Uniform explicit Stewart’s theorem on prime factors of linear recurrences

Yuri Bilu\textsuperscript{a}, Sanoli Gun\textsuperscript{b} and Haojie Hong\textsuperscript{c}

Version of October 4, 2022

\textit{To the memory of Andrzej Schinzel}

Abstract

Stewart (2013) proved that the biggest prime divisor of the \(n\)th term of a Lucas sequence of integers grows quicker than \(n\), answering famous questions of Erdős and Schinzel. In this note we obtain a fully explicit and, in a sense, uniform version of Stewart’s result.

Contents

1 Introduction 1
2 Notation and preliminaries 4
3 Logarithmic forms 5
4 Proof of Theorem 1.4 6
5 Quadratic fields 9
6 Multiplicatively independent elements 10
7 Proof of Theorem 1.6 13
8 Cyclotomic polynomials and primitive divisors 16
9 Proof of Theorem 1.7 17
10 Proof of Theorem 1.9 19

1 Introduction

For a non-zero algebraic number \(\gamma\), denote by \(\omega(\gamma)\) the number of distinct primes \(p\) of the field \(\mathbb{Q}(\gamma)\) with the property \(\nu_p(\gamma) \neq 0\). We denote by \(N\gamma\) the \(\mathbb{Q}\)-norm: \(N\gamma = N_{\mathbb{Q}(\gamma)/\mathbb{Q}}(\gamma)\).

The following theorem was proved by Stewart in his seminal article \[16\].

\textsuperscript{a}Supported by the SPARC Project P445 (India) and ANR project JINVARIANT
\textsuperscript{b}Supported by the SPARC Project P445 (India)
\textsuperscript{c}Supported by the China Scholarship Council grant CSC202008310189
Theorem 1.1. Let $\gamma$ be a non-zero algebraic number, not a root of unity, satisfying the following:

- either $\gamma \in \mathbb{Q}$,
- or $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2$ and $N\gamma = \pm 1$.

Then there exists $n_0$, depending only on $\omega(\gamma)$ and the field $K = \mathbb{Q}(\gamma)$, with the following property. For every $n > n_0$ there exists a prime $p$ of $K$, with the underlying rational prime $p$, such that $\nu_p(\gamma^n - 1) \geq 1$ and

$$p \geq n \exp \left( \frac{1}{104} \log n \right).$$

This result answered famous questions posed by Erdős and Schinzel, see the introduction of [16] for a historical account.

Note that Stewart’s [16, Theorem 1.1] is stated in different terms, but what he actually proves is exactly Theorem 1.1 above.

In this note we re-examine Stewart’s argument with the following objectives:

**(uniformity)** we show that Stewart’s $n_0$ depends only on $\mathbb{Q}(\gamma)$, but not on $\omega(\gamma)$; in particular, if $\gamma \in \mathbb{Q}$ then $n_0$ is an absolute constant;

**(explicitness)** we obtain a totally explicit expression for $n_0$.

We prove the following two theorems.

**Theorem 1.2.** Let $\gamma$ be a non-zero rational number, distinct from $\pm 1$. Set $n_0 = \exp(10^6)$. Then for every $n \geq n_0$ there is a prime number $p$ such that $\nu_p(\gamma^n - 1) \geq 1$ and $p \geq n \exp \left( 0.0005 \frac{\log n}{\log \log n} \right)$.

**Theorem 1.3.** Let $\gamma$ be a non-zero algebraic number of degree 2, not a root of unity. We denote $D_K$ the discriminant of the number field $K = \mathbb{Q}(\gamma)$, and we set $n_0 = \exp \exp \left( \max \{10^9, 3|D_K|\} \right)$. Assume that $N\gamma = \pm 1$. Then for every $n \geq n_0$ there exists a prime $p$ of $K$, with the underlying rational prime $p$, such that $\nu_p(\gamma^n - 1) \geq 1$ and

$$p \geq n \exp \left( 0.0002 \frac{\log n}{\log \log n} \right).$$

Our numerical constants 0.0005 and 0.0002 are worse than Stewart’s 1/104. On the other hand, our $n_0$ do not depend on $\omega(\gamma)$. Our argument, being very close to Stewart’s, allows one, in principle, to obtain 1/104 (but, probably, not 1/102), for the price of increasing the numerical value of $n_0$.

We deduce Theorems 1.2 and 1.3 from the following two theorems (again, essentially, due to Stewart, see [16, Section 4]), which are of independent interest. We denote by $h(\cdot)$ the absolute logarithmic height, see Section 2. We also denote $\log^* = \max\{\log, 1\}$, and we denote by $\mathcal{N}p$ the absolute norm of the ideal $p$; that is, $\mathcal{N}p = \#O_K/p$. 

2
Theorem 1.4. Let $\gamma$ be a non-zero algebraic number of degree $d$, not a root of unity. Set $p_0 = \exp(80000d(\log^* d)^2)$. Then for every prime $p$ of the field $K = \mathbb{Q}(\gamma)$ with $N_p \geq p_0$, and every positive integer $n$ we have
\[ \nu_p(\gamma^n - 1) \leq N_p \exp \left( -0.002d^{-1} \frac{\log N_p}{\log \log N_p} \right) h(\gamma) \log^* n. \]

Theorem 1.5. Let $\gamma$ be as in Theorem 1.3; that is, a non-zero algebraic number of degree 2 and norm $\pm 1$, but not a root of unity. We again denote $D_K$ the discriminant of the field $K = \mathbb{Q}(\gamma)$, and we set $p_0 = \exp(\exp(\max\{10^8, 2|D_K|\}))$. Then for every prime $p$ of $K$ with underlying rational prime $p \geq p_0$, and every positive integer $n$ we have
\[ \nu_p(\gamma^n - 1) \leq p \exp \left( -0.001 \frac{\log p}{\log \log p} \right) h(\gamma) \log^* n. \] (1.1)

Remark 1.6. 1. The principal tool in the proof of Theorem 1.2 is Theorem 1.4, which holds not only for $\gamma \in \mathbb{Q}$, but for arbitrary algebraic $\gamma$. One may wonder whether Theorem 1.2 can be extended to this generality. One may expect the following statement: for $n$ large enough, there exists a prime $p$ of the number field $\mathbb{Q}(\gamma)$ such that $\nu_p(\gamma^n - 1) \geq 1$ and $N_p \geq n \exp \left( c \frac{\log n}{\log \log n} \right)$, where $c$ is a positive number not depending on $n$.

Unfortunately, the present argument does not seem to be capable of proving this. See Remark 9.1 for more details.

2. Our values of $n_0$ and $p_0$ are rather huge numerically. In particular, in Theorems 1.3 and 1.5 our $n_0$, respectively $p_0$, are double exponential in $|D_K|$. Of course, this is quite unsatisfactory for practical purposes. Unfortunately, not much can be done here without involving substantially new ideas. The reason is that we have to use the numerical Prime Number Theorem from [2] (see Proposition 5.2). And using this theorem requires parameter $x$ therein to be exponential in $|D_K|$. Since in the subsequent proof of Theorem 1.5 this $x$ is set to be around $\log p$, this yields double exponential dependence in $|D_K|$. Note also that the original approach of Stewart leads to even triple exponential dependence, as explained in Section 6.

We follow the main lines of Stewart’s argument, with two changes. Uniformity in $\gamma$ is achieved by using Lemmas 4.1 and 7.1. Another deviation of Stewart’s argument is of more technical nature and is explained in detail in Section 6.

Plan of the article Our principal tool is Yu’s [19] bound for a $p$-adic logarithmic form. In Section 3 we present a simplified version of Yu’s result adapted for our purposes. In Section 4 we prove Theorem 1.4.

In Section 5 and 6 we collect various facts about quadratic fields used in the proof of Theorem 1.5 which is proved afterwards in Section 7.
In Section 8 we recall basic facts about cyclotomic polynomials and primitive divisors, needed for the proofs of Theorems 1.2 and 1.3. These latter are proved in the final Sections 9 and 10 respectively.

2 Notation and preliminaries

Let $K$ be a number field. We denote by $D_K$ and $h_K$ the discriminant and the class number of $K$. By a prime of $K$ we mean a prime ideal of the ring of integers $\mathcal{O}_K$. We denote by $\mathbb{F}_p$ the residue field $\mathcal{O}_K/p$, and $Np = \#\mathbb{F}_p$ the absolute norm of $p$.

Let $a, b$ be non-zero fractional ideals of $K$. We call them involved if there exists a $K$-prime $p$ such that $\nu_p(a), \nu_p(b) \neq 0$. If no such prime exists, then we call $a, b$ disjoint (so that “not involved” and “disjoint” are synonyms). We call $\alpha, \beta \in K^\times$ involved, resp. disjoint if so are the principal ideals $(\alpha), (\beta)$.

We denote by $h(\alpha)$ the usual absolute logarithmic height of $\alpha \in \overline{\mathbb{Q}}$:

$$h(\alpha) = [K : \mathbb{Q}]^{-1} \sum_{v \in M_K} d_v \log^+ |\alpha|_v,$$

where $\log^+ = \max\{\log, 0\}$ and $d_v$ denotes the local degree. Here $K$ is an arbitrary number field containing $\alpha$, and the places $v \in M_K$ are normalized to extend the standard places of $\mathbb{Q}$; that is, $|p|_v = p^{-1}$ if $v | p < \infty$ and $|x|_v = |x|$ if $v | \infty$ and $x \in \mathbb{Q}$.

If $K$ is a number field of degree $d$ and $\alpha \in K$ then the following formula is an immediate consequence of the definition of the height:

$$h(\alpha) = \frac{1}{d} \left( \sum_{\sigma : K \rightarrow \mathbb{C}} \log^+ |\alpha^\sigma| + \sum_p \max\{0, -\nu_p(\alpha)\} \log Np \right),$$

where the first sum runs over the complex embeddings of $K$ and the second sum runs over the primes of $K$. If $\alpha \neq 0$ then $h(\alpha) = h(\alpha^{-1})$, and we obtain the formula

$$h(\alpha) = \frac{1}{d} \left( \sum_{\sigma : K \rightarrow \mathbb{C}} -\log^- |\alpha^\sigma| + \sum_p \max\{0, \nu_p(\alpha)\} \log Np \right),$$

(2.1)

where $\log^- = \min\{\log, 0\}$.

Besides $\log^+$ and $\log^-$ we will also use $\log^* = \max\{\log, 1\}$.

We use $O_1(\cdot)$ as the quantitative version of the familiar $O(\cdot)$ notation: $A = O_1(B)$ means $|A| \leq B$.

We will use the following estimates for the arithmetical functions $\omega(n), \varphi(n)$
and \( \pi(x) \):

\[
\omega(n) \leq 1.4 \frac{\log n}{\log \log n} \quad (n \geq 3), \quad (2.2)
\]

\[
\varphi(n) \geq 0.5 n \frac{\log \log n}{\log n} \quad (n \geq 10^{20}), \quad (2.3)
\]

\[
\frac{x}{\log x} \leq \pi(x) \leq 1.3 \frac{x}{\log x} \quad (x \geq 3). \quad (2.4)
\]

See [12, Théorème 11], [13, Theorem 15] and [13, page 69, Corollary 1].

### 3 Logarithmic forms

In this section, \( K \) is a number field of degree \( d \), and \( p \) is a prime of \( K \) with underlying rational prime \( p \geq 5 \). Note that we will have \( p \geq 5 \) in both Sections 4 and 7, where Theorem 3.1 will be applied: see (4.5) and (7.3). Let \( u \) be such that \( K \) contains a primitive root of unity of order \( 2^u \), but not of order \( 2^{u+1} \).

We pick a primitive root of unity of order \( 2^u \) and denote it \( \zeta \).

Our principal tool will be the following result of Yu [19]. Recall that \( \alpha \in K^\times \) is called a \( p \)-adic unit if \( \nu_p(\alpha) = 0 \).

**Theorem 3.1.** Let \( \alpha_1, \ldots, \alpha_k \in K^\times \) be multiplicatively independent \( p \)-adic units. Let \( \delta \) and \( \Omega \) be real numbers satisfying

\[
\delta \leq \begin{cases} 
[p^\times_p : \langle \zeta, \alpha_1, \ldots, \alpha_k \rangle], & \text{if } [K(\alpha_1^{1/2}, \ldots, \alpha_k^{1/2}) : K] = 2^k, \\
1, & \text{otherwise},
\end{cases}
\]

\[
\Omega = \max \left\{ \frac{N_p}{\delta} \left( \frac{k}{\log N_p} \right)^k, e^{k \log N_p} \right\},
\]

where \( \langle \zeta, \alpha_1, \ldots, \alpha_k \rangle \) is the subgroup of the multiplicative group \( F_p^\times \) generated by the images of \( \zeta, \alpha_1, \ldots, \alpha_k \).

Furthermore, let \( b_1, \ldots, b_k \) be rational integers, not all 0, and denote

\[
B = \max \{|b_1|, \ldots, |b_k|\}.
\]

Then

\[
\nu_p(\alpha_1^{b_1} \cdots \alpha_k^{b_k} - 1) \leq 10^5 d^{k+2}(\log^* d)^3 \cdot 30^k K^{5/2}(\log^* k) h(\alpha_1) \cdots h(\alpha_k) \Omega \log^* B.
\]

**Proof.** This is a simplification (with slightly bigger numerical constants) of [16 Lemma 3.1], which, on its own, is a simplification of the main theorem of [19].

Let us explain how we deduce (3.1) from [16 Lemma 3.1]. Note that our \( k \) corresponds to \( n \) in [16]. We will repeatedly use the observations of the following kind: for \( a \geq 0 \) and \( x, y \geq 1 \) we have \( a + x + y \leq (a + 2)xy \).
Plugging the estimates

\[
\max\{\log^* B, (k + 1)(5.4k + \log d)\} \leq \log^* B \cdot 13k^2 \log^* d, \\
(k + 1)^{1/2} \leq \sqrt{2}k^{1/2}, \\
7e \frac{p - 1}{p - 2} \leq \frac{28}{3}e \quad \text{(recall that } p \geq 5), \\
\log(e^4(k + 1)d) \leq 8 \log^* d \log^* k
\]

into \[\text{[16 Lemma 3.1]} \] (with \(n\) replaced by \(k\)), we bound the left-hand side of (3.1) by

\[
376 \left(\frac{28}{3}e\right)^k d^{k^2} \cdot 104 \sqrt{2}k^{5/2} \log^* k(\log^* d)^3 h(\alpha_1) \cdots h(\alpha_k) \Omega \log^* B. \tag{3.2}
\]

This is clearly smaller than the right-hand side of (3.1).

\[\square\]

4 Proof of Theorem \[\ref{thm:main} \]

The following lemma is totally trivial, but we state it here because it is our principal tool in making \(p_0\) independent of \(\gamma\).

**Lemma 4.1.** Let \(K\) be a field, \(\gamma_1, \ldots, \gamma_k \in K^\times\) multiplicatively independent, and \(\gamma \in K^\times\) not a root of unity. Then, after a suitable renumbering of \(\gamma_1, \ldots, \gamma_k\), the numbers \(\gamma, \gamma_2, \ldots, \gamma_k\) become multiplicatively independent.

We will also need a lower bound for the height of an algebraic number.

**Lemma 4.2.** Let \(\gamma\) be an algebraic number of degree \(d\), not a root of unity. Then

\[
\begin{align*}
\h(\gamma) &\geq \log 2 & \text{for } d = 1, \\
2\h(\gamma) &\geq \log \left(1 + \sqrt{5}\right) & \text{for } d = 2, \\
\h(\gamma) &\geq \frac{1}{4(\log^* d)^3} & \text{for any } d.
\end{align*}
\]

**Proof.** Inequality (4.1) is trivial, and (4.2) is a famous result of Schinzel [15, see also [6] for a very simple proof]. Inequality (4.3), for sufficiently large \(d\), follows from the famous work of Dobrowolski [5]. To obtain it for all \(d \geq 3\), we invoke Voutier’s numerical adaptation [17] of Dobrowolski’s result. In particular, [17, Corollary 2] gives \(\h(\gamma) \geq 2/(\log(3d))^3\), which clearly implies (4.3) for \(d \geq 3\). Finally, for \(d \leq 2\) inequality (4.3) follows from (4.1) and (4.2).

We can now start the proof of Theorem [17]. To simplify notation, we denote \(\mathcal{N}p = p_0 = \exp(80000d(\log^* d)^2)\) (4.4)
throughout the proof. Since \( Np \leq p^d \), we have
\[
p \geq p_0^{1/d} \geq \exp(80000(\log^* d)^2) \geq 5,
\]
which is required to apply Theorem 3.1.

Let \( x \) be specified later to satisfy
\[
x \geq 200(\log^* d)^2.
\]
(4.6)

Denote \( k = \pi(x) \). Let \( \ell_1, \ldots, \ell_k \) be the \( k \) primes not exceeding \( x \) numbered somehow, not necessarily in the increasing order. Since \( \ell_1, \ldots, \ell_k \) are multiplicatively independent and \( \gamma \) is not a root of unity, Lemma 4.1 implies that, after renumbering, the numbers \( \gamma, \ell_2, \ldots, \ell_k \) are multiplicatively independent.

We apply Theorem 3.1 with
\[
\alpha_1 = \frac{\gamma}{\ell_2 \cdots \ell_k}; \quad \alpha_i = \ell_i \quad (i = 2, \ldots, k);
\]
\[
b_i = n \quad (i = 1, \ldots, k); \quad \delta = 1.
\]

Since \( h(\ell_i) = \log \ell_i \leq \log x \), we obtain
\[
\nu_p(\gamma^n - 1) = \nu_p(\alpha_1^n \ell_2^n \cdots \ell_k^n - 1)
\leq 10^5 d^{k+2}(\log^* d)^3 \cdot 30^k k^{5/2}(\log^* k)h(\alpha_1)(\log x)^{k-1} \Omega \log^* n,
\]
where \( \Omega = \max\{P(k/\log P)^k, e^k \log P\} \). We will see later, when we specify \( x \), that
\[
P(k/\log P)^k \geq e^k \log P,
\]
(4.7)
and so we have \( \Omega = P(k/\log P)^k \).

Using Lemma 4.2, we estimate
\[
h(\alpha_1) \leq h(\gamma) + (k - 1) \log x \leq 4d(\log^* d)^3 h(\gamma) k \log x.
\]

Hence
\[
\nu_p(\gamma^n - 1) \leq 4 \cdot 10^5 d^3(\log^* d)^3 k^{5/2}(\log^* k)P \left( \frac{30dk \log x}{\log P} \right)^k h(\gamma) \log^* n.
\]

We want to simplify this estimate.

It follows from (4.6) that \( k \geq \pi(200) = 46 \), which easily implies that
\[
4 \cdot 10^5 k^{5/2}(\log^* k) \leq 2^k.
\]

Also, using (2.4), we obtain
\[
k \geq \frac{200(\log^* d)^2}{\log(200(\log^* d)^2)},
\]

which implies that $d^3 (\log^* d)^6 \leq 2^k$. Indeed, this is obvious when $d = 1, 2$. When $d \geq 3$, it is sufficient to prove that

$$\frac{200 (\log d)^2}{\log(200) + 2 \log \log d} \geq \frac{3 \log d + 6 \log \log d}{\log 2}.$$  

This is true since $200 \log 2 (\log d)^2 \geq 9 \log d (\log 200 + 2 \log d)$ holds when $d \geq 3$.

Finally, again using (2.4), we estimate $k \log x \leq 1.3x$. Since

$$2 \cdot 2 \cdot 1.3 \cdot 30 < 160,$$

this implies the estimate

$$\nu_p(\gamma - 1) \leq P \left( \frac{160dx}{\log P} \right)^k h(\gamma) \log^* n. \quad (4.8)$$

It is the time to specify $x$. We set $x = (1/400d) \log P$, which gives

$$\nu_p(\gamma - 1) \leq P \cdot 0.4^k h(\gamma) \log^* n. \quad (4.9)$$

Note that (4.6) is satisfied with our choice of $x$, because of (4.4).

Now we are almost done. Once again using (2.4), we obtain

$$k \geq \frac{x}{\log x} \geq \frac{1}{400d \log \log P}.$$  

Substituting this to (4.9), we obtain

$$\nu_p(\gamma - 1) \leq P \exp \left( -0.002d^{-1} \frac{\log P}{\log \log P} \right) h(\gamma) \log^* n,$$

as wanted.

We are left with checking that assumption (4.7) holds true with our choice of $x$. It suffices to show that $P \geq (e \log P)^{k+1}$. As we have seen above, $k \geq 46$, and we use (2.4) to obtain

$$k + 1 \leq \frac{47}{46} \pi(x) \leq 1.4 \frac{x}{\log x} \leq \frac{1.4}{400 \log ((1/400) \log P)}.$$

Since $P \geq e^{80000}$, we have

$$\frac{1}{400} \log P \geq (\log P)^{0.4}, \quad e \log P \leq (\log P)^{1.1}.$$  

It follows that

$$k + 1 \leq 0.009 \frac{\log P}{\log \log P}, \quad (e \log P)^{k+1} \leq P^{0.01} \leq P.$$  

This completes the proof of the theorem.
5 Quadratic fields

We need to recall some facts about quadratic fields. In this section, unless otherwise stated, \( K \) denotes a quadratic field. We denote by \( D_K \) and \( h_K \) the discriminant and the class number of \( K \) respectively. If \( K \) is a real quadratic field then we denote by \( \eta_K \) the fundamental unit \( \eta \) satisfying \( \eta > 1 \). It will be convenient to set \( \eta_K = 1 \) for imaginary \( K \). We denote by \( \sigma \) the non-trivial Galois morphism of \( K \) over \( \mathbb{Q} \). Note that, when \( K \) is real, we have

\[
\eta_K \geq \frac{1 + \sqrt{5}}{2}. \tag{5.1}
\]

We set \( \mu = \# \mathcal{O}_K^\times / 2; \) in other words,

\[
\mu = \begin{cases} 
3, & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\
2, & \text{if } K = \mathbb{Q}(i), \\
1, & \text{in all other cases.}
\end{cases}
\]

Proposition 5.1.

1. Let \( K \) be an imaginary quadratic field. Then

\[
h_K \leq \mu \pi^{-1/2} |D_K|^{1/2} (2 + \log |D_K|). \tag{5.2}
\]

2. Let \( K \) be a real quadratic field. Then

\[
h_K \log \eta_K \leq \pi^{-1/2} D_K^{1/2} (2 + \log D_K). \tag{5.3}
\]

3. For any quadratic field, \( K \), we have

\[
h_K \leq 3 |D_K|^{1/2} \log |D_K|, \tag{5.4}
\]

\[
\log \eta_K \leq |D_K|^{1/2} \log |D_K|. \tag{5.5}
\]

Proof. Estimates (5.2) and (5.3) are well-known; see, for instance, Theorems 10.1 and 14.3 in [8, Chapter 12]. Estimate (5.4) follows, in the imaginary case, from \( \mu \leq 3 \) and \( |D_K| \geq 3 \), and in the real case from (5.1) and \( |D_K| \geq 5 \). Finally, (5.5) is trivial in the imaginary case, and in the real case it follows from \( h_K \geq 1 \) and \( D_K \geq 5 \).

Denote by \( \pi_s(x, K) \) the counting function of rational primes that split in \( K \).

Proposition 5.2. For

\[
x \geq \max\{10^{10}, e^{|D_K|}\} \tag{5.6}
\]

we have

\[
\pi_s(x, K) \geq \frac{1}{2} \frac{x}{\log x} - \frac{\varphi(|D_K|)}{320} \frac{x}{(\log x)^2}. \tag{5.7}
\]
Proof. We denote \( D = D_K \). An odd rational prime \( p \) splits in \( K \) if and only if \((D/p) = 1\). Primes satisfying this condition belong to one of \( \varphi(|D|)/2 \) residue classes mod\( |D| \). If \( a \) mod \( |D| \) is one such class, then for \( x \) satisfying (5.6) we have
\[
\pi(x; |D|, a) \geq \frac{1}{\varphi(|D|)} \operatorname{Li}(x) - \frac{1}{160} \frac{x}{(\log x)^2},
\]
see Theorem 1.3 in Bennett et al. \[2\]. As usual, we denote by \( \pi(x; m, a) \) the counting function for primes in the congruence class \( a \) mod \( m \).

Note that \( \operatorname{Li}(x) > x/\log x \) for \( x \geq 7 \), because the function
\[
f(x) = \operatorname{Li}(x) - x/\log x
\]
satisfies \( f'(x) = 1/(\log x)^2 > 0 \) and \( f(7) = 0.114 \ldots > 0 \). It follows that
\[
\pi(x; |D|, a) \geq \frac{1}{\varphi(|D|)} \frac{x}{\log x} - \frac{1}{160} \frac{x}{(\log x)^2}.
\]
Summing up over the \( \varphi(|D|)/2 \) residue classes \( a \) mod \( |D| \), we obtain (5.7).

\section{6 Multiplicatively independent elements}

We retain the notation and conventions of Section 5.

Stewart’s argument in the quadratic case \[16, \text{Section 4}\] requires producing in \( K \) many multiplicatively independent elements of norm 1 and controllable height. Stewart uses for this purpose prime numbers \( p \) with the following properties:

- \( p \) splits in \( K \), and
- the \( K \)-primes above \( p \) are principal.

We call them \textit{Stewart primes} in the sequel.

Let \( \pi \) be a principal \( K \)-prime above a Stewart prime \( p \). If \( K \) is imaginary then \( |\pi| = |\pi^\sigma| = p^{1/2} \). If \( K \) is real then, multiplying \( \pi \) by a suitable power of the fundamental unit \( \eta_K \), we may assume that \( (p/\eta_K)^{1/2} \leq |\pi|, |\pi^\sigma| \leq (p\eta_K)^{1/2} \).

Stewart associates to \( p \) the algebraic number \( \theta_p = \pi/\pi^\sigma \). For this \( \theta_p \) we have \( N\theta_p = 1 \), and
\[
h(\theta_p) = \frac{1}{2} \log p + O_1 \left( \frac{1}{2} \log \eta_K \right);
\]
recall that \( O_1(\cdot) \) is quantitative version of \( O(\cdot) \), see Section 2. Clearly, numbers \( \theta_p \) corresponding to distinct Stewart primes \( p \) are multiplicatively independent.

Using the Class Field Theory and the Tchebotarev Density Theorem, one can show that the relative density of Stewart primes in the set of all primes is \((2h_K)^{-1}\). Moreover, using recent explicit versions of the Tchebotarev Density Theorem, as in \[1, 9, 18\], one can give a totally explicit lower estimate for the counting function of Stewart primes.
Unfortunately, following this path, we end up with a rather huge value for the constant $p_0$ in Theorem 1.5, triple exponential in the discriminant of $K$. For instance, Theorem 5 of [9] applies for $x \geq x_1 := \exp(|D_L|^{1/2})$, where, in our case, $L$ is the Hilbert Class Field of $K$. We have $|D_L| = |D_K|^{h_K}$, which would lead to a double exponential value for $x_1$. And $p_0$, as it is clear from the proof of Theorem 1.5, is exponential in $x_1$, leading to the triple exp dependence of $p_0$ in $|D_K|$. For this reason, we do not pursue this approach in the present article.

Instead of Stewart primes, which are quite sparse, we use all (sufficiently large) split primes, which have relative density $1/2$. More precisely, denote by $S(K)$ the set of rational primes $p$ which split in $K$ and satisfy $p \geq |D_K|^{1/2}$. To every $p \in S(K)$ we want to associate a certain element $\theta_p \in K$. We do it as follows.

Given $p \in S(K)$, let $p$ be a $K$-prime above $p$. Recall that every ideal class contains an integral ideal $a$ such that $N(a) < |D_K|^{1/2}$. We take such $a$ in the class of $p^{-1}$, so that $pa$ is a principal ideal. Let $\alpha$ be a generator of $pa$. Then $|\alpha\alpha^*| = N(pa)$. Note also that, since $N(a) < |D_K|^{1/2}$, the number $\alpha$ is not involved with any prime from the set $S(K)$ other than $p$ itself.

If $K$ is imaginary then $|\alpha| = |\alpha^*| = N(pa)^{1/2}$. If $K$ is real then, multiplying $\alpha$ by a suitable power of $\eta_K$, we may assume that

$$N(pa)^{1/2} \eta_K^{-1/2} \leq |\alpha|, |\alpha^*| \leq N(pa)^{1/2} \eta_K^{1/2}. \tag{6.1}$$

Now we set

$$\theta_p = \alpha/\alpha^*.$$

**Proposition 6.1.**

1. For every $p \in S(K)$ we have $N\theta_p = 1$ and

$$h(\theta_p) = \frac{1}{2} \log p + O_1 \left( \frac{1}{4} \log |D_K| + \frac{1}{2} \log \eta_K \right).$$

2. In particular, if $p \geq \exp(100|D_K|^{1/2} \log |D_K|)$ then

$$h(\theta_p) \leq 0.51 \log p. \tag{6.2}$$

3. Each $\theta_p$ is involved with $p$, but disjoint from any other prime exceeding $|D_K|^{1/2}$. In particular, it is disjoint from any prime belonging to the set $S(K)$. If $p$ is a $K$-prime over $p$, then $\nu_p(\theta_p) = \pm 1$.

4. If $p_1, \ldots, p_k$ are distinct elements of $S(K)$ then $\theta_{p_1}, \ldots, \theta_{p_k}$ are multiplicatively independent. Moreover, $[K(\sqrt{\theta_{p_1}}, \ldots, \sqrt{\theta_{p_k}}) : K] = 2^k$.

**Proof.** Items 1 and 2 follow from (6.1), the definition of $\theta_p$ and the upper bound $N(a) < |D_K|^{1/2}$. To prove item 4 it suffices to show that

$$0.01 \log p \geq \frac{1}{4} \log |D_K| + \frac{1}{2} \log \eta_K.$$
In view of (5.5), this would follow from
\[ \log p \geq 100 \left( \frac{1}{4} \log |D_K| + \frac{1}{2} |D_K|^{1/2} \log |D_K| \right). \]

And this is a consequence of our assumption about \( p \).

To prove item 4, denote
\[ L_i = K \left( \sqrt{\theta_{p_1}}, \ldots, \sqrt{\theta_{p_i}} \right) \]
(with the convention \( L_0 = K \)), and let \( p_i \) be a prime of \( K \) above \( p_i \). Item 3 implies that \( p_i \) ramifies in \( L_i \) but not in \( L_{i-1} \). Hence \( [L_i : L_{i-1}] = 2 \), whence the result.

Item 2 of this proposition suggests to count the split primes \( p \) satisfying \( p \geq \exp(100|D_K|^{1/2} \log |D_K|) \). The following is an immediate consequence of Proposition 5.2.

**Corollary 6.2.** For \( x \geq \exp(\text{max}\{10^7, |D_K|\}) \) we have
\[ \pi_s(x, K) - \pi_s(\exp(100|D_K|^{1/2} \log |D_K|), K) \geq 0.49 \frac{x}{\log x}. \]

**Proof.** Using Proposition 5.2,
\[ \pi_s(x, K) - \pi_s(\exp(100|D_K|^{1/2} \log |D_K|), K) \]
\[ \geq \frac{1}{2} \frac{x}{\log x} - \frac{\varphi(|D_K|)}{320} \frac{x}{(\log x)^2} - \exp(100|D_K|^{1/2} \log |D_K|). \] (6.3)

Let us estimate both the extra terms in the right-hand side of (6.3). We have \( \log x \geq |D_K| \), which implies that
\[ \frac{\varphi(|D_K|)}{320} \frac{x}{(\log x)^2} \leq \frac{1}{320} \frac{x}{\log x}. \]

Next, using \( \log x \geq |D_K| \) and \( \log x \geq 10^7 \), we obtain
\[ 100|D_K|^{1/2} \log |D_K| \leq 100(\log x)^{1/2} \log x < 0.6 \log x. \]

Hence
\[ \exp(100|D_K|^{1/2} \log |D_K|) < x^{0.6} < 10^{-10} \frac{x}{\log x}, \]
where we again use the assumption \( \log x \geq 10^7 \).

We conclude that the right-hand side of (6.3) exceeds
\[ \left( \frac{1}{2} - \frac{1}{320} - 10^{-10} \right) \frac{x}{\log x}, \]
which is bigger than \( 0.49 x / \log x \).  \( \square \)
7 Proof of Theorem 1.5

As in Section 4, we start from a simple lemma.

**Lemma 7.1.** Let $K$ be a field of characteristic 0, let $\gamma_1, \ldots, \gamma_k \in K^\times$ be such that

$$[K(\sqrt{\gamma_1}, \ldots, \sqrt{\gamma_k}) : K] = 2^k,$$

and let $\gamma \in K^\times$ be not a square in $K$. Then, after suitable renumbering $\gamma_1, \ldots, \gamma_k$, we have

$$[K(\sqrt{\gamma}, \sqrt{\gamma_2}, \ldots, \sqrt{\gamma_k}) : K] = 2^k. \quad (7.1)$$

**Proof.** Let $\bar{\gamma}, \bar{\gamma}_1, \ldots, \bar{\gamma}_k$ be the images of $\gamma, \gamma_1, \ldots, \gamma_k$ in the group $K^\times/(K^\times)^2$. Viewing the latter as an $F_2$-vector space, the vectors $\bar{\gamma}_1, \ldots, \bar{\gamma}_k$ are linearly independent and vector $\bar{\gamma}$ is non-zero. Hence, after renumbering, vectors $\bar{\gamma}, \bar{\gamma}_2, \ldots, \bar{\gamma}_k$ become linearly independent. This yields (7.1) by Kummer’s theory, as given, for instance, in [10, Section VI.8]. Indeed, Theorem 8.1 therein implies that

$$[K(\sqrt{\gamma}, \sqrt{\gamma_2}, \ldots, \sqrt{\gamma_k}) : K] = [\Gamma : (K^\times)^2],$$

where $\Gamma$ is the subgroup of $K^\times$ generated by $\gamma, \gamma_2, \ldots, \gamma_k$ and $(K^\times)^2$. The quotient $\Gamma/(K^\times)^2$ is isomorphic, as $F_2$-vector space, to the space generated by $\bar{\gamma}, \bar{\gamma}_2, \ldots, \bar{\gamma}_k$. Hence $[\Gamma : (K^\times)^2] = 2^k$, and we are done. \qed

Now we are ready to start the proof of Theorem 1.5. In this section, $K = \mathbb{Q}(\gamma)$ and $p$ is a prime of $K$, whose underlying rational prime $p$ satisfies

$$p \geq p_0 = \exp\exp(\max\{10^8, 2|D_K|\}). \quad (7.2)$$

In particular,

$$p \geq 5, \quad (7.3)$$

which is required to apply Theorem 3.1.

If $Np = p$ then Theorem 1.5 follows from the case $d = 2$ of Theorem 1.4. Therefore we will assume that $Np = p^2$. In particular, the residue field $\mathbb{F}_p$ is the finite field $\mathbb{F}_{p^2}$.

Let $x$ be a positive real number to be specified later to satisfy

$$x \geq \exp(\max\{10^7, |D_K|\}). \quad (7.4)$$

The results of Section 6 imply the following. There exists a positive integer $k$ and distinct prime numbers $\ell_1, \ldots, \ell_k \in S(K)$ such that

$$k \geq 0.49 \frac{x}{\log x}, \quad \ell_i \leq x,$$

$$h(\theta_{\ell_i}) \leq 0.51 \log x \quad (1 \leq i \leq k). \quad (7.5)$$

Note also that

$$k \leq \pi(x) \leq 1.3 \frac{x}{\log x}. \quad (7.6)$$
Next, let $r$ be the biggest positive integer with the following property: there exists $\theta \in K^\times$ such that $\theta^r = \gamma$. This $\theta$ is not a square in $K$ by the definition of $r$, and Lemma \ref{lemma:theta_not_square} implies that, after renumbering $\ell_1, \ldots, \ell_k$, we have

$$[K(\sqrt{\theta}, \sqrt{\theta\ell_2}, \ldots, \sqrt{\theta\ell_k}) : K] = 2^k.$$

Denote by $G$ the subgroup of the multiplicative group $F_p^\times = F_p^{x}$, consisting of elements of norm $\pm 1$:

$$G = \{x \in F_p^\times : \mathcal{N}_{F_p^2/F_p} x = \pm 1\}.$$

Since the norm map $\mathcal{N} : F_p^\times \to F_p^\times$ is surjective (see, for instance, \cite[Theorem 2.28(ii)]{28}), we have $[F_p^\times : G] = (p-1)/2$. The $F_p$-images of $\theta, \sqrt{\theta\ell_2}, \ldots, \sqrt{\theta\ell_k}$ belong to $G$. Hence we can use Theorem \ref{thm:height_bound} with

$$\alpha_1 = \frac{\theta}{\theta\ell_2 \cdots \theta\ell_k}; \quad \alpha_i = \theta\ell_i \quad (i = 2, \ldots, k);$$

$$b_i = nr \quad (i = 1, \ldots, k); \quad \delta = \frac{p-1}{2}; \quad d = 2.$$

Note that $\alpha_1, \ldots, \alpha_k$ are $p$-adic units, as required in Theorem \ref{thm:height_bound}. Indeed, item 3 of Proposition \ref{prop:unit_prop} implies that each $\alpha_i$ is disjoint from any rational prime exceeding $|D_K|^{1/2}$, except perhaps $\ell_1, \ldots, \ell_k$. We have $p \neq \ell_1, \ldots, \ell_k$ (because $p$ is inert in $K$, and the primes $\ell_i$ split in $K$), and $p \geq |D_K|^{1/2}$ by (7.2). Hence $\alpha_i$ is disjoint from $p$, that is, it is a $p$-adic unit.

Using the upper bound (7.5) for the heights of $\theta\ell_i$'s, we obtain

$$\nu_p(\gamma^n - 1) = \nu_p(\alpha_1^{nr} \theta\ell_2^{nr} \cdots \theta\ell_k^{nr} - 1) \leq 10^6 \cdot 60^k 5^{k/2} \log^* k h(\alpha_1)(0.51 \log x)^{k-1} \Omega \log^*(nr), \quad (7.7)$$

where

$$\Omega = \max \left\{ \frac{2p^2}{p-1} \left( \frac{k}{2 \log p} \right)^k, 2e^k \log p \right\}.$$

We will see later that

$$\Omega = \frac{2p^2}{p-1} \left( \frac{k}{2 \log p} \right)^k \quad (7.8)$$

with our choice of $x$. Using $p \geq p_0$, this implies that

$$\Omega \leq 2.1p \left( \frac{k}{2 \log p} \right)^k.$$ 

Next, we have $2h(\theta) \geq \log((1 + \sqrt{5})/2)$ by Lemma \ref{lemma:theta_height}. Using this, the definition of $\alpha_1$ and the upper bound (7.5) for the height of the $\theta\ell_i$'s, we estimate

$$h(\alpha_1) \leq h(\theta) + 0.51(k-1) \log x \leq 5h(\theta) k \log x = \frac{5}{r} h(\gamma) k \log x.$$
Also, a quick verification shows that \( \log^*(nr) \leq r \log^*n \) for all possible choices of \( n \) and \( r \). Substituting all these estimates into (7.7), we obtain

\[
\nu_p(\gamma^n - 1) \leq 10^8k^{7/2}(\log^*k)p \left( \frac{15.3k \log x}{\log p} \right)^k \log(\gamma) \log^*n.
\]

We want to simplify this estimate. It follows from (7.4) that

\[
k \geq 0.49 \frac{x}{\log x} \geq \exp(10^6),
\]

which easily implies that \( 10^8k^{7/2}(\log^*k) < 1.1^k \). Also, \( k \log x \leq 1.3x \) by (7.6). Since \( 1.1 \cdot 1.3 \cdot 15.3 < 30 \), we obtain the estimate

\[
\nu_p(\gamma^n - 1) \leq p \left( \frac{30x}{\log p} \right)^k \log(\gamma) \log^*n.
\]

Now we set \( x = 300^{-1} \log p \). Then (7.4) is satisfied, and we have

\[
\nu_p(\gamma^n - 1) \leq p \cdot 0.1^k \log(\gamma) \log^*n.
\]

Since

\[
k \geq 0.49 \frac{x}{\log x} > \frac{0.001 \log p}{\log \log p},
\]

we obtain

\[
\nu_p(\gamma^n - 1) \leq p \exp \left( -0.002 \frac{\log p}{\log \log p} \right) \log(\gamma) \log^*n,
\]

which is even better than wanted.

It remains to verify that (7.8) holds with our choice of \( x \). It suffices to prove that \( p > (2e \log p)^{k+1} \). Using the lower estimates \( p \geq \exp \exp(10^8) \) and \( x \geq \exp(10^7) \) (see (7.2), (7.4)) together with the upper estimate (7.6), we obtain

\[
k + 1 < \frac{1.4x}{\log x} = \frac{1.4 \log p}{300 \log \log p - \log 300} < 0.01 \frac{\log p}{\log \log p}
\]

and \( \log(2e \log p) < 2 \log \log p \). It follows that \( (k + 1) \log(2e \log p) < \log p \). This completes the proof of the theorem.

8 Cyclotomic polynomials and primitive divisors

In this section, we collect some results on cyclotomic polynomials and primitive divisors. We denote by \( \Phi_n(t) \) the cyclotomic polynomial of order \( n \). Recall that \( \deg \Phi_n = \varphi(n) \), the Euler totient.

The following results go back to Schinzel [14], but in the present form they can be found in [4]. Recall (see Section 2) that \( A = O_1(B) \) means \( |A| \leq B \).
Proposition 8.1. 1. Let $\gamma$ be an algebraic number. Then

$$h(\Phi_n(\gamma)) = \varphi(n)h(\gamma) + O_1(2^{\omega(n)}\log(\pi n)).$$

2. Let $\gamma$ be a complex algebraic number of degree $d$, non-zero and not a root of unity. Then

$$\log |\Phi_n(\gamma)| \geq -10^{14}d^3(h(\gamma) + 1) \cdot 2^{\omega(n)} \log(n + 1) \quad (8.1).$$

Proof. Item 1 is [4, Theorem 3.1]. Item 2 follows from [4, Corollary 3.5], which gives the inequality

$$\log |\Phi_n(\gamma)| \geq -10^3d^3(h(\gamma) + 1) \cdot 2^{\omega(n)} \log(n + 1).$$

We have clearly $\log(n + 1) \leq 1$. Also, Lemma 4.2 implies that

$$d(h(\gamma) + 1) \leq d(h(\gamma) + 1) \cdot 2^{\omega(n)} \log(n + 1).$$

This proves (8.1).

Let $K$ be a number field of degree $d$ and $\gamma \in K^\times$ not a root of unity. We consider the sequence $u_n = \gamma^n - 1$. We call a $K$-prime $p$ primitive divisor of $u_n$ if

$$\nu_p(u_n) \geq 1, \quad \nu_p(u_k) = 0 \quad (k = 1, \ldots, n - 1).$$

Let us recall some basic properties of primitive divisors.

Proposition 8.2. 1. Let $p$ be a primitive divisor of $u_n$. Then $\nu_p(\Phi_n(\gamma)) \geq 1$ and $\mathcal{N} \equiv 1 \mod n$; in particular, $\mathcal{N} \geq n + 1$.

2. Let $p$ be a primitive divisor of $u_n$ and $p$ the rational prime underlying $p$. If $\gamma$ is of degree 2 and absolute norm 1, then $p \equiv \pm 1 \mod n$.

3. Assume that $n \geq 2^{d+1}$. Let $p$ be not a primitive divisor of $u_n$. Then $\nu_p(\Phi_n(\gamma)) \leq \nu_p(n)$.

Proof. Item 3 is Lemma 4 of Schinzel [14]; see also [4, Lemma 4.5]. Items 1 and 2 are well-known, but we include short proofs for the reader’s convenience.

To prove item 1 note first of all that we must have $\nu_p(\gamma) = 0$, because $\nu_p(\gamma^n - 1) > 0$. Furthermore,

$$\nu_p(\gamma^n - 1) = \sum_{m|n} \nu_p(\Phi_m(\gamma)),$$

where each summand is non-negative because $\nu_p(\gamma) = 0$. Since $p$ is a primitive divisor of $u_n$, we must have $\nu_p(\Phi_m(\gamma)) = 0$ for every $m < n$. It follows that $\nu_p(\Phi_n(\gamma)) = \nu_p(\gamma^n - 1) \geq 1$.

Let $\bar{\gamma}$ be the image of $\gamma$ in $\mathbb{F}_p = \mathcal{O}_K/p$. Then saying that $p$ is a primitive divisor of $\gamma^n - 1$ is equivalent to saying that $n$ is the order of $\bar{\gamma}$ in the multiplicative group $\mathbb{F}_p^\times$. In particular, $n$ must divide $\mathcal{N} - 1$, the order of this group. This complete the proof of item 1.
In item 2 if $Np = p$ then the result follows from item 1 (and we do not need the assumption $N\gamma = 1$). Now assume that $Np = p^2$. The subgroup 
\[ \{ x \in \mathbb{F}_p^\times : N_{F/F_p} x = 1 \} \]
is of order $p + 1$, because the norm map is surjective \[11, \text{Theorem 2.28(ii)}\]. Since $\tilde{\gamma}$ belongs to this subgroup, we must have $n \mid (p + 1)$. This proves item 2. 

\[ \square \]

9 Proof of Theorem 1.2

We set $n_0 = \exp(10^6)$ and we assume that $n \geq n_0$ in the sequel.

Let $P$ be the biggest prime number $p$ with the property $\nu_p(\Phi_n(\gamma)) \geq 1$. We want to show that 
\[ P \geq n \exp \left( 0.0005 \frac{\log n}{\log \log n} \right). \tag{9.1} \]
We will deduce this from Theorem 1.4, used with $d = 1$, and the properties of cyclotomic polynomials and primitive divisors collected in Section 8.

We apply equation (2.1) with $\alpha = \Phi_n(\gamma)$. Here $d = 1$, and we obtain the following:
\[ h(\Phi_n(\gamma)) = -\log -|\Phi_n(\gamma)| + \sum_p \max\{0, \nu_p(\Phi_n(\gamma))\} \log p. \tag{9.2} \]

We estimate the first term in (9.2) using item 2 of Proposition 8.1:
\[ -\log -|\Phi_n(\gamma)| \leq 10^{14} h(\gamma) \cdot 2^{\omega(n)} \log n. \tag{9.3} \]
Next, let us call $p$ primitive if it is a primitive divisor of $\gamma^n - 1$, as defined in Section 8 and non-primitive otherwise. We split the sum in (9.2) into two sums:
\[ \sum_p \max\{0, \nu_p(\Phi_n(\gamma))\} \log p = \sum_{p \text{ primitive}} + \sum_{p \text{ non-primitive}} = \Sigma_p + \Sigma_{np}. \]
We estimate $\Sigma_{np}$ using item 3 of Proposition 8.2:
\[ \Sigma_{np} \leq \sum_p \nu_p(n) \log p = \log n. \]

Thus,
\[ h(\Phi_n(\gamma)) \leq 10^{14} h(\gamma) \cdot 2^{\omega(n)} \log n + \log n + \Sigma_p. \]
On the other hand, item 1 of Proposition 8.1 implies the lower bound
\[ h(\Phi_n(\gamma)) \geq \varphi(n) h(\gamma) - 2^{\omega(n)} \log(\pi n). \]
Combining the two bounds, we obtain the following lower estimate for $\Sigma_p$:
\[ \Sigma_p \geq \varphi(n) h(\gamma) - 2^{\omega(n)} \log(\pi n) - 10^{14} h(\gamma) \cdot 2^{\omega(n)} \log n - \log n. \tag{9.4} \]
Inequalities (2.2), (2.3) and our assumption \( n \geq \exp(10^6) \) imply that the right-hand side of (9.4) is bounded from below by \( 0.9 \varphi(n) h(\gamma) \). Thus, we obtain the lower estimate

\[
\Sigma_p \geq 0.9 \varphi(n) h(\gamma).
\] (9.5)

Now let us bound \( \Sigma_p \) from above. Recall that primitive \( p \) satisfy \( p \equiv 1 \mod n \). In particular, \( p \geq n + 1 > n_0 \). Since our \( n_0 \) is bigger than the \( p_0 \) from Theorem 1.4, the latter applies, and we obtain, for primitive \( p \), the estimate

\[
\nu_p(\Phi_n(\gamma)) = \nu_p(\gamma^n - 1) \leq p \exp \left( -0.002 \frac{\log p}{\log \log p} \right) h(\gamma) \log n.
\]

Since \( p > n > e^e \), we have

\[
\frac{\log p}{\log \log p} \geq \frac{\log n}{\log \log n}.
\]

Hence

\[
\nu_p(\Phi_n(\gamma)) \leq P \exp \left( -0.002 \frac{\log n}{\log \log n} \right) h(\gamma) \log n.
\]

It follows that

\[
\Sigma_p \leq \sum_{p \equiv 1 \mod n, p \leq P} \max \{0, \nu_p(\Phi_n(\gamma))\} \log p
\]

\[
\leq \pi(P; n, 1) h(\gamma) P \exp \left( -0.002 \frac{\log n}{\log \log n} \right) \log n \log P,
\]

where, as usual, \( \pi(x; m, a) \) counts primes \( p \leq x \) satisfying \( p \equiv a \mod m \). To estimate \( \pi(P; n, 1) \), Stewart uses the Brun-Titchmarsh inequality. However, just the trivial estimate \( \pi(P; n, 1) \leq P/n \) would suffice. We obtain

\[
\Sigma_p \leq 2h(\gamma) P^2 \log P \exp \left( -0.002 \frac{\log n}{\log \log n} \right) \frac{\log n}{n}.
\] (9.6)

Thus, we have a lower bound (9.5) and an upper bound (9.6) for \( \Sigma_p \). Combining the two, we obtain

\[
P^2 \log P \geq 0.4 \frac{n \varphi(n)}{\log n} \exp \left( 0.002 \frac{\log n}{\log \log n} \right).
\]

We may assume that \( P < n^2 \), since otherwise there is nothing to prove. Using this assumption and (2.3), we obtain

\[
2P^2 \log n \geq P^2 \log P
\]

\[
\geq 0.4 \frac{n \varphi(n)}{\log n} \exp \left( 0.002 \frac{\log n}{\log \log n} \right)
\]

\[
\geq 0.2 \frac{n^2}{\log n \log \log n} \exp \left( 0.002 \frac{\log n}{\log \log n} \right).
\]
This can be re-written as
\[ P \geq \sqrt{0.1} \frac{n}{\log n \log \log n} \exp \left( 0.001 \frac{\log n}{\log \log n} \right). \]

Since \( n \geq \exp(10^6) \), we must have
\[ \sqrt{0.1} \frac{n}{\log n \log \log n} \exp \left( 0.001 \frac{\log n}{\log \log n} \right) \geq n \exp \left( 0.0005 \frac{\log n}{\log \log n} \right). \]

Hence (9.1) is proved.

Remark 9.1. As it is already indicated in the introduction, Theorem 1.2 holds not only for \( \gamma \in \mathbb{Q} \), but for arbitrary algebraic \( \gamma \), and one may wonder whether Theorem 1.2 can be extended to this generality, like: for \( n \) large enough, there exists a prime \( p \) of the number field \( \mathbb{Q}(\gamma) \) such that
\[ \nu_p(\gamma^n - 1) \geq 1, \quad Np \geq n \exp \left( c \frac{\log n}{\log \log n} \right), \]
where \( c \) is a positive number not depending on \( n \).

Unfortunately, the present argument does not seem to be capable of proving this. The reason is that, when \( \gamma \notin \mathbb{Q} \), there is no good bound for the number of \( p \) satisfying \( Np \equiv 1 \mod n \). For instance, if \( \gamma \) is of degree 2, we have to count rational primes satisfying \( p^2 \equiv 1 \mod n \). Since the ring \( \mathbb{Z}/n\mathbb{Z} \) may have as much as \( 2^{\omega(n)} \) square roots of unity, we cannot obtain, without involving extra ideas, an upper bound sharper than \( 2^{\omega(n)} \) for the number of such primes. And, since \( \omega(n) \) can be of magnitude as big as \( \log n / \log \log n \), this would destroy the tiny gain \( \exp \left( -0.002d^{-1} \frac{\log Np}{\log \log Np} \right) \) obtained in Theorem 1.4.

In the case \( d = 2 \) this difficulty is overcome in \( 7 \), using ideas from the previous article \( 3 \). However, the case \( d \geq 3 \) remains open.

10 Proof of Theorem 1.3

We follow the proof of Theorem 1.2 with appropriate modification. In particular, we set \( n_0 = \exp(\exp(\max\{10^9, 3|D_K|\})) \) and we assume that \( n \geq n_0 \) throughout the proof.

Let \( P \) be the biggest element of the set
\[ \{ p : p \text{ is a rational prime lying below a prime } p \text{ of } K, \text{ with } \nu_p(\Phi_n(\gamma)) \geq 1 \}. \]

We want to show that
\[ P \geq n \exp \left( 0.0002 \frac{\log n}{\log \log n} \right). \] (10.1)

We apply equation (2.1) with \( \alpha = \Phi_n(\gamma) \). Here \( d = 2 \), and we obtain
\[ 2h(\Phi_n(\gamma)) = -\log^- |\Phi_n(\gamma)| - \log^- |\Phi_n(\gamma^7)| + \sum_p \max\{0, \nu_p(\Phi_n(\gamma))\} \log Np, \] (10.2)
where $\sigma$ is the non-trivial morphism of $\mathbb{Q}(\gamma)/\mathbb{Q}$.

We use item 2 of Proposition 8.1 to estimate the first term of (10.2):

$$- \log^{-|\Phi_n(\gamma)|} - \log^{-|\Phi_n(\gamma^\sigma)|} \leq 2^6 \cdot 10^{14} \cdot h(\gamma) \cdot 2^{\omega(n)} \log n. \quad (10.3)$$

We split the sum in (10.2) into two parts:

$$\sum_p \max \{0, \nu_p(\Phi_n(\gamma))\} \log Np = \sum_{p \text{ primitive}} + \sum_{p \text{ non-primitive}} = \Sigma_p + \Sigma_{np}.$$

By item 3 of Proposition 8.2 we can bound the non-primitive part,

$$\Sigma_{np} \leq \sum_p \nu_p(n) \log Np \leq 2 \log n.$$  

Thus

$$h(\Phi_n(\gamma)) \leq 10^{16} h(\gamma) \cdot 2^{\omega(n)} \log n + \Sigma_p/2 + \log n. \quad (10.4)$$

On the other hand, by item 1 of Proposition 8.1

$$h(\Phi_n(\gamma)) \geq \varphi(n) h(\gamma) - 2^{\omega(n)} \log(\pi n) \quad (10.5)$$

Combining (10.4) and (10.5), we have

$$\Sigma_p/2 \geq \varphi(n) h(\gamma) - 2^{\omega(n)} \log(\pi n) - 10^{16} h(\gamma) 2^{\omega(n)} \log n - \log n \quad (10.6)$$

Inequalities (2.2), (2.3) and our assumption $n \geq n_0 \geq \exp(\exp(10^9))$ imply that the right-hand side of (10.6) is bounded from below by $0.9 \varphi(n) h(\gamma)$. Thus, we obtain the lower estimate

$$\Sigma_p \geq 1.8 \varphi(n) h(\gamma). \quad (10.7)$$

Now let us bound $\Sigma_p$ from above. By item 1 of Proposition 8.2, a primitive divisor $p$ of $\gamma^n - 1$ satisfies $Np \equiv 1 \mod n$. In particular $Np \geq n + 1$ and thus the underlying rational prime $p$ is bigger than $\sqrt{n_0} = \exp(\exp(\max\{10^9, 3|D_K|\}/2)$, which is bigger than the $p_0$ in Theorem 1.5. So we obtain, for primitive $p$ with underlying prime $p$,

$$\nu_p(\Phi_n(\gamma)) = \nu_p(\gamma^n - 1) \leq p \exp \left( -0.001 \frac{\log p}{\log \log p} \right) h(\gamma) \log n.$$  

Since $p^2 \geq Np > n > e^\varepsilon$, we have

$$\frac{\log p}{\log \log p} \geq \frac{1}{2} \frac{\log n}{\log \log n}.$$  

Hence

$$\nu_p(\Phi_n(\gamma)) \leq h(\gamma) P \exp \left( -0.0005 \frac{\log n}{\log \log n} \right) \log n.$$  

20
Using this and items 1, 2 of Proposition 8.2, we obtain
\[
\sum_p \leq \sum_{Np \equiv 1 \pmod{n}} \max\{0, \nu_p(\Phi_n(\gamma))\} \log Np
\]
\[
\leq 2(\pi(P; n, 1) + \pi(P; n, -1))h(\gamma) P \exp \left(-0.0005 \frac{\log n}{\log \log n}\right) \log n \log P.
\]
As in Section 9 we estimate trivially \(\pi(P; n, 1) + \pi(P; n, -1) \leq 2P/n\). We obtain
\[
\Sigma_p \leq 8h(\gamma)P^2 \log P \exp \left(-0.0005 \frac{\log n}{\log \log n}\right) \frac{\log n}{n}.
\]
(10.8)
Combining the lower bound (10.7) the upper bound (10.8), we obtain
\[
P^2 \log P \geq 0.1 \frac{n\varphi(n)}{\log n} \exp \left(0.0005 \frac{\log n}{\log \log n}\right).
\]
Using again \(n \geq \exp(10^9)\) we obtain (10.1), arguing as in the end of the proof of Theorem 1.2 in Section 4.

Acknowledgments  Yuri Bilu and Sanoli Gun acknowledge support of the SPARC Project P445 “Arithmetical aspects of the Fourier coefficients of modular forms”. Yuri Bilu was also supported by the ANR project JINVARIANT. Haojie Hong was supported by the China Scholarship Council grant CSC202008310189.

The authors thank Keith Conrad, Florian Luca, Kevin O’Bryant and Fabien Pazuki for useful discussions. We especially thank the anonymous referee for careful reading of the manuscript and many suggestions, that helped us to correct mistakes and improve the presentation.

References

[1] Jeoung-Hwan Ahn and Soun-Hi Kwon, Lower estimates for the prime ideal of degree one counting function in the Chebotarev density theorem, Acta Arith. 191 (2019), no. 3, 289–307. MR 4017533
[2] Michael A. Bennett, Greg Martin, Kevin O’Bryant, and Andrew Rechnitzer, Explicit bounds for primes in arithmetic progressions, Illinois J. Math. 62 (2018), no. 1-4, 427–532. MR 3922423
[3] Yuri Bilu, Haojie Hong, and Florian Luca, Big prime factors in orders of elliptic curves over finite fields, Publ. Math. Debrecen, to appear; arXiv:2112.07046, 2021.
[4] Yuri Bilu and Florian Luca, Binary polynomial power sums vanishing at roots of unity, Acta Arith. 198 (2021), no. 2, 195–217. MR 4228301
[5] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. 34 (1979), no. 4, 391–401. MR 543210
[6] G. Höhn and N.-P. Skoruppa, Un résultat de Schinzel, J. Théor. Nombres Bordeaux 5 (1993), no. 1, 185. MR 1251237
[7] Haojie Hong, Stewart’s theorem revisited: suppressing the norm ±1 hypothesis, Bol. Soc. Mat. Mex. (3) 28 (2022), no. 3, Paper No. 60. MR 4462796
[8] Loo Keng Hua, *Introduction to number theory*, Springer-Verlag, Berlin-New York, 1982, Translated from the Chinese by Peter Shiu. MR 665428

[9] Habiba Kadiri and Peng-Jie Wong, *Primes in the Chebotarev density theorem for all number fields (with an Appendix by Andrew Fiori)*, J. Number Theory 241 (2022), 700–737. MR 4472459

[10] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556

[11] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn. MR 1429394

[12] Guy Robin, *Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction ω(n) nombre de diviseurs premiers de n*, Acta Arith. 42 (1983), no. 4, 367–389. MR 736719

[13] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94. MR 137689

[14] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. 268(269) (1974), 27–33. MR 344221

[15] Addendum to the paper: “On the product of the conjugates outside the unit circle of an algebraic number” (Acta Arith. 24 (1973), 385–399), Acta Arith. 26 (1974/75), no. 3, 329–331. MR 371853

[16] Cameron L. Stewart, *On divisors of Lucas and Lehmer numbers*, Acta Math. 211 (2013), no. 2, 291–314. MR 3143892

[17] Paul Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. 74 (1996), no. 1, 81–95. MR 1367580

[18] Bruno Winckler, *Théorème de Chebotarev effectif*, arXiv:1311.5715, 2013.

[19] Kunrui Yu, *p-adic logarithmic forms and a problem of Erdős*, Acta Math. 211 (2013), no. 2, 315–382. MR 3143893

**Yuri Bilu & Haojie Hong:** Institut de Mathématiques de Bordeaux, Université de Bordeaux & CNRS, Talence, France

**Sanoli Gun:** The Institute of Mathematical Sciences, Taramani, Chennai, Tamil Nadu, India