Big prime factors in orders of elliptic curves over finite fields

Yuri Bilu\textsuperscript{a}, Haojie Hong\textsuperscript{b} and Florian Luca\textsuperscript{a}

December 15, 2021

Abstract

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$. We prove that, when $n$ is a sufficiently large positive integer, $\#E(\mathbb{F}_{q^n})$ has a prime factor exceeding $n \exp(c \log n / \log \log n)$.

Contents

1 Introduction 1
   1.1 Notation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
2 Auxiliary facts 4
   2.1 The Theorems of Stewart . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
   2.2 Cyclotomic polynomials and primitive divisors . . . . . . . . . . . . . . . . . 4
   2.3 Counting $S$-units . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
3 Proof of Theorem 1.1 7
   3.1 Case (3.3) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
   3.2 Case (3.4) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

1 Introduction

A Lucas sequence $(u_n)_{n \geq 0}$ is a binary recurrent sequence of integers satisfying $u_{n+2} = ru_{n+1} + su_n$ for all $n \geq 0$, and with $u_0 = 0$, $u_1 = 1$. The parameters $r$, $s$ are assumed to be nonzero coprime integers such that $r^2 + 4s \neq 0$. In this case,

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

holds for all $n \geq 0$,

where $\alpha, \beta$ are the two roots of the quadratic $x^2 - rx - s = 0$. It is further assumed that $\alpha/\beta$ is not a root of unity. The Lucas sequences have nice divisibility properties. For example, if $m$, $n$ are positive integers with $m \mid n$ then $u_m \mid u_n$.

A primitive divisor of $u_n$ is a prime factor $p$ of $u_n$ which does not divide $u_m$ for any positive integer $m < n$ and does not divide $r^2 + 4s$. Working with

\textsuperscript{a}Supported by the ANR project JINVARIANT

\textsuperscript{b}Supported by the China Scholarship Council grant CSC202008310189
the sequence of algebraic integers of general term \( v_n = (\alpha - \beta)u_n = \alpha^n - \beta^n \), one can reformulate the above definition by saying that a primitive divisor is a prime number \( p \) which divides \( v_n \) but not \( v_m \) for any positive integer \( m < n \). It was shown in \([2]\) that primitive divisors always exist if \( n \geq 31 \). Particular instances of this result were proved much earlier by Zsigmondy \([14]\) (the case of rational integers \( \alpha, \beta \)) and Carmichael \([5]\) (the case of real \( \alpha, \beta \)).

It is known that primitive divisors are congruent to \( \pm 1 \pmod{n} \). In particular, writing \( P(m) \) for the largest prime factor of the integer \( m \) with the convention that \( P(0) = P(\pm 1) = 1 \), one has

\[
P(u_n)/n \geq (n - 1)/n \quad \text{for} \quad n \geq 31.
\]

Erdős \([7]\) conjectured that \( P(u_n)/n \) tends to infinity. This was proved to be so by Stewart \([13]\) who showed that

\[
P(u_n) > n \exp\left(\frac{\log n}{(104 \log \log n)}\right)
\]

holds for \( n > n_0 \), where \( n_0 \) is a constant which Stewart did not compute and which depends on the discriminant of the field \( \mathbb{Q}(\alpha) \) and the number of distinct prime factors of \( s \). Explicit values for \( n_0 \) were computed in \([3]\) at the cost of replacing \( 1/104 \) by somewhat smaller constants (see Theorem 2.1 and 2.2 below). It is also shown in \([3]\) that \( n_0 \) depends only on the field \( \mathbb{Q}(\alpha) \), but is independent of the number of prime divisors of \( s \).

Schinzel \([11]\) generalized the primitive divisor theorem to algebraic numbers in the following way. Let \( \gamma \) be an algebraic number of degree \( d \) which is not a root of unity, and denote \( v_n = \gamma^n - 1 \). A prime ideal \( \mathfrak{p} \subset O_K \) is called a primitive divisor of \( v_n \) if \( \mathfrak{p} \) appears at positive exponent in the factorization of the principal fractional ideal \( v_n O_K \) but \( \mathfrak{p} \) does not appear in the factorization of \( v_m O_K \) for any positive integer \( m < n \).

Schinzel proved that \( v_n \) has a primitive divisor for \( n \geq n_0(d) \). Stewart \([12]\) gave an explicit value for \( n_0(d) \) but he assumed that \( \gamma \) has a representation of the form \( \gamma = \alpha/\beta \) with coprime integers \( \alpha, \beta \) in \( O_K \). An explicit value for \( n_0 \) without any additional hypothesis was given in \([4]\).

In this note we show that Stewart’s type result can be obtained for recurrent sequences other than Lucas. We look at the prime factors of a certain linear recurrent sequences of order 4 which is a particular instance of a norm of a complex quadratic Lucas sequence. Namely, we let \( q \) and \( a \) be integers satisfying

\[
q \geq 2, \quad |a| < 2\sqrt{q}.
\]

We denote \( \alpha \) and \( \bar{\alpha} \) the complex conjugate roots of \( x^2 - ax + q \). We prove the following theorem.

**Theorem 1.1.** Set \( n_0 := \exp\exp(\max\{10^{10}, 3q\}) \) Let \( n \) be a positive integer satisfying \( n \geq n_0 \). Then the rational integer \( (\alpha^n - 1)(\bar{\alpha}^n - 1) \) has a prime divisor \( p \) satisfying

\[
p \geq n \exp\left(0.0001 \frac{\log n}{\log \log n}\right).
\]

When \( q \) is a prime power, the number

\[
(\alpha - 1)(\bar{\alpha} - 1) = a\bar{\alpha} - (\alpha + \bar{\alpha}) + 1 = q - a + 1
\]

is the order of the group \( \#E(\mathbb{F}_q) \) of \( \mathbb{F}_q \)-rational points on a certain elliptic curve \( E \). Furthermore, \( (\alpha^n - 1)/(\bar{\alpha}^n - 1) \) represents the order of the group...
The numbers \( \#E(F_{q^n}) \) of \( F_{q^n} \)-rational points. The numbers \( \#E(F_{q^n}) \) form a linearly recurrent sequence of order 4 with roots 1, \( \alpha \), \( \overline{\alpha} \), \( q \). Like the Lucas sequences, these numbers have the property that \( \#E(F_{q^m}) \mid \#E(F_{q^n}) \) when \( m \mid n \) (because \( F_{q^n} \) is an extension of \( F_{q^m} \) of degree \( n/m \)). However, in spite of those similarities, some non-trivial new ideas are needed to extend Stewart’s argument to these sequences, see Subsection 3.2.

Note that big prime factors of orders of elliptic curves were studied before, albeit in a different set-up. For instance, Akbary [1] studied big prime factors of \( \#E(F_q) \), where \( E \) is a fixed elliptic curve over \( \mathbb{Q} \) with complex multiplication. He proved that, for a positive proportion of primes \( q \), the number \( \#E(F_q) \) has a prime divisor bigger than \( q^\theta \), where \( \theta = 1 - e^{-1/4}/2 = 0.6105 \ldots \) We invite the reader to consult the comprehensive survey [6] for more information.

1.1 Notation

Unless the contrary is stated explicitly, \( m \) and \( n \) (with or without indices) always denote positive integers and \( p \) (with or without indices) denotes a prime number.

Let \( K \) be a number field. We denote \( D_K \) 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 \( \mathcal{O}_K \). If \( p \) is prime of \( K \) with underlying rational prime \( p \), then we denote \( f_p \) its absolute residual degree and \( N_p = p^{f_p} \) its absolute norm.

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

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

where \( \log^+ = \max\{\log, 0\} \). Here \( K \) is an arbitrary number field containing \( \alpha \), and the places \( v \in M_K \) are normalized to extend standard places of \( \mathbb{Q} \); that is, \( |p|_v = p^{-1} \) if \( v \mid p < \infty \) and \( |2021|_v = 2021 \) if \( v \mid \infty \).

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:

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

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

\[
h(\alpha) = \frac{1}{d} \left( \sum_{\sigma: K \hookrightarrow \mathbb{C}} -\log^- |\sigma(\alpha)| + \sum_p \max\{0, \nu_p(\alpha)\} \log N_p \right), \quad (1.1)
\]

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

Besides \( \log^+ \) and \( \log^- \) we will also widely 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 \( |A| \leq B \).
2 Auxiliary facts

2.1 The Theorems of Stewart

The following two theorems are, essentially, due to Stewart [13], though in the present form they can be found in [3], see Theorems 1.4 and 1.5 there in.

Theorem 2.1. 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 $K = \mathbb{Q}(\gamma)$ whose absolute norm satisfies $N_p \geq p_0$, 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 2.2. Let $\gamma$ be a non-zero algebraic number of degree 2, not a root of unity. Assume that $N_\gamma = \pm 1$. Set $p_0 = \exp \exp(\max\{10^8, 2|D_K|\})$, where $D_K$ is the discriminant of the quadratic field $K = \mathbb{Q}(\gamma)$. Then for every prime $p$ of $K$ with underlying rational prime $p \geq p_0$, and every positive integer $n$ we have

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

2.2 Cyclotomic polynomials and primitive divisors

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. We denote by $\Phi_n(t)$ the $n$th cyclotomic polynomial.

Items 1 and 2 of the following proposition are well-known and easy, and item 3 is Lemma 4 of Schinzel [11]; see also [4] Lemma 4.5.

Proposition 2.3. 1. Let $p$ be a primitive divisor of $u_n$. Then $\nu_p(\Phi_n(\gamma)) \geq 1$ and $N_p \equiv 1 \mod n$; in particular, $N_p \geq n + 1$.

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 $p \equiv \pm 1 \mod n$. More specifically,

$$
p \equiv \begin{cases} 
1 \mod n & \text{if } p \text{ splits in } \mathbb{Q}(\gamma), \\
-1 \mod n & \text{if } p \text{ is intert in } \mathbb{Q}(\gamma).
\end{cases}
$$

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

Remark 2.4. In item 2 the ramified $p$ seem to be missing. However, it is easy to show that, when $N_\gamma = 1$ and $p$ ramifies in $\mathbb{Q}(\gamma)$ then $\nu_p(\gamma - 1) > 0$ or $\nu_p(\gamma + 1) > 0$. Hence, $n = 1$ or $n = 2$ in this case.
2.3 Counting \( S \)-units

Let \( S \) be a set of prime numbers. A positive integer is called \( S \)-unit if all its prime factors belong to \( S \). We denote \( \Theta(x, S) \) the counting function for \( S \)-units:

\[
\Theta(x, S) = \# \{ n \leq x : p \mid n \Rightarrow p \in S \}.
\]

We want to bound this function from above.

**Proposition 2.5.** Let \( S \) be a set of \( k \) prime numbers. Then for \( x \geq 3 \) we have

\[
\Theta(x, S) \leq \exp \left( 2k^{1/2} \log \log x + 20 \left( \frac{\log x}{\log^* k} \right) \log^* \left( \frac{k \log^* k}{\log x} \right) \right). \tag{2.2}
\]

To start with, note the following trivial bound.

**Proposition 2.6.** In the set-up of Proposition 2.5 assuming \( x \geq 7 \) we have

\[
\Theta(x, S) \leq \exp(2k \log \log x). \tag{2.3}
\]

**Proof.** If \( n \leq x \) then for every \( p \) we have \( \nu_p(n) \leq \log x / \log 2 \). Hence

\[
\Theta(x, S) \leq \left( \frac{\log x}{\log 2} + 1 \right)^k \leq \exp(2k \log \log x),
\]

as wanted. \( \Box \)

Next, let us consider a special case, when the primes from \( S \) are not too small.

**Proposition 2.7.** In the set-up of Proposition 2.5 assume that \( p \geq k^{1/2} \) for every \( p \in S \). Then

\[
\Theta(x, S) \leq \exp \left( 10 \left( \frac{\log x}{\log^* k} \right) \log^* \left( \frac{k \log^* k}{\log x} \right) \right). \tag{2.4}
\]

**Proof.** If \( x < 7 \), then either \( \Theta(x, S) = 0 \) so the above inequality is trivially true, or \( k \leq 25 \), and the right-hand side above is at least

\[
\exp \left( \left( \frac{10}{\log 25} \right) \log x \right) > x^3 > |x| \geq \Theta(x, S).
\]

If \( x \geq 7 \) and \( k \leq 2 \) then (2.4) follows from (2.3). From now on we assume that \( k \geq 3 \); in particular, \( \log^* k = \log k \). Write \( S = \{ p_1, p_2, \ldots, p_k \} \). Then every \( S \)-unit \( n \) can be presented as \( p_1^{a_1} \cdots p_k^{a_k} \) with non-negative integers \( a_1, \ldots, a_k \). If \( n \leq x \) then

\[
a_1 \log p_1 + \cdots + a_k \log p_k \leq \log x.
\]

By the assumption, \( \log p_i \geq (1/2) \log k \) for \( i = 1, \ldots, k \). Hence,

\[
a_1 + \cdots + a_k \leq \ell, \tag{2.5}
\]
where \( \ell = \lceil \frac{2 \log x}{\log k} \rceil \). We may assume that \( \ell \geq 1 \): if \( \ell = 0 \) then the only solution of (2.5) is \( a_1 = \cdots = a_k = 0 \), and \( \Theta(x, S) = 1 \). For further use, note that

\[
\frac{\log x}{\log k} \leq \ell \leq 2 \left( \frac{\log x}{\log k} \right).
\]

Inequality (2.5) has exactly

\[
\sum_{i=0}^{\ell} \binom{k+i}{i}
\]

solutions in \( (a_1, \ldots, a_k) \in \mathbb{Z}_{\geq 0}^k \). Hence,

\[
\Theta(x, S) \leq (\ell + 1) \left( \frac{k + \ell}{\ell} \right) \leq (\ell + 1) \left( e \left( \frac{k + \ell}{\ell} \right) \right)^{\ell} \leq \exp \left( \ell \log \left( 2e \left( \frac{k + \ell}{\ell} \right) \right) \right) \quad \text{(we used } \ell + 1 \leq 2\ell \text{)}
\]

\[
\leq \exp \left( 2 \left( \frac{\log x}{\log k} \right) \log \left( 2e \left( \frac{k + \ell}{\ell} \right) \right) \right).
\]

If \( k \leq 9\ell \) then

\[
\log \left( 2e \left( \frac{k + \ell}{\ell} \right) \right) \leq \log(20e) < 4,
\]

and we are done. If \( k \geq 9\ell \) then

\[
\log \left( 2e \left( \frac{k + \ell}{\ell} \right) \right) \leq \log \left( 8 \left( \frac{k}{\ell} \right) \right) \leq \log \left( 8 \left( \frac{k \log k}{\log x} \right) \right) \leq 4 \log^* \left( \frac{k \log k}{\log x} \right),
\]

and we are done again. \( \square \)

**Proof of Proposition 2.6** Write \( S = S_1 \cup S_2 \), where

\[
S_1 = \{ p \in S : p < k^{1/2} \}, \quad S_2 = \{ p \in S : p \geq k^{1/2} \}.
\]

Then, clearly \( \Theta(x, S) \leq \Theta(x, S_1) \Theta(x, S_2) \). We estimate \( \Theta(x, S_1) \) using Proposition 2.6 and \( \Theta(x, S_2) \) using Proposition 2.7

\[
\Theta(x, S_1) \leq \exp(2k^{1/2} \log \log x),
\]

\[
\Theta(x, S_2) \leq \exp \left( 10 \left( \frac{\log x}{\log^* (k - k^{1/2})} \right) \log^* \left( \frac{k \log^* k}{\log x} \right) \right) \leq \exp \left( 20 \left( \frac{\log x}{\log^* k} \right) \log^* \left( \frac{k \log^* k}{\log x} \right) \right).
\]

The result follows. \( \square \)
3 Proof of Theorem 1.1

Denote $\mathbb{K} = \mathbb{Q}(\alpha)$. It is an imaginary quadratic field. Hence, for a non-zero $\theta \in \mathcal{O}_K$ we have

$$h(\theta) = \log |\theta| = \frac{1}{2} \sum \nu_p(\theta) \log N_p,$$

the sum being over the finite primes of $\mathbb{K}$.

We apply this with $\theta = \Phi_n(\alpha)$ (recall that $\Phi_n(t)$ denotes the $n$th cyclotomic polynomial). We have

$$\log |\Phi_n(\alpha)| = \varphi(n) \log |\alpha| + \sum_{d|n} \mu \left( \frac{n}{d} \right) \log |1 - \alpha^{-d}| = \frac{1}{2} \varphi(n) \log q + O_1(5). \quad (3.1)$$

Indeed, we have $|\alpha| = q^{1/2} \geq \sqrt{2}$ and $|\log |1 + z|| \leq 2|z|$ for $|z| \leq 1/\sqrt{2}$. Hence

$$\sum_{d|n} \mu \left( \frac{n}{d} \right) \log |1 - \alpha^{-d}| < 2 \sum_{d=1}^{\infty} |\alpha|^{-d} < 5,$$

which proves (3.1). Thus,

$$\sum_p \nu_p(\Phi_n(\alpha)) \log N_p = \varphi(n) \log q + O_1(10).$$

Proposition 2.3.3 implies that, for $n \geq 8$,

$$\sum_{p \text{ not primitive}} \nu_p(\Phi_n(\alpha)) \log N_p \leq 2 \log n,$$

the sum being over $p$ which are non-primitive divisors of $\alpha^n - 1$. Hence,

$$\sum_{p \text{ primitive}} \nu_p(\Phi_n(\alpha)) \log N_p \geq \varphi(n) \log q - 10 - 2 \log n.$$

The Euler totient function $\varphi(n)$ satisfies

$$\varphi(n) \geq 0.5 \frac{n}{\log \log n} \quad (n \geq 10^{20}) \quad (3.2)$$

(see [10, Theorem 15]). Hence for $n \geq 10^{20}$ we have

$$\sum_{p \text{ primitive}} \nu_p(\Phi_n(\alpha)) \log N_p \geq 0.8 \varphi(n) \log q.$$

From now on, the proof splits into two cases, depending on whether the primes with residual degree 1 contribute more to the sum, or those with residual degree 2 do. Precisely, we have

either \[ \sum_{\substack{p \text{ primitive} \\ f_p = 1}} \nu_p(\Phi_n(\alpha)) \log N_p \geq 0.4 \varphi(n) \log q, \] (3.3)

or \[ \sum_{\substack{p \text{ primitive} \\ f_p = 2}} \nu_p(\Phi_n(\alpha)) \log N_p \geq 0.4 \varphi(n) \log q. \] (3.4)
Case (3.3) is easier, the proof follows the same lines as the proof of Theorem 1.2 in [3]. Case (3.4) is harder and requires more intricate arguments.

3.1 Case (3.3)

We will apply Theorem 2.1 with $\gamma = \alpha$ and $K = \mathbb{Q}(\alpha)$, so that $d = 2$ and $p_0 = \exp(160000)$. We may assume that $n > p_0$, because $n_0$ from Theorem 1.1 is bigger than $p_0$.

Let $P$ be the biggest rational prime $p$ with the following two properties: $p$ splits in $K = \mathbb{Q}(\alpha)$, and $\alpha^n - 1$ admits a primitive divisor $p$ with underlying prime $p$. We want to show that

$$P > n \exp \left( 0.0002 \frac{\log n}{\log \log n} \right).$$

(3.5)

Let $p$ be a primitive divisor of $\alpha^n - 1$ with $f_p = 1$, and $p$ the underlying rational prime. Then $p \leq P$ and $p = Np \equiv 1 \mod n$ by Proposition 2.3.1. In particular, $p > n > p_0$, and Theorem 2.1 applies:

$$\nu_p(\alpha^n - 1) \leq P \exp \left( -0.001 \frac{\log n}{\log \log n} \right) \frac{1}{2} \log q \log n$$

$$\leq P \exp \left( -0.001 \frac{\log n}{\log \log n} \right) \log q \log n.$$

Hence,

$$\sum_{p \text{ primitive } \frac{f_p}{p} = 1} \nu_p(\Phi_n(\alpha)) \log Np \leq \pi(P; n, 1)P \exp \left( -0.001 \frac{\log n}{\log \log n} \right) \log q \log n \log P,$$

where, as usual $\pi(x; m, a)$ counts prime in the residue class $a \mod m$. Estimating trivially $\pi(P; n, 1) \leq P/n$, we obtain

$$\sum_{p \text{ primitive } \frac{f_p}{p} = 1} \nu_p(\Phi_n(\alpha)) \log Np \leq \frac{P^2 \log P}{n} \exp \left( -0.001 \frac{\log n}{\log \log n} \right) \log n \log q.$$

Compared with (3.3), this implies

$$P^2 \log P \geq 0.4 \frac{\omega(n)}{\log n} \exp \left( 0.001 \frac{\log n}{\log \log n} \right).$$

Using (3.2), this implies (3.5) for $n > n_0$.

3.2 Case (3.4)

If $p$ is a prime of $K$ with $f_p = 2$ then it is a rational prime, and we write $p$ instead of $p$. For such $p$ we have $\nu_p(\alpha^n - 1) = \nu_p(\tilde{\alpha}^n - 1)$. Setting $\gamma = \tilde{\alpha}/\alpha$, we obtain

$$\nu_p(\gamma^n - 1) \geq \nu_p((\tilde{\alpha}^n - 1) - (\alpha^n - 1)) \geq \nu_p(\alpha^n - 1) \geq \nu_p(\Phi_n(\alpha)).$$

8
Hence, (3.4) implies the inequality
\[ \sum_{p \in P} \nu_p(\gamma^n - 1) \log p \geq 0.2\varphi(n) \log q \]
(note that \(\mathcal{N}p = p^2\), where the set \(P\) consists of the rational primes \(p\) inert in \(K\) and satisfying \(\nu_p(\alpha^n - 1) > 0\):
\[ P = \{ p \text{ inert in } K \text{ and } \nu_p(\alpha^n - 1) > 0 \}. \]

We are now tempted to bound the sum on the left as we did in Subsection 3.1, but with Theorem 2.1 replaced by Theorem 2.2, which applies here because \(\mathcal{N}\gamma = 1\). However, now instead of \(p \equiv 1 \mod n\) we have merely \(p^2 \equiv 1 \mod n\), and we have to use a more delicate argument.

Denote \(v_n = \gamma^n - 1\). If \(\nu_p(v_n) > 0\) then there is a divisor \(d\) of \(n\) such that \(p\) is primitive for \(v_n/d\). We denote it \(d_p\). We have
\[ \nu_p(v_n) \leq \nu_p(v_{n/d}) + \sum_{m \mid n \atop m \neq n/d} \nu_p(\Phi_m(\gamma)). \]

Proposition 2.3.3 bounds the sum on the right by
\[ \sum_{m \mid n} \nu_p(m) + \sum_{m=1}^7 \nu_p(\Phi_m(\gamma)). \]

It follows that
\[ \sum_{p \in P} \nu_p(\gamma^n - 1) \log p \leq \sum_{p \in P} \nu_p(v_{n/d_p}) + \sum_{m \mid n} \log m + \sum_{m=1}^7 \sum_{p} \nu_p(\Phi_m(\gamma)) \log p. \]

The middle sum on the right is trivially estimated by \(\tau(n) \log n\), where \(\tau(n)\) denotes the number of divisors of \(n\):
\[ \tau(n) = \sum_{m \mid n} 1. \]

To estimate the double sum on the right, note that
\[ \nu_p(\Phi_m(\gamma)) \leq \nu_p(v_m) \leq \frac{1}{2} \nu_p((\alpha_m - \bar{\alpha})^2). \]

Since \((\alpha_m - \bar{\alpha})^2\) is a rational integer of absolute value not exceeding \(4q^m\), this implies that
\[ \sum_{p} \nu_p(v_m) \log p \leq \frac{1}{2} m \log q + \log 2. \]

Hence,
\[ 7 \sum_{m=1}^7 \sum_{p} \nu_p(\Phi_m(\gamma)) \log p \leq 14 \log q + 7 \log 2. \]

Putting all this together, we obtain the inequality
\[ \sum_{p \in P} \nu_p(v_{n/d_p}) \log p \geq 0.2\varphi(n) \log q - \tau(n) \log n - 14 \log q - 7 \log 2. \]
3.2.1 Disposing of big $d_p$

We want to get rid in our sum of primes $p$ with $d_p \geq \tau(n) \log n$. Using (3.6), we obtain

$$\sum_{d_p \geq \tau(n) \log n} \nu_p(v_{n/d_p}) \log p \leq \frac{1}{2} n \log q \sum_{d \geq \tau(n) \log n} \frac{1}{d} + \tau(n) \log 2$$

The sum on the right is trivially estimated as

$$\frac{\tau(n)}{\tau(n) \log n} = \frac{1}{\log n}.$$  

Hence,

$$\sum_{d_p \geq \tau(n) \log n} \nu_p(v_{n/d_p}) \log p \leq \frac{n}{2 \log n} \log q + \tau(n) \log 2.$$ 

Denote by $P'$ the subset of $P$ consisting of $p$ with $d_p < \tau(n) \log n$:

$$P' = \{p \in P : d_p < \tau(n) \log n\}.$$

Then we obtain

$$\sum_{p \in P'} \nu_p(v_{n/d_p}) \log p \geq 0.2 \varphi(n) \log q - \tau(n) \log n - 14 \log q - 7 \log 2$$

$$- \frac{n}{2 \log n} \log q - \tau(n) \log 2.$$ 

We have

$$\tau(n) \leq \exp \left(1.1 \frac{\log n}{\log \log n}\right) \quad (n \geq 3) \quad (3.7)$$  

(see [8, Theorem 1]). Using this and (3.2), we deduce that, for

$$n \geq n_0 \geq \exp\exp(10^{10})$$

(which is true by assumption), we have

$$\sum_{p \in P'} \nu_p(v_{n/d_p}) \log p \geq 0.1 \varphi(n) \log q. \quad (3.8)$$

3.2.2 Counting divisors $d < \tau(n) \log n$

The number of divisors $d < \tau(n) \log n$ can be estimated using Proposition 2.5. Denote $x = \tau(n) \log n$ and denote by $S$ the set of prime factors of $n$, so that

$$\#S = \omega(n).$$

Then

$$\#\{d \mid n : d < x\} \leq \Theta(x, S)$$

$$\leq \exp \left(2 \omega(n)^{1/2} \log \log x + 20 \frac{\log x}{\log^* \omega(n)} \log^* \omega(n) \log^* \omega(n) \log x \right).$$
For further use, note the trivial estimates

\[ \log \tau(n) \geq \omega(n) \log 2, \quad (3.9) \]
\[ \log \tau(n) \leq \omega(n) \log \left( \frac{\log n}{\log 2} + 1 \right) \leq 2\omega(n) \log \log n \quad (3.10) \]

(recall that \( n \geq \exp(\exp(10^{10})) \)). Note also the estimates

\[ \log \tau(n) \leq 1.1 \frac{\log n}{\log \log n}, \quad (3.11) \]
\[ \omega(n) \leq 1.4 \frac{\log n}{\log \log n} \quad (3.12) \]

(see (3.7) and [11 Théorème 11]).

Using (3.11) and (3.12), we deduce that, for \( n \geq \exp(\exp(10^{10})) \), we have

\[ 2\omega(n)^{1/2} \log x \leq (\log n)^{1/2} \log \log n. \quad (3.13) \]

Using (3.9) and (3.12), we deduce that

\[ \frac{\omega(n)^* \omega(n)}{\log x} \leq \frac{\omega(n)^* \omega(n)}{\log \tau(n)} \leq \frac{\omega(n)^*}{\log 2} \leq 2 \log \log n. \quad (3.14) \]

To estimate \( x/\log^* \omega(n) \), we consider two cases. Assume first that

\[ \omega(n) \leq \frac{\log n}{(\log \log n)^3}. \]

In this case, using (3.10), we estimate

\[ \frac{\log x}{\log^* \omega(n)} \leq \frac{2\omega(n) \log \log n + \log \log n}{\log \log n} \leq 3\omega(n) \log \log n \leq \frac{3 \log n}{(\log \log n)^2}. \]

Now assume that

\[ \omega(n) \geq \frac{\log n}{(\log \log n)^3}. \]

In this case, using (3.11), we obtain

\[ \frac{\log x}{\log^* \omega(n)} \leq \frac{1.1 \frac{\log n}{\log \log n} + \log \log n}{\log \log n - 3 \log \log \log n} \leq \frac{3 \log n}{(\log \log n)^2}. \]

Thus, in any case

\[ \frac{\log x}{\log^* \omega(n)} \leq \frac{3 \log n}{(\log \log n)^2}. \]

Putting this all together, we obtain

\[ \# \{ d \mid n : d < x \} \leq \exp \left( (\log n)^{1/2} \log \log n + 20 \cdot 3 \frac{\log n}{(\log \log n)^2} \log(2 \log \log n) \right) \]
\[ \leq \exp \left( 70 \frac{\log n \log \log \log n}{(\log \log n)^2} \right). \quad (3.15) \]
3.2.3 The cardinality of $P'$

The crucial step is estimating the number of primes in the set $P'$. Denote $P$ the biggest element of $P'$. We are going to prove that

$$\# P' \leq \left( \frac{P}{n} + 1 \right) \exp \left( \frac{80 \log n \log \log \log n}{(\log \log n)^2} \right). \quad (3.16)$$

Let $p$ be a prime from the set $P'$. Recall that $n \mid p^2 - 1$; in particular, $p > 2$. Assume first that $n$ is odd. In this case the numbers $\gcd(p - 1, n)$ and $\gcd(p + 1, n)$ are coprime. We write them, respectively, $d$ and $n/d$. Thus, we have

$$p \equiv -1 \mod n/d, \quad p \equiv 1 \mod d \quad (3.17)$$

for some $d$ dividing $n$ and such that $\gcd(n/d, d) = 1$. By the definition of $d_p$ we must have $d \mid d_p$. In particular, if $p \in P'$ then $d < \tau(n) \log n$.

By the Chinese Remainder Theorem, for every $d \mid n$ such that $\gcd(n/d, d) = 1$, there exists a unique $a_d \in \{1, \ldots, n - 1\}$ such that $p \equiv a_d \mod n$ holds for every $p$ satisfying (3.17). It follows that

$$\# P' \leq \sum_{d \mid n : \gcd(n/d, d) = 1} \pi(P; n, a_d).$$

We estimate trivially $\pi(P; n, a_d) \leq P/n + 1$. Hence, when $n$ is odd, we have the upper bound

$$\# P' \leq \left( \frac{P}{n} + 1 \right) \# \{d \mid n : d < \tau(n) \log n \}. \quad (3.18)$$

If $n$ is even, the argument is similar, but slightly more complicated. Assume, for instance, that $p \equiv 3 \mod 4$. Then the numbers

$$\gcd \left( \frac{p - 1}{2}, \frac{n}{2} \right), \quad \gcd \left( \frac{p + 1}{2}, \frac{n}{2} \right)$$

are coprime, and we write them $d$ and $n/2d$, respectively; note also that $d$ is odd. We have $2d \mid d_p$, and, in particular, $d < \tau(n) \log n$. The system of congruences

$$p \equiv -1 \mod \frac{n}{2d}, \quad p \equiv 1 \mod d$$

is equivalent to $p \equiv a_d \mod n/2$, where $a_d \in \{1, \ldots, n/2 - 1\}$ depends only on $d$. Similarly, when $p \equiv 1 \mod 4$, we have $p \equiv b_d \mod n/2$, where $d < \tau(n) \log n$ and $b_d \in \{1, \ldots, n/2 - 1\}$ depends only on $d$. We obtain

$$\# P' \leq \sum_{d \mid n : \gcd(n/d, d) = 1} \left( \pi(P; n/2, a_d) + \pi(P; n/2, b_d) \right)$$

$$\leq \left( \frac{P}{n} + 2 \right) \# \{d \mid n : d < \tau(n) \log n \}. \quad (3.19)$$
We see that upper bound (3.19) holds in all cases. Combining it with (3.15), we obtain

\[ \#P' \leq \left( \frac{P}{n} + \frac{1}{2} \right) \exp \left( 70 \frac{\log n \log \log n}{(\log \log n)^2} + \log 4 \right), \]

which is sharper than (3.16).

### 3.2.4 Using Stewart

Now it is the time to use Theorem [2.2]. To start with, note that \( |D_K| \leq q \). Hence, \( p_0 \) from Theorem [2.2] does not exceed \( n_0^{1/2} \). Now if \( \nu_p(\gamma^n - 1) > 0 \) then \( n \mid p^2 - 1 \), see Proposition [2.3.1]. Hence, \( p > n^{1/2} \geq n_0^{1/2} \geq p_0 \), and Theorem [2.2] applies. For \( p \in P' \) it gives

\[ \nu_p(\gamma^n - 1) \leq p \exp \left( -0.001 \frac{\log p}{\log \log p} \right) h(\gamma) \log n \]

\[ \leq 2P \exp \left( -0.0005 \frac{\log n}{\log \log n} \right) \log q \log n, \quad (3.20) \]

because

\[ p \leq P, \quad \frac{\log p}{\log \log p} \geq \frac{1}{2} \frac{\log n}{\log \log n}, \quad h(\gamma) \leq 2q. \]

Since \( \nu_p(v_{n/d_p}) \leq \nu_p(\gamma^n - 1) \), we can combine (3.20) with (3.8), obtaining

\[ 2P \log P \exp \left( -0.0005 \frac{\log n}{\log \log n} \right) \#P' \log q \log n \geq 0.1 \varphi(n) \log q. \]

Using (3.16) and (3.2), this implies, for \( n \geq \exp\exp(10^{10}) \), that

\[ P(P + n) \log P \geq n^2 \exp \left( \left( 0.0004 - 100 \frac{\log \log n}{\log \log \log n} \right) \frac{\log n}{\log \log n} \right) \]

\[ \geq n^2 \exp \left( 0.0003 \frac{\log n}{\log \log n} \right). \]

If \( P < n \) then the latter inequality is clearly impossible for \( n \geq \exp\exp(10^{10}) \). Hence, \( P \geq n \), and we obtain

\[ P^2 \log P \geq \frac{1}{2} n^2 \exp \left( 0.0003 \frac{\log n}{\log \log n} \right), \]

which implies

\[ P \geq n \exp \left( 0.0001 \frac{\log n}{\log \log n} \right). \]

Theorem [1.1] is proved.
References

[1] Amir Akbary, On the greatest prime divisor of $N_p$, J. Ramanujan Math. Soc. 23 (2008), no. 3, 259–282. MR 2446601

[2] Yu. Bilu, G. Hanrot, and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, J. Reine Angew. Math. 539 (2001), 75–122, With an appendix by M. Mignotte. MR 1863855

[3] Yuri Bilu, Haojie Hong, and Sanoli Gun, Uniform explicit Stewart’s theorem on prime factors of linear recurrences, arXiv:2108.09857 (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] R. D. Carmichael, On the numerical factors of the arithmetic forms $a^n \pm b^n$, Ann. of Math. (2) 15 (1913/14), no. 1-4, 49–70. MR 1502459

[6] Alina Carmen Cojocaru, Primes, elliptic curves and cyclic groups, Analytic methods in arithmetic geometry, Contemp. Math., vol. 740, Amer. Math. Soc., Providence, RI, 2019 ©2019, With an appendix by Cojocaru, Matthew Fitzpatrick, Thomas Insley and Hakan Yilmaz, pp. 1–69. MR 4033729

[7] Paul Erdős, Some recent advances and current problems in number theory, Lectures on Modern Mathematics, Vol. III, Wiley, New York, 1965, pp. 196–244. MR 0177933

[8] J.-L. Nicolas and G. Robin, Majorations explicites pour le nombre de diviseurs de $N$, Canad. Math. Bull. 26 (1983), no. 4, 485–492. MR 716590

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

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

[11] 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

[12] C. L. Stewart, Primitive divisors of Lucas and Lehmer numbers, Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), 1977, pp. 79–92. MR 0476628

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

[14] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. Phys. 3 (1892), no. 1, 265–284. MR 1546236

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

Florian Luca: School of Maths, Wits University, South Africa and King Abdulaziz University, Jeddah, Saudi Arabia and IMB, Université de Bordeaux, France and Centro de Ciencias Matematicas UNAM, Morelia, Mexico

14