^k \)-th power in \( \kappa_p \) may be formulated in terms of the splitting behavior of \( p \) in the normal number field

\[
F_k = K(\zeta_{\ell^{k+1}}, \sqrt[k]{x}).
\]

More precisely, the condition means that \( p \) splits completely in \( K(\zeta_{\ell^k}, \sqrt[k]{x}) \), but not in \( K(\zeta_{\ell^{k+1}}, \sqrt[k]{x}) \). We can now apply the Chebotarev density theorem as in [2, 3, 5, 9] to obtain the following.

**4.3. Split density theorem.** Let \( \ell \) and \( x \) be as in 4.1. Then the set of rational primes \( p \) that split completely in \( K = \mathbb{Q}(x) \) and for which \( f_p(x) \) is coprime to \( \ell \) has natural density

\[
\delta_{\ell}^+(x) = \sum_{k=0}^{\infty} \left( \frac{1}{[K(\zeta_{\ell^k}, \sqrt[k]{x}) : \mathbb{Q}]} - \frac{1}{[K(\zeta_{\ell^{k+1}}, \sqrt[k]{x}) : \mathbb{Q}]} \right).
\]

This density is a positive rational number strictly less than \([K : \mathbb{Q}]^{-1}\). In lowest terms, its denominator divides \([K : \mathbb{Q}] \cdot (\ell^2 - 1) \cdot \ell^\infty\).

**Proof.** For \( k \geq 0 \), we put \( d_k = [K(\zeta_{\ell^k}) : \mathbb{Q}] \) and write \( \Sigma_k \) for the set of primes \( p \) that split completely in \( K \) and have \( \text{ord}_\ell(p - 1) = k \). Then \( \Sigma_k \) has natural density \( d_k^{-1} - d_{k+1}^{-1} \), and the sum of these densities for all \( k \geq 0 \) is clearly equal to the density \( d_0^{-1} = [K : \mathbb{Q}]^{-1} \) of the primes that split completely in \( K/\mathbb{Q} \). The set of primes \( p \in \Sigma_k \) for which \( f_p(x) \) is coprime to \( \ell \) has natural density equal to the \( k \)-th term of the sum in 4.3. As densities do not in general add for infinite disjoint unions, we find a priori only that the given sum is a lower density for the set of primes under consideration. However, in this case we have in a similar way a lower density for the complementary set of primes that split in \( K/\mathbb{Q} \) and for which \( f_p(x) \) is not coprime to \( \ell \). As the lower densities for these complementary sets have sum \( d_0^{-1} \), they are densities.

All terms in the sum in 4.3 have denominators dividing \([K : \mathbb{Q}] \cdot (\ell - 1) \cdot \ell^\infty\). If we disregard finitely many terms, we have a geometric series with ratio \( \ell^{-2} \) in which the \( k \)-th term equals \((1 - 1/\ell)[K(\zeta_{\ell^k}, \sqrt[k]{x}) : \mathbb{Q}]^{-1}\). As \( \ell - 1 \) divides the numerator of \( 1 - 1/\ell \), summation yields a rational number of the indicated type.

The preceding argument further shows that the \( k \)-th term in 4.3 is positive for large \( k \) and equal to some fraction of the density of the set of primes \( \Sigma_k \) that decreases exponentially with \( k \). It follows that the sum is positive and strictly smaller than the density \([K : \mathbb{Q}]^{-1}\) of the set of splitting primes. \( \square \)
If $K = \mathbb{Q}(x)$ is quadratic with ring of integers $\mathcal{O}$, we need a complement to 4.3 in order to compute the density of the set of primes $p$ that are inert in $K$ and for which the order $f_p(x)$ of $x$ in the residue class field $\mathcal{O}/p\mathcal{O}$ is coprime to $\ell$. The approach is analogous to that in the split case, but the details are more involved. The inertia condition on $p$ forces us to look at the Galois structure of the extensions involved.

4.4. Inert density theorem for odd primes. Let $\ell \neq 2$ and $x$ be as in 4.1, and suppose that $K = \mathbb{Q}(x)$ is quadratic. Then the set of rational primes $p$ that are inert in $K$ and for which $f_p(x)$ is coprime to $\ell$ has a natural density. If $K$ is not the quadratic subfield of $\mathbb{Q}(\zeta_\ell)$, it equals

$$\delta_\ell^{-}(x) = \frac{\ell - 2}{2(\ell - 1)} + \sum_{k=1}^{\infty} \frac{\ell - 1}{[K(\zeta_{\ell^k+1}, \sqrt[k]{x}) : \mathbb{Q}]}.$$ 

If it is, we have $\delta_\ell^{-}(x) = \frac{1}{2}$ for $\ell \equiv 1 \pmod{4}$ and

$$\delta_\ell^{-}(x) = \frac{\ell - 3}{2(\ell - 1)} + \sum_{k=1}^{\infty} \frac{\ell - 1}{[K(\zeta_{\ell^k+1}, \sqrt[k]{x}) : \mathbb{Q}]}$$

for $\ell \equiv 3 \pmod{4}$. In all cases, $\delta_\ell^{-}(x)$ is rational. In lowest terms, its denominator divides $2 \cdot (\ell^2 - 1) \cdot \ell^\infty$.

Proof. As the group $\kappa_p$ from (3.4) is now the subgroup of order $p+1$ inside the cyclic group $(\mathcal{O}/p\mathcal{O})^*$ of order $p^2 - 1$, we let $\Sigma_k$ be the set of inert primes in $K/\mathbb{Q}$ with $\text{ord}_\ell(p+1) = k$.

The set $\Sigma_0$ consists of the primes $p \equiv -1 \pmod{\ell}$ that are inert in $K/\mathbb{Q}$. Clearly, for $p \in \Sigma_0$ any element in $\kappa_p$ has order coprime to $\ell$. If $K$ is not the quadratic subfield of $\mathbb{Q}(\zeta_\ell)$, then $\Sigma_0$ has density $\frac{\ell-2}{2(\ell-1)}$. If it is, then $\Sigma_0$ consists of the primes in the non-square residue classes modulo $\ell$ different from $-1 \pmod{\ell}$. For $\ell \equiv 3 \pmod{4}$, this is a set of density $\frac{\ell-3}{2(\ell-1)}$. For $\ell \equiv 1 \pmod{4}$, it is simply the set of all primes that are inert in $K/\mathbb{Q}$, and we immediately find $\delta_\ell^{-}(x) = \frac{1}{2}$. In the other cases, the density of $\Sigma_0$ contributes the ‘separate term’ to the indicated sum for $\delta_\ell^{-}(x)$. We further assume that we are in one of these cases, and continue with the contribution from the sets $\Sigma_k$ with $k > 0$.

Assume $k > 0$ for the rest of the proof. We have $\text{ord}_\ell(p+1) = k$ if and only if $p$ and $-1 + \ell^k$ generate the same subgroup of $(\mathbb{Z}/\ell^{k+1}\mathbb{Z})^*$. As $\ell$ is odd, this means that the multiplicative order of $p$ modulo $\ell^{k+1}$ equals $2\ell$. It follows that a prime $p$ is in $\Sigma_k$ for $k \geq 1$ if and only if its Frobenius substitution in $\text{Gal}(K(\zeta_{\ell^k+1})/\mathbb{Q})$ acts non-trivially on $K$ and has order $2\ell$ when restricted to $\mathbb{Q}(\zeta_{\ell^k+1})$. Let $B_k \subset K(\zeta_{\ell^k+1})$ be the fixed field of the subgroup generated by such a Frobenius element. Then $B_k$ is an abelian number field does not contain $K$ or $\mathbb{Q}(\zeta_\ell)$, and $K(\zeta_{\ell^k})$ is a quadratic extension of $B_k$ that is obtained by adjoining to $B_k$ a root of unity $\zeta_\ell$ or $\zeta_{\ell^k}$, or any generator of $K$ over $\mathbb{Q}$. 
Pick \( p \in \Sigma_k \). Then we have \( \text{ord}_\ell(p^2 - 1) = \text{ord}_\ell(p + 1) = k \), and for our element \( x \in K^* \) the order \( f_p(x) \) of \( (x \mod p) \) in \( \kappa_p \) is coprime to \( \ell \) exactly when it is an \( \ell^k \)-th power in \((O/\mathfrak{p}O)^*\). Thus, we have \( \ell \nmid f_p(x) \) if and only if \( p \) splits completely in \( B_k/Q \), remains inert in the cyclic extension \( B_k \subset K(\zeta_{\ell^k+1}) \) of degree \( 2\ell \) and splits again completely in \( K(\zeta_{\ell^k+1}) \subset K(\zeta_{\ell^k+1}, \zeta'(x)). \) We find that, just as in the split case, the primes \( p \in \Sigma_k \) with \( \ell \nmid f_p(x) \) can be characterized in terms of their splitting behavior in

\[ F_k = K(\zeta_{\ell^k+1}, \sqrt[\ell^k]{x}). \]

In order to prove our formula for \( \delta_\ell(x) \), it remains to show that there are exactly \( \ell - 1 \) Frobenius substitutions for \( p \) in \( \text{Gal}(F_k/Q) \) that correspond to this splitting behavior. Proving this requires knowledge of the structure of the Galois group \( \text{Gal}(F_k/B_k) \).

We claim that, with \( y = \sqrt[\ell^k]{x} \) some \( \ell^k \)-th root of \( x \), the extension \( B_k \subset F_k \) is a linearly disjoint compositum of a cyclic extension \( B_k \subset B_k(y+1/y) \) of \( \ell \)-power degree and a cyclic extension \( B_k \subset K(\zeta_{\ell^k+1}) \) of degree \( 2\ell \). In terms of these fields, our splitting condition on \( p \) is simply that the Frobenius substitution of \( p \) in \( \text{Gal}(F_k/Q) \) is one of the \( \ell - 1 \) generators of the normal cyclic subgroup \( \text{Gal}(F_k/B_k(y + y^{-1})) \) of order \( 2\ell \), so proving this claim finishes the proof of 4.4.

As for our claim, we show first that \( B_k \subset B_k(y) \) is a cyclic extension of degree twice an \( \ell \)-power. Let \( \varphi_k^* \in \text{Gal}(B_k(y)/B_k) \) be an element of order 2. As \( \ell \) is odd, \( \varphi_k^* \) extends the generator \( \varphi_k \in \text{Gal}(B_k(x)/B_k) \). It therefore acts by inversion both on \( x \) and on the \( \ell^k \)-th roots of unity. The Galois equivariancy of the Kummer pairing

\[ \text{Gal}(B_k(y)/B_k(x)) \times \langle x \rangle \rightarrow \langle \zeta_{\ell^k} \rangle \]

now implies that the conjugation action of \( \varphi_k \) on \( \text{Gal}(B_k(y)/B_k(x)) \) is trivial, and that \( \text{Gal}(B_k(y)/B_k) \), being the direct product of the cyclic groups \( \text{Gal}(B_k(y)/B_k(x)) \) and \( \langle \varphi_k^* \rangle \) of coprime order, is cyclic.
We finally need to show that $\zeta_{2k+1}$ and $y$ generate independent extensions of $K(\zeta_{2k})$. As $y$ generates a cyclic extension of $\ell$-power degree, it suffices to show that its subextension $E$ of degree $\ell$ over $K(\zeta_{2k})$, if it exists, is not the cyclotomic extension $K(\zeta_{2k})$ of $K$. As $E$ is obtained by extraction of an $\ell$-th power of an element of $K$, it is not even abelian over $K$ whenever $K$ does not contain a primitive $\ell$-th root of unity. As $K$ is quadratic, we have $\zeta_{\ell} \in K$ only for $\ell = 3$ and $K = \mathbb{Q}(\zeta_3)$. 

The preceding proof has to be modified in various ways for $\ell = 2$.

4.4. Inert density theorem at $2$. **

**Proof.** We let $\Sigma_k$ be the set of inert primes $p > 2$ in $K/\mathbb{Q}$ with $\text{ord}_2(p+1) = k$.

The set $\Sigma_0$ is empty, and $\Sigma_1$ consists of the primes $p \equiv 1 \mod{4}$ that are inert in $K/\mathbb{Q}$. For $K = \mathbb{Q}(i)$ this is again the empty set. For $p \in \Sigma_1$ the norm relation $N(x) = x^{p+1} = 1 \in \kappa_p$ shows that there is at most one factor 2 in $f_p(x)$, and that $f_p(x)$ is odd exactly when $x$ is the square of an element in $\kappa_p$. We have $x = y^2$ for some $y \in (\mathcal{O}/p\mathcal{O})^*$ of norm ±1. As $x$ and $y$ are both quadratic over $\mathbb{F}_p$, we have $y + 1/y \in \mathbb{F}_p$ for $N(y) = 1$ and $y - 1/y \in \mathbb{F}_p$ for $N(y) = -1$. The identity $(y + 1/y)^2 = \text{Tr}(x) + 2 \in \mathbb{F}_p$ shows that we have $N(y) = 1$ exactly when $\text{Tr}(x) + 2$ is a square modulo $p$.

We can find the element $y$ in the preceding argument as the reduction modulo $p$ of a global square root $y = \sqrt{x}$ of $x$. The extension $\mathbb{Q} \subset K(\sqrt{x})$ is either quadratic (if $x$ is a square in $K$) or Galois with group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the latter case the quadratic subfields are $K$ and the fields $\mathbb{Q}(y \pm 1/y) = \mathbb{Q}(\sqrt{\text{Tr}_{K/\mathbb{Q}}(x)} \pm 2)$. Thus $p \in \Sigma_1$ has $f_p(x)$ odd if and only if the Frobenius substitution of $p$ in $\text{Gal}(K(i, \sqrt{x})/\mathbb{Q})$ is the unique element that leaves $i$ and $\sqrt{\text{Tr}_{K/\mathbb{Q}}(x)} + 2$ invariant but not $x$. The corresponding density is $[K(i, \sqrt{x}) : \mathbb{Q}]^{-1}$ for all $K \neq \mathbb{Q}(i)$.

For $k \geq 2$ we are dealing with primes $p \equiv 3 \mod{4}$, and in this case $p \in \Sigma_k$ implies $\text{ord}_2(p^2-1) = k+1$. The primes in $\Sigma_k$ are the primes for which the Frobenius substitution in $\text{Gal}(K(\zeta_{2k+1})/\mathbb{Q})$ is the element $\varphi$ of order 2 that raises $\zeta_{2k+1}$ to the power $-1 + 2^k$ and inverts $x$. As in the proof of 3.8, we let $B_k$ be the invariant field of $\langle \varphi \rangle$. This time the order $f_p(x)$ for $p \in \Sigma_k$ is odd exactly when $x$ is a $2^{k+1}$-th power modulo $p$. The higher exponent means that we have to work in the slightly larger field

$$F_k = B_k(\sqrt[2^{k+1}]{x}) = K(\zeta_{2^{k+1}}, \sqrt[2^{k+1}]{x}).$$

The primes we want for each $k \geq 1$ are those $p$ that split completely in $B_k/\mathbb{Q}$, are inert in the quadratic extension $B_k(x)/B_k$ and then again split completely in the cyclic 2-power extension $F_k/B_k(x)$. Whether this is possible depends on the structure of the Galois group $\text{Gal}(F_k/B_k)$, for which there are various possibilities.

\[\square\]

5. Explicit densities for torsion sequences

For every given torsion sequence, the theorems in the preceding section enable us to compute the density of the set of its prime divisors. The large number of possibilities for
the various field degrees and Galois groups in the previous section makes clear that it is not feasible to give a general expression for $\delta_X$ in terms of the class $[q, r]$ of the sequence.

*** The computation is easy if the $\ell$-power cyclotomic extension $K(\zeta_\ell^\infty)$ is linearly disjoint over $K$ from every extension $K(\sqrt[\ell]{x})$ obtained by adjoining some $\ell$-power root of $x$ to $K$. Especially for $\ell = 2$, this is not in general the case.

As before, we let the exponent of an element $x \in K_N^* \setminus \mu_K$ be the order of the torsion subgroup of $K_N^*/\mu_K \cdot (x)$. If $K$ contains no primitive $\ell$-th root of unity, the exponent of $x$ is the largest integer $e$ for which $x$ is an $\ell$-th power in $K^*$.

3.11. Proposition. Let $\ell$ be an odd prime, and $\ell^t$ the largest $\ell$-power dividing the exponent of $x \in K_N^* \setminus \mu_K$. Write $c_K = [K(\zeta_\ell) : \mathbb{Q}(\zeta_\ell)] \in \{1, 2\}$, and let $\delta_\ell^+$ be the density of the set of primes that are split in $K$ for which $\ell$ divides $f_p(x)$. Then we have

$$\delta_\ell^+ = c_K^{-1} \cdot \frac{\ell^{1-t}}{t^2 - 1},$$

unless we have $\ell = 3$ and $x$ is not a $3^t$-th power in $K^*$. In this particular case we have

$$\delta_3^+ = \frac{1}{8}(4 - 3^{-t}).$$

Proof. For $\ell > 3$, there is no primitive $\ell$-th root of unity in $K$, and we can write $x = y^{\ell^t}$ for some $y \in K^*$ that is not an $\ell$-th power in $K^*$. Then $y$ is not an $\ell$-th power in any cyclotomic extension $K(\zeta_\ell^k)$ of $K$, because $K(\sqrt[t]{y})$ is not a normal number field and therefore not a subfield of the abelian number field $K(\zeta_\ell^k)$.

By Kummer theory, we find that $\sqrt[t]{x}$ generates a cyclic extension of degree $\ell^{\max(0,k-t)}$ of both $K(\zeta_\ell^k)$ and $K(\zeta_\ell^{k+1})$. We write $d_k = [K(\zeta_\ell^k) : \mathbb{Q}]$ as in the proof of 4.2. We are dealing here with the primes for which $f_p(x)$ is not coprime to $\ell$, so we obtain

$$d_0^{-1} - \delta_\ell^+ = \sum_{k=0}^{t} (d_k^{-1} - d_{k+1}^{-1}) + \sum_{k=t+1}^{\infty} \ell^{t-k} (d_k^{-1} - d_{k+1}^{-1}).$$

The terms $d_0^{-1}$ cancel, and plugging in $d_k = c_K \phi(\ell^k) = c_K (\ell^k - \ell^{k-1})$ for $k \geq 1$ yields the indicated value of $\delta_\ell^+$.

For $\ell = 3$, the preceding analysis fails only when we have $K = \mathbb{Q}(\zeta_3)$ and $x = \zeta_3 y^{3^t}$ for some $t > 0$. In this case, the terms with $k = t$ in the sum in 4.2 vanish, and we find $\frac{1}{2} - \delta_3^+ = \sum_{k=t+1}^{\infty} 3^{t-k} (d_k^{-1} - d_{k+1}^{-1}) = \sum_{k=t+1}^{\infty} 3^{t-2k} = 3^{-t}/8$. The desired formula follows.

The analysis for $\ell = 2$ is more complicated for a number of reasons. Even when $K$ is not a quadratic subfield of $\mathbb{Q}(\zeta_8)$ and $x$ is of exponent 1, the extension $K \subset K(\sqrt{2})$ can be a subextension of $K \subset K(\sqrt{5})$.

3.12. Proposition. ** $\ell = 2$ **
3.13. Proposition. Let \( \ell \) be a prime, and \( \ell^t \) the largest \( \ell \)-power dividing the exponent of \( x \in K_N^* \setminus \mu_K \). Write \( c_K = [K(\zeta_\ell) : \mathbb{Q}(\zeta_\ell)] \in \{1, 2\} \), and let \( \delta^+_\ell \) be the density of the set of primes that are inert in \( K \) and for which \( \ell \) divides \( f_p(x) \). Then we have

\[
*** \delta^+_\ell = c_K^{-1} \cdot \frac{\ell^{1-t}}{\ell^2 - 1}.
\]

for \( \ell > 3 \), or for \( \ell = 3 \) when \( x \) is a \( 3^t \)-th power in \( K^* \). For \( \ell = 3 \) and \( x \) not a \( 3^t \)-th power in \( K^* \), we have

\[
\delta^+_3 = \frac{1}{8} (4 - 3^{-t}).
\]

Proof.
References


Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands.
E-mail address: psh@math.leidenuniv.nl