Lehmer’s Conjecture for Polynomials Satisfying a Congruence Divisibility Condition and an Analogue for Elliptic Curves

JOSEPH H. SILVERMAN

Abstract. A number of authors have proven explicit versions of Lehmer’s conjecture for polynomials whose coefficients are all congruent to 1 modulo $m$. We prove a similar result for polynomials $f(X)$ that are divisible in $(\mathbb{Z}/m\mathbb{Z})[X]$ by a polynomial of the form $1 + X + \cdots + X^n$ for some $n \geq \deg(f)$. We also formulate and prove an analogous statement for elliptic curves.

INTRODUCTION

Let

$$h : \overline{\mathbb{Q}} \longrightarrow [0, \infty)$$

denote the absolute logarithmic height [9, 11]. Lehmer’s conjecture [15] asserts that there is an absolute constant $C > 0$ such that if $f(X) \in \mathbb{Z}[X]$ is a monic polynomial of degree $D \geq 1$ whose roots are not roots of unity, then

$$\sum_{f(\alpha) = 0} h(\alpha) \geq C.$$  \hspace{1cm} (1)

This problem has a long history; see for example [2, 15, 21, 22, 23]. The best general result known, which is due to Dobrowolski [5], says that $\sum h(\alpha) \geq C(\log \log D/\log D)^3$. Various authors have considered Lehmer’s problem for restricted values of $\alpha$. For example, Amoroso and Dvornicich [1] show that if the roots of $f(X)$ generate an abelian extension of $\mathbb{Q}$, then $\sum h(\alpha) \geq D(\log 5)/12$.

An interesting class of polynomials are those whose coefficients are all odd. More generally, one can consider polynomials whose coefficients are congruent to 1 modulo $m$, as in the following result.
**Theorem 1.** (Borwein, Dobrowolski, Mossinghoff [3]) Let $m \geq 2$, and let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree $D$ that satisfies

$$f(X) \equiv X^D + X^{D-1} + \cdots + X^2 + X + 1 \pmod{m}. \quad (2)$$

Then

$$\sum_{f(\alpha)=0} h(\alpha) \geq \frac{D}{D+1} C_m,$$

where we may take

$$C_2 = \frac{1}{4} \log 5 \quad \text{and} \quad C_m = \log \frac{\sqrt{m^2 + 1}}{2} \quad \text{for} \ m \geq 3.$$ 

We mention that an earlier paper [4] does the case of non-reciprocal polynomials, and subsequent papers [6, 10] give improved values for $C_m$, although asymptotically they all have the form $C_m = \log(m/2) + O(1/m^2)$. We also note the papers [17, 18] which give various generalizations of Theorem 1 including weakening the congruence condition (2), working over number fields, and considering heights of points and subspaces in projective space.

Our first result is the following generalization of Theorem 1, albeit with less sharp constants. See Theorem 10 and Corollary 13 for our precise results.

**Theorem 2.** For all $\epsilon > 0$ there is a constant $C_\epsilon > 0$ with the following property: Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree $D$ such that

$$f(X) \text{ is divisible by } X^{n-1} + X^{n-2} + \cdots + X + 1 \text{ in } (\mathbb{Z}/m\mathbb{Z})[X] \quad (3)$$

for some integers

$$m \geq 2 \quad \text{and} \quad n \geq \max\{\epsilon D, 2\}.$$ 

Suppose further that no root of $f(X)$ is a root of unity. Then

$$\sum_{f(\alpha)=0} h(\alpha) \geq C_\epsilon \log m.$$ 

In particular, Lehmer’s conjecture (1) is true for this class of polynomials.

The elliptic analogue of Lehmer’s conjecture says that if $E/K$ is an elliptic curve defined over a number field, then there is a constant $C_{E/K} > 0$ such that for all nontorsion points $Q \in E(\bar{K})$ of degree $D_Q = [K(Q) : K]$ we have

$$D_Q \hat{h}_E(Q) \geq C_{E/K}.$$ 

(4)
Here \( \hat{h}_E \) is the logarithmic canonical height on \( E \). There has been considerable work on the elliptic Lehmer conjecture; see for example [8, 14, 16]. Our second main result is an elliptic analogue of Theorem 2. An initial difficulty is to find an appropriate elliptic version of the mod \( m \) divisibility condition \( (3) \). In Section 1 we show that \( (3) \) implies a lower bound for a certain sum over the roots of \( f \), and it is this weaker property that we generalize and adapt to the elliptic setting. Using this definition, we are able to prove the following result. (See Corollary 21 for a precise statement.)

**Theorem 3.** Let \( K/\mathbb{Q} \) be a number field and let \( E/K \) be an elliptic curve. Fix some \( \epsilon > 0 \). Then the elliptic Lehmer conjecture \( (4) \) is true for all points \( Q \in E(\bar{K}) \) satisfying an elliptic mod \( m \) condition analogous to \( (3) \) for some ideal \( m \) such that \( N_{K/\mathbb{Q}}m \geq 2 \) and such that \( E \) has good reduction at all primes dividing \( m \) and for some \( n \geq \max\{\epsilon D_Q, 2\} \). The lower bound in \( (4) \) will have the form \( C_{E/K, \epsilon} \log m \).

Theorem 2 deals with congruences related to cyclotomic polynomials, which is natural when studying Lehmer’s problem, but one might consider other sorts of congruence conditions. For example, suppose that \( f(X) \) is congruent modulo \( m \) to \( X^D + X^{D-1} + \cdots + X^2 + X - 1 \). Samuels [17] has considered general conditions of this sort. In Section 5 we briefly reprove one of Samuels’ results and use it to make a number of remarks concerning possible generalizations.

**Remark 4.** Our Theorem 2 and some of Samuels’ principal results [17] are height bounds for polynomials satisfying various sorts of congruence conditions, so we conclude this introduction by briefly describing how the results differ. Our polynomials satisfy a divisibility condition modulo \( m \), so multiplying by \( X - 1 \), our theorem applies to polynomials \( F(X) \) of the form

\[
F(X) = (X^n - 1)A(X) + mB(X) \quad \text{for some } A, B \in \mathbb{Z}[X].
\]

In general, we obtain a bound for all \( n \) (see Lemma 15), and in particular we prove Lehmer’s conjecture if \( n \geq \epsilon \deg(F) \). The results in [17] apply to (factors of) polynomials that are congruent modulo \( m \) to a simpler polynomial of the same degree. For example, a typical result in [17] is a bound for (noncyclotomic factors of) polynomials \( F(X) \) of degree \( nr \) satisfying

\[
F(X) = (X^n - 1)^r + mB(X) \quad \text{for some } B \in \mathbb{Z}[X].
\]

Thus although there is some overlap, our result and the results in [17] apply to largely different classes of polynomials. It might be interesting...
to combine the methods of the two papers to prove a general result encompassing both.

Acknowledgements. The author would like to thank Michael Mossinghoff for introducing him to the topic of polynomials whose coefficients satisfy congruence conditions and both Michael and Igor Shparlinski for their helpful comments on an initial draft of the paper.

1. A Reformulation of Property \(2\)

We start by normalizing our absolute values.

**Definition.** We let \(M_\mathbb{Q}\) be the usual collection of absolute values on \(\mathbb{Q}\), and for any algebraic extension \(K/\mathbb{Q}\), we write \(M_K\) for the set of all extensions of these absolute values to \(K\). For \(\alpha \in \bar{\mathbb{Q}}\) and \(v \in M_\mathbb{Q}\), we define a normalized absolute value by choosing a finite extension \(K/\mathbb{Q}\) with \(\alpha \in K\) and setting

\[
\|\alpha\|_v = |\alpha|^{[K_v:Q_v]/[K:\mathbb{Q}]}.\]

We also define a normalized valuation by

\[
v(\alpha) = -\log \|\alpha\|_v.\]

Then the absolute logarithmic height of \(\alpha\) is defined by

\[
h(\alpha) = \sum_{v \in M_K} \max\{\log \|\alpha\|_v, 0\}.\]

We write \(M_K^0\), respectively \(M_K^\infty\), for the set of nonarchimedean, respectively archimedean, absolute values in \(M_K\).

**Remark 5.** With the above normalization we have the product formula

\[
\prod_{v \in M_K} \|\alpha\|_v = 1 \quad \text{for all } \alpha \in K^*.\]

In particular, if \(\alpha \in K\) is a nonzero algebraic integer, then

\[
h(\alpha) = \sum_{v \in M_K^\infty} \max\{\log \|\alpha\|_v, 0\} = \sum_{v \in M_K^0} v(\alpha).\]

We also remark that

\[
\prod_{v \in M_K^\infty} \|\alpha\|_v = \prod_{v \in M_K^0} \|\alpha\|_v^{-1} = N_{K/\mathbb{Q}}(\alpha)^{1/[K:\mathbb{Q}]}.
\]

**Remark 6.** Let \(f(X) \in \mathbb{Z}[X]\) be a monic polynomial. Then the classical Mahler measure \(M(f)\) of \(f\) is related to the heights of its roots via the formula

\[
\log M(f) = \sum_{f(\alpha) = 0} h(\alpha).
\]
In this paper we use the “sum the heights” notation because it has an obvious generalization to other algebraic groups such as elliptic curves. In such sums, we always include the roots of $f$ with their multiplicities.

**Definition.** For notational convenience, we let

$$\Phi_n(X) = X^n + X^{n-1} + \cdots + X + 1.$$  

If $n$ is prime, this is the usual cyclotomic polynomial; in general it is a product of classical cyclotomic polynomials.

Property (2) of Theorem 1 says that all of the coefficients of the polynomial $f$ are congruent to 1 modulo $m$. This is equivalent to saying that the monic degree $D$ polynomial $f(X) \in \mathbb{Z}[X]$ is divisible by $\Phi_D(X)$ in the ring $(\mathbb{Z}/m\mathbb{Z})[X]$. Note that although this ring will contain zero divisors if $m$ is composite, divisibility by a monic polynomial is still a well-behaved property. The next proposition gives some properties that are weaker than Property (2) of Theorem 1.

**Proposition 7.** Let $m, n \geq 2$, and let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree $D$. Consider the following three conditions:

(i) $f(X)$ is divisible by $\Phi_{n-1}(X)$ in $(\mathbb{Z}/m\mathbb{Z})[X]$.

(ii) $m^{n-1} \mid \text{Res}(f(X), \Phi_{n-1}(X))$.

(iii) \[\sum_{v \mid m} \sum_{f(\alpha) = 0} v(\alpha^n - 1) \geq (n - 1) \log m.\]

Then \[\text{(i)} \implies \text{(ii)} \implies \text{(iii)}.\]

(In (iii), we may work over any field in which $f$ factors completely. The way that we have normalized our absolute values ensures that the choice of field does not matter.)

**Proof.** Property (i) says that

$$f(X) = \Phi_{n-1}(X)A(X) + mB(X) \quad \text{for some } A(X), B(X) \in \mathbb{Z}[X].$$

This implies that

$$\text{Res}(f(X), \Phi_{n-1}(X)) = \text{Res}(\Phi_{n-1}(X)A(X) + mB(X), \Phi_{n-1}(X))$$

$$= \text{Res}(mB(X), \Phi_{n-1}(X))$$

$$= m^{n-1} \text{Res}(B(X), \Phi_{n-1}(X)).$$

Thus (ii) is true.
We next prove that (ii) implies (iii). For any non-archimedean absolute value \( v \) we have
\[
\| \text{Res}(f(X), x^n - 1) \|_v = \| \text{Res}(f(X), \Phi_{n-1}(X)) \|_v \| f(1) \|_v \leq \| m \|_v^{n-1}. \tag{5}
\]
A standard formula for the resultant \([13, \text{Section V.10}]\) is
\[
\text{Res}(f(X), X^n - 1) = \prod_{\alpha \in A} (\alpha^n - 1). \tag{6}
\]
We take the \( v \)-absolute value of (6), use (5), and multiply over all \( v \mid m \) to obtain the estimate
\[
\prod_{v \mid m} \prod_{f(\alpha) = 0} \| \alpha^n - 1 \|_v \leq \prod_{v \mid m} \| m \|_v^{n-1} = m^{-(n-1)}. \tag{7}
\]
Taking \(- \log (\cdot)\) gives (iii). \(\square\)

We now define a quantity that generalizes the sum appearing in Property (iii) of Proposition 7.

**Definition.** Let \( A \subset \overline{\mathbb{Q}}^* \) be a finite set of algebraic integers and let \( m \) and \( n \) be positive integers. We define
\[
\Delta(A, m, n) = \sum_{\alpha \in A} \frac{1}{\log m} \sum_{v \mid m} \frac{1}{n} v(\alpha^n - 1).
\]
The inner sum is over all \( v \in M_{\overline{Q}}^K \) with \( v \mid m \), where \( K \) is any number field containing \( A \). Our normalization of the valuations in \( M_{\overline{Q}} \) implies that the sum is independent of the choice of \( K \).

**Proposition 8.** Let \( A \) be a finite set of algebraic integers, let \( j, m, n \geq 1 \) be rational integers, and let \( A^j = \{ \alpha^j : \alpha \in A \} \). Then
\[
\Delta(A^j, m, n) \geq \Delta(A, m, n).
\]
**Proof.** From the factorization
\[
X^{jn} - 1 = (X^n - 1)\Phi_{j-1}(X^n),
\]
we see that
\[
v(\alpha^{jn} - 1) = v(\alpha^n - 1) + v(\Phi_{j-1}(\alpha^n)) \geq v(\alpha^n - 1)
\]
for any algebraic integer \( \alpha \) and any nonarchimedean absolute value \( v \). Summing over \( \alpha \in A \) and \( v \mid m \), and then dividing by \( n \log m \), gives the desired result. \(\square\)
Remark 9. We observe that if \( f(X) \in \mathbb{Z}[X] \) is a monic polynomial of degree \( D \) and if we write \( \mathcal{A}_f \) for the set of roots of \( f(X) \), then Property (iii) of Proposition \[7\] can be succinctly written as

\[
\Delta(\mathcal{A}_f, m, n) \geq \frac{n - 1}{n}.
\] (8)

In particular, if \( f \) satisfies the congruence

\[
f(X) \equiv \Phi_D(X) \pmod{m}
\]
as in the statement of Theorem \[\text{I} \]
then

\[
\Delta(\mathcal{A}_f, m, D + 1) \geq \frac{D}{D + 1}.
\]

2. A Height Bound for Polynomials Satisfying Congruence Conditions

The next theorem is our main result for number fields. As we will see, it generalizes \[\text{[3, 4, 6, 10]}\] (Theorem \[\text{I} \]
albeit with worse constants. Later we will prove an elliptic curve version of this theorem and its consequences.

Theorem 10. Let \( \mathcal{A} \subset \bar{\mathbb{Q}} \) be a finite set of algebraic integers, that does not contain any roots of unity and let \( m \) and \( n \) be positive integers. Then for all integers \( J \geq 1 \) we have

\[
\sum_{\alpha \in \mathcal{A}} h(\alpha) \geq \frac{3}{J + 2} \left( \Delta(\mathcal{A}, m, n) \log m - \frac{|\mathcal{A}| \log(J/2 + 1) + 1}{J} \right). \tag{9}
\]

Remark 11. It is always possible to choose a value of \( J \) to obtain a nontrivial, i.e., positive, lower bound in (9). The optimal choice of \( J \) depends on the relative sizes of \( \Delta(\mathcal{A}, m, n) \log m \) and \( |\mathcal{A}|/n \). In the application most closely related to Theorem \[\text{I} \]
we have

\[
n = D + 1 \quad \text{and} \quad \Delta(\mathcal{A}, m, n) \log m = \frac{|\mathcal{A}|}{n} = \frac{D}{D + 1},
\]

so we get

\[
\sum_{f(\alpha) = 0} h(\alpha) \geq \frac{D}{D + 1} \cdot \frac{3}{J + 2} \cdot \left( \log m - \frac{\log(J/2 + 1) + 1}{J} \right).
\]

If \( m \geq 5 \), then we obtain a nontrivial lower bound with \( J = 1 \), while for \( 3 \leq m \leq 4 \) we need to take \( J = 2 \), and for \( m = 2 \) we must take \( J = 3 \). Of course, the bound that we obtain is not sharp. However, our goal is not to get sharp bounds in this particular case, where other authors \[\text{[3, 4, 6, 10]}\] have used intricate techniques to obtain better bounds than we could obtain even if we took more care. Instead,
we aim to show how to obtain nontrivial bounds that, among other things, imply that Lehmer’s conjecture is true for an interesting class of polynomials that is larger than the class considered in [3, 4, 6, 10].

The proof of Theorem 10 uses the following standard Fejér kernel estimate, whose proof we relegate to Section 6.

**Proposition 12.** For all \( J \geq 1 \) we have

\[
\sup_{z \in \mathbb{C}, |z| \leq 1} \sum_{j=1}^{J} \left( 1 - \frac{j}{J+1} \right) \log |1 - z^j| \leq \frac{1}{2} \log \left( \frac{J}{2} + 1 \right) + \frac{1}{2}.
\]

**Proof of Theorem 10.** Let \( K \) be a number field such that \( \mathcal{A} \subset K \). For \( \alpha \in \mathcal{A} \) and \( v \in M_K \), we let

\[
\alpha_v = \begin{cases} 
\alpha & \text{if } \|\alpha\|_v \leq 1, \\
\alpha^{-1} & \text{if } \|\alpha\|_v > 1,
\end{cases}
\]

so in particular \( \|\alpha_v\|_v \leq 1 \). We now compute

\[
(n \log m) \Delta(\mathcal{A}, m, n) = \sum_{\alpha \in \mathcal{A}} \sum_{v|m} v(\alpha^n - 1) \quad \text{def. of } \Delta(\mathcal{A}, m, n), \\
\leq \sum_{\alpha \in \mathcal{A}} \sum_{v \in M_K^n} v(\alpha^n - 1) \quad \text{since } \alpha \in \mathbb{Z}, \\
= \sum_{\alpha \in \mathcal{A}} \sum_{v \in M_K^n} \log \|\alpha^n - 1\|_v \quad \text{product rule,} \\
\leq \sum_{\alpha \in \mathcal{A}} \sum_{v \in M_K^n} \log \|\alpha^n\|_v + \sum_{\alpha \in \mathcal{A}} \sum_{v \in M_K^n} \log \|\alpha^n_v - 1\|_v \\
= n \sum_{\alpha \in \mathcal{A}} h(\alpha) + \sum_{\alpha \in \mathcal{A}} \sum_{v \in M_K^n} \log \|\alpha^n_v - 1\|_v. \quad (10)
\]

We now replace \( \mathcal{A} \) with \( \mathcal{A}^j \). Then using \( h(\alpha^j) = jh(\alpha) \) and Proposition 8 which says that \( \Delta(\mathcal{A}, m, n) \leq \Delta(\mathcal{A}^j, m, n) \), we find that

\[
(n \log m) \Delta(\mathcal{A}, m, n) \leq nj \sum_{\alpha \in \mathcal{A}} h(\alpha) + \sum_{\alpha \in \mathcal{A}} \sum_{v \in M_K^n} \log \|\alpha^n_v - 1\|_v.
\]
We multiply by the Fejér multiplier $1 - \frac{j}{J+1}$ and sum over $1 \leq j \leq J$ to obtain

$$\frac{Jn \log m}{2} \Delta(A, m, n) \leq \frac{(J^2 + 2J)n}{6} \sum_{\alpha \in A} h(\alpha) + \sum_{\alpha \in A} \sum_{v \in \mathbb{R}_\infty^k} \sum_{j=1}^{J} \left(1 - \frac{j}{J+1}\right) \log \|\alpha_v^j n - 1\|_v.$$ 

Note that the sum over $v$ is over archimedean absolute values, so if we assume that $\alpha_v$ is chosen in the unit disk to maximize the innermost sum over $j$, we get the estimate

$$\frac{Jn \log m}{2} \Delta(A, m, n) \leq \frac{(J^2 + 2J)n}{6} \sum_{\alpha \in A} h(\alpha) + |A| \sup_{z \in \mathbb{C}} \left|z^J - 1\right|.$$ 

We can now use Proposition 12 to conclude that

$$\frac{Jn \log m}{2} \Delta(A, m, n) \leq \frac{(J^2 + 2J)n}{6} \sum_{\alpha \in A} h(\alpha) + \frac{|A|}{2} \left(\log \left(\frac{J}{2} + 1\right) + 1\right).$$

After a little bit of algebra, we obtain the desired result. □

We now use our main theorem to prove that Lehmer’s conjecture is true for a certain interesting collection of polynomials.

**Corollary 13.** Fix $0 < \epsilon \leq 1$. Then Lehmer’s conjecture (1) is true for the set of polynomials

$$\left\{ f(X) \in \mathbb{Z}[X] : \begin{array}{l} f(X) \text{ is monic, its roots are not roots of unity, and there exist integers } m \geq 2 \\
\text{and } n \geq \max\{2, \epsilon \deg(f)\} \text{ such that } \\
\Phi_{n-1}(X) \text{ divides } f(X) \text{ in } (\mathbb{Z}/m\mathbb{Z})[X] \end{array} \right\}. \quad (11)$$

More precisely, if $f(X)$ is in the set (11), then

$$\sum_{f(\alpha)=0} h(\alpha) \geq \frac{\log m}{185 \epsilon^{-1} \log(24 \epsilon^{-1})}. \quad (12)$$

**Remark 14.** Igor Shparlinski has pointed out that for large $m$, we may take $\epsilon = (\log \log m)/(\log m)$ and conclude that if $\Phi_{n-1}(X)$ divides $f(X)$ in $(\mathbb{Z}/m\mathbb{Z})[X]$ for some $n \geq ((\log \log m)/(\log m))(\deg f)$, then

$$\sum_{f(\alpha)=0} h(\alpha) \geq \frac{1}{185} + O\left(\frac{\log \log \log m}{\log m}\right).$$
where the big-\(O\) constant is absolute.

The proof of the corollary uses a combination of Theorem 10 and Proposition 7 as reformulated in Remark 9. We state the exact result that we require as a lemma.

**Lemma 15.** Let \( f(X) \in \mathbb{Z}[X] \) be a monic polynomial of degree \( D \) whose roots are not roots of unity, let \( m, n \geq 2 \) be integers, and suppose that \( \Phi_{n-1}(X) \) divides \( f(X) \) in \((\mathbb{Z}/m\mathbb{Z})[X]\). Then

\[
\sum_{f(\alpha)=0} h(\alpha) \geq \begin{cases} 
\frac{(\log m)}{264} & \text{if } \log m \geq D/16n, \\
\log m - \frac{128}{n} \log m \log(16D/n \log m) & \text{if } \log m \leq D/16n.
\end{cases}
\]

**Proof.** Let \( \mathcal{A}_f \) be the set of roots of \( f \). As noted in Remark 9, the divisibility condition on \( f \) implies that \( \Delta(\mathcal{A}_f, m, n) \geq (n-1)/n \). Substituting this into (9) of Theorem 10 and using \( |\mathcal{A}_f| = D \), we find that for all integers \( J \geq 1 \) we have

\[
\sum_{f(\alpha)=0} h(\alpha) \geq \frac{3}{J+2} \left( \frac{n}{n} - \frac{D \log(J/2+1)+1}{J} \right).
\]

Since we are not concerned with optimizing our constants, we observe that for \( n \geq 2 \) and \( J \geq 2 \), this implies that

\[
\sum_{f(\alpha)=0} h(\alpha) \geq \frac{1}{J} \left( \frac{1}{2} \log m - \frac{4D \log(J)}{n} \right). \tag{13}
\]

We now consider two cases. First, if \( m \) is large, say

\[
\log m \geq D/16n,
\]

then taking \( J = 57 \) gives

\[
\sum_{f(\alpha)=0} h(\alpha) \geq \frac{1}{J} \left( \frac{1}{2} \log m - \frac{4D \log(J)}{n} \right) \log m \geq \frac{\log m}{264}. \tag{14}
\]

Second, suppose that \( m \) is small,

\[
\log m \leq D/16n.
\]

Then we want to choose \( J \) to be an integer satisfying

\[
\frac{J}{\log J} \geq \frac{16D}{n \log m}. \tag{15}
\]

In particular, since \( 16D/n \log m \geq 256 \), it suffices to take

\[
J = \left\lfloor \frac{32D}{n \log m} \log \left( \frac{16D}{n \log m} \right) \right\rfloor - 1.
\]
Substituting (15) into (13) and adjusting the constants yields
\[
\sum_{f(\alpha)=0} h(\alpha) \geq \frac{\log m}{4J} \geq \frac{\log m}{(128D/n \log m) \log(16D/n \log m)}.
\] (16)

Combining (14) and (16) completes the proof of Lemma 15. □

Proof of Corollary 13. We are given that \( n \geq \max\{\epsilon D, 2\} \). If \( \log m \geq D/16n \), then Lemma 15 says that
\[
\sum_{f(\alpha)=0} h(\alpha) \geq \frac{\log m}{264}.
\]
This is stronger than (12), since we have assumed that \( \epsilon \leq 1 \), so we are reduced to the case that \( \log m \leq D/16n \). Since \( n \geq \epsilon D \), this implies that\[
\frac{D}{n \log m} \leq \frac{D}{\epsilon D \log m} \leq \frac{1}{\epsilon \log m},
\]
where the upper bound is at least 16. Substituting this into Lemma 15, we find that
\[
\sum_{f(\alpha)=0} h(\alpha) \geq \frac{\log m}{(128/\epsilon \log m) \log(16/\epsilon \log m)}.
\]
Since \( m \geq 2 \), this gives something slightly stronger than the desired result. □

3. An Elliptic Analogue of \( \Delta(A, m, n) \)

An amalgamation of Proposition 7, Remark 9, and Theorem 10 says that if \( f(X) \in \mathbb{Z}[X] \) is a monic polynomial of degree \( D \) whose roots are not roots of unity, then
\[
\left( f(X) \right. \text{ has coefficients congruent to 1 modulo } m \left. \right) \quad \implies \quad \Delta(A_f, m, D + 1) \geq \frac{D}{D + 1}
\]
\[
\implies \sum_{f(\alpha)=0} h(\alpha) \geq \frac{D}{D + 1} C_m.
\]
The key estimate is Theorem 10 which gives a general lower bound for \( \sum h(\alpha) \) in terms of \( \Delta(A, m, n) \). In this section we define an elliptic analogue of the quantity \( \Delta(A, m, n) \), and in the next section we prove an elliptic analogue of Theorem 10. We begin by recalling some basic properties of canonical height functions on elliptic curves.

Definition. Let \( E/K \) be an elliptic curve defined over a number field. We write
\[
\hat{h} : E(\bar{K}) \to \mathbb{R}
\]
for the absolute logarithmic canonical height \[20, \text{VIII \S 9}\], and for each \(v \in M_K\) we let

\[\hat{\lambda}_v : E(K_v) \smallsetminus \{0\} \to \mathbb{R}\]

be a local canonical height, normalized as described in \[19\] Chapter VI].

**Proposition 16.** The local canonical height satisfies the following:

(a) For all \(v \in M_K\) there is a constant \(c(v)\) such that

\[\lambda_v(P) \geq -c(v) \quad \text{for all } P \in E(K_v).\]

Further, if \(v \in M_K^0\) and \(E\) has good reduction at \(v\), then we can take \(c(v) = 0\).

(b) The global height is the sum of the local heights. Thus for any finite extension \(L/K\) and any \(P \in E(L) \smallsetminus \{0\}\) we have

\[\hat{h}(P) = \sum_{v \in M_L} \hat{\lambda}_v(P).\]

**Proof.** The first part of (a) follows from \[19\] Theorem VI.1.1(a)], which says in particular that \(\hat{\lambda}_v\) has a logarithmic pole as \(P \to O\) in the \(v\)-adic topology and that \(\lambda_v\) is bounded on the complement of any \(v\)-adic neighborhood of \(O\). The second part of (a) follow from \[19\] Theorem VI.4.1], which says that if \(P\) reduces to a non-singular point modulo \(v\), then

\[\hat{\lambda}_v(P) = \frac{1}{2} \max \{-v(x(P)), 0\} + \frac{1}{12} v(D_{E/K}).\]

This quantity is clearly non-negative. Finally, \[19\] Theorem VI.2.1] gives a proof of (b). \(\square\)

**Definition.** Given

- \(K/\mathbb{Q}\) a number field,
- \(m\) an integral idea of \(K\) with norm \(m = N_{K/\mathbb{Q}} m \geq 2\),
- \(E/K\) an elliptic curve, and
- \(P\) a finite set of nontorsion points in \(E(K)\),

we define

\[\Delta(P, m, n) = \sum_{P \in P} \frac{1}{\log m} \sum_{v|m} \frac{1}{n^2} \hat{\lambda}_v(nP).\]

This quantity is the elliptic analogue of the quantity \(\Delta(A, m, n)\) that we defined in Section \[4\].

The following estimate will be used later when we do an averaging argument. It is the analogue of Proposition \[8\].
Lemma 17. With notation as above, assume that $E$ has potential good reduction at every prime dividing $m$. Let $j \geq 1$ be an integer, and let $j\mathcal{P} = \{jP : P \in \mathcal{P}\}$. Then

$$\Delta(j\mathcal{P}, m, n) \geq \Delta(\mathcal{P}, m, n).$$

Proof. Replacing $K$ by a finite extension, we may assume that $E$ has good reduction at all primes dividing $m$. Let $v \in M_0^K$ be any place at which $E$ has good reduction, and let $\pi_v \in K$ be a uniformizer at $v$. Further, let

$$E_0(\bar{K}_v) \subset E_1(\bar{K}_v) \subset E_2(\bar{K}_v) \subset \cdots$$

be the formal group filtration of $E(\bar{K}_v)$; see [20, Chapters IV, VII]. Here $E_0 = E$, since we have assumed good reduction, and $E_1$ is the formal group. The explicit formula for $\hat{\lambda}_v$ [19, Theorem VI.4.1] then has the form

$$\hat{\lambda}_v(P) = \max \{r \geq 0 : P \in E_r(\bar{K}_v)\} v(\pi_v).$$

Since the filtration consists of subgroups, it is immediate that

$$\hat{\lambda}_v(jP) \geq \hat{\lambda}_v(P) \quad \text{for all } j \geq 1.$$

Summing over $P \in \mathcal{P}$ and $v | m$, and dividing by $n^2 \log m$, the desired result is immediate from the definition of $\Delta$. □

Remark 18. If $E$ has potential multiplicative reduction at $v$, then it is possible to have $\hat{\lambda}_v(jP) < \hat{\lambda}_v(P)$, so $\Delta(j\mathcal{P}, m, n)$ may be strictly smaller than $\Delta(\mathcal{P}, m, n)$.

4. A Height Lower Bound for Points on Elliptic Curves

In this section we prove our second main result, which is an elliptic analogue of the height lower bound given in Theorem 10. We do not explicitly keep track of the dependence on the field $K$ or the curve $E$, although it would be possible to do so. We start with a Fourier averaging estimate that is analogous to Proposition 12 and that has been applied in the past to the elliptic Lehmer conjecture [7], to Lang’s height lower bound conjecture [3], and to Arakelov theory [12]. In order to state the result, we use the following useful definition from [11].

Definition. Let $K/\mathbb{Q}$ be a number field. An $M_K$-constant is a map

$$c : M_K \to [0, \infty)$$

with the property that $\{v \in M_K : c(v) \neq 0\}$ is a finite set. (For convenience, we consider only non-negative $M_K$-constants.) A normalized $M_{\mathbb{Q}}$-constant is a collection of $M_K$-constants

$$c_K : M_K \to \mathbb{R},$$
one for each number field $K/\mathbb{Q}$, satisfying the compatibility condition that for all number fields $L/K$ and all $v \in M_K$,

$$\sum_{w \in M_L, w|v} \frac{[L_w : K_v]}{[L : K]} c_L(w) = c_K(v).$$

**Proposition 19.** Let $E/\overline{\mathbb{Q}}$ be an elliptic curve. There are normalized $\mathbb{Q}$-constants $c_1$ and $c_2$, depending only on $E$, such that for all integers $J \geq 2$, all nontorsion points $P \in E(\overline{\mathbb{Q}})$, and all absolute values $v \in M_{\overline{\mathbb{Q}}}$ we have

$$\sum_{j=1}^J \left( 1 - \frac{j}{J+1} \right) \hat{\lambda}_v(jP) \geq -c_1(v) \log(J) - c_2(v). \quad (17)$$

(We may, in fact, take $c_1(v) = 0$ for all nonarchimedean $v$.)

**Proof.** If $v$ is nonarchimedean and $E$ has good reduction at $v$, then the local height $\hat{\lambda}_v$ is non-negative, so we can take $c_1(v) = c_2(v) = 0$. For nonarchimedean $v$ of bad reduction, the inequality (17) with $c_1(v) = 0$ is proven in [8]. Finally, for archimedean $v$, the local height functions are Green’s functions and the desired result follows from a general theorem of Elkies [12, Theorem 5.1] that is valid on curves of positive genus. More precisely, Elkies’ theorem says that there is a constant $c = c(E, v)$ such that for any distinct points $P_0, \ldots, P_J \in E(K_v)$ we have

$$\sum_{0 \leq i < j \leq J} \hat{\lambda}_v(P_j - P_i) \geq -\frac{1}{2\pi} (J+1) \log J - cJ. \quad (18)$$

(We are using the fact that $\hat{\lambda}_v$ is an even function.) Taking $P_j = jP$ for $0 \leq j \leq J$, we find that

$$\sum_{0 \leq i < j \leq J} \hat{\lambda}_v(P_j - P_i) = \sum_{0 \leq i < j \leq J} \hat{\lambda}_v((j-i)P) = \sum_{j=1}^J (J+1-j) \hat{\lambda}_v(jP). \quad (19)$$

Combining (18) and (19) and dividing by $J+1$ gives (17). \qed

We have now assembled all of the tools required to prove our main result on elliptic curves.

**Theorem 20.** Suppose that we are given the following quantities:

- $K/\mathbb{Q}$ a number field.
- $E/K$ an elliptic curve.
- $n$ a positive integer.
- $m$ an integral ideal of $K$ with norm $m = N_{K/\mathbb{Q}}m \geq 2$.
- $\mathcal{P}$ a finite set of nontorsion points in $E(K)$. 

Suppose that we are given the following quantities:
Suppose further that \( E \) has potential good reduction at every prime dividing \( m \). Then there is a constant \( C_E \), depending only on \( E \), such that for all integers \( J \geq 1 \) we have

\[
\sum_{P \in \mathcal{P}} \hat{h}(P) \geq \frac{6}{(J+1)(J+2)} \left( \Delta(\mathcal{P}, m, n) \log m - C_E \frac{|\mathcal{P}|}{n^2} \cdot \frac{\log(J+1)}{J} \right).
\]

Proof. To ease notation, we let

\[
f_j = 1 - \frac{j}{J+1} \quad \text{and} \quad F_k = \sum_{j=1}^{J} j^k f_j.
\]

Earlier we used the values of \( F_0 \) and \( F_1 \). In this section we will use the values

\[
F_0 = \frac{J}{2} \quad \text{and} \quad F_2 = \frac{J(J+1)(J+2)}{12}.
\]

Replacing \( K \) by a finite extension, we may assume that \( \mathcal{P} \subset E(K) \). We let

\[
M_{K}^{\text{bad}} = M_{K}^{\infty} \cup \{ v \in M_{K} : E \text{ has bad reduction at } v \}.
\]

Then

\[
v \in M_{K} \setminus M_{K}^{\text{bad}} \implies \lambda_{v}(Q) \geq 0 \quad \text{for all } Q \in E(\bar{K}_v).
\]

We compute

\[
n^2 \sum_{P \in \mathcal{P}} \hat{h}(P) = \sum_{P \in \mathcal{P}} \hat{h}(nP)
\]

\[
= \sum_{P \in \mathcal{P}} \sum_{v \in M_{K}} \hat{\lambda}_{v}(nP)
\]

\[
\geq \sum_{P \in \mathcal{P}} \sum_{v | m} \hat{\lambda}_{v}(nP) + \sum_{P \in \mathcal{P}} \sum_{v \in M_{K}^{\text{bad}}} \hat{\lambda}_{v}(nP)
\]

\[
= (n^2 \log m)\Delta(\mathcal{P}, m, n) + \sum_{P \in \mathcal{P}} \sum_{v \in M_{K}^{\text{bad}}} \hat{\lambda}_{v}(nP).
\]

Replacing \( \mathcal{P} \) with \( j\mathcal{P} = \{ jP : P \in \mathcal{P} \} \) and using Lemma 17 which says that \( \Delta(j\mathcal{P}, m, n) \geq \Delta(\mathcal{P}, m, n) \) (this is where we use the assumption that \( E \) has potential good reduction at the primes dividing \( m \)), we find that

\[
n^2 j^2 \sum_{P \in \mathcal{P}} \hat{h}(P) \geq (n^2 \log m)\Delta(\mathcal{P}, m, n) + \sum_{P \in \mathcal{P}} \sum_{v \in M_{K}^{\text{bad}}} \hat{\lambda}_{v}(njP).
\]

Multiplying both sides by \( f_j \) and summing \( j = 1 \) to \( J \) gives

\[
F_2 n^2 \sum_{P \in \mathcal{P}} \hat{h}(P)
\]
\[ \geq F_0(n^2 \log m) \Delta(P, m, n) + \sum_{j=1}^{J} \sum_{P \in \mathcal{P}} \sum_{v \in M_{K}^{bad}} f_j \hat{\lambda}_v(njP) \]
\[ \geq F_0(n^2 \log m) \Delta(P, m, n) + |\mathcal{P}| \inf_{v \in M_{K}^{bad}} \sum_{Q \in E(K)} \sum_{j=1}^{J} f_j \hat{\lambda}_v(jQ). \]

Proposition \[19\] says that there are \( M_K \)-constants \( c_1 \) and \( c_2 \), depending only on \( E \), such that
\[ \inf_{Q \in E(K)} \sum_{j=1}^{J} f_j \hat{\lambda}_v(jQ) \geq -c_1(v) \log(J) - c_2(v). \]

Summing over \( v \in M_{K}^{bad} \) gives constants that depend only on \( E \), so adjusting the constants and using the assumption that \( J \geq 1 \), we find that there is a constant \( C_E \), depending only on \( E \), such that
\[ F_{2n^2} \sum_{P \in \mathcal{P}} \hat{\lambda}(P) \geq F_0(n^2 \log m) \Delta(P, m, n) - C_E |\mathcal{P}| \log(J + 1). \]

Using the formulas \[20\] for \( F_0 \) and \( F_2 \), dividing by \( F_{2n^2} \), and adjusting the constant gives the desired result. \( \square \)

Corollary \[13\] says roughly that the classical Lehmer’s conjecture is true for polynomials \( f(X) \) such that
\[ \Phi_{n-1}(X) \text{ divides } f(X) \text{ in } (\mathbb{Z}/m\mathbb{Z})[X] \text{ for some } n \geq \epsilon \deg(f). \] (21)

As noted in Remark \[9\] the divisibility condition in \[21\] is stronger than the assertion that \( \Delta(\mathcal{A}_f, m, n) \geq (n-1)/n \), where \( \mathcal{A}_f \) denotes the set of roots of \( f \). Since we assume that \( n \geq 2 \), this implies in particular that \( \Delta(\mathcal{A}_f, m, n) \) is uniformly bounded away from 0. Thus the following result is an elliptic version of a strengthening of Corollary \[13\].

Definition. Let \( E/K \) be an elliptic curve and let \( Q \in E(\bar{K}) \). We let
\[ \mathcal{P}_Q = \{ \sigma(Q) : \sigma \in \text{Gal}(\bar{K}/K) \} \text{ and } D_Q = [K(Q) : K] = |\mathcal{P}_Q|. \]

We remark that all of the points in \( \mathcal{P}_Q \) have the same canonical height; cf. \[20\] Theorem VIII.5.10.

Corollary 21. Let \( E/K \) be an elliptic curve defined over a number field. Fix constants \( \delta, \epsilon > 0 \). Then the elliptic Lehmer conjecture \[1\] is true for the following set of points:
\[ \left\{ Q \in E(\bar{K}) : \begin{array}{l}
\text{there exists an integral ideal } \mathfrak{m} \text{ of } K \text{ with } \\
N_{K/Q}\mathfrak{m} \geq 2 \text{ such that } E \text{ has good reduction at all primes dividing } \mathfrak{m} \text{ and an integer } \\
n \geq \max\{\sqrt{\epsilon D_Q}, 2\} \text{ with } \Delta(P, m, n) \geq \delta
\end{array} \right\}. \] (22)
For points in the set \( (22) \), the constant in \( (4) \) will have the form
\[
C_{E/K,\delta,\epsilon} \log m,
\]
where \( C_{E/K,\delta,\epsilon} \) is positive and depends only on the indicated quantities.

Proof. We are given that \( n \geq \sqrt{\epsilon D_Q} \) and \( \Delta(P_Q, m, n) \geq \delta \). Using these values in Theorem 20 together with some trivial estimates yields
\[
\sum_{P \in \mathcal{P}_Q} \hat{h}(P) \geq \frac{1}{J^2} \left( \delta \log m - \frac{C_E}{\epsilon} \cdot \frac{\log(J + 1)}{J} \right).
\]
We now choose \( J \) to be the smallest integer satisfying
\[
\frac{\log(J + 1)}{J} \leq \min \left\{ \frac{\epsilon \delta}{2C_E \log m}, \frac{1}{2} \right\}.
\]
This yields an estimate of the desired form
\[
D_Q \hat{h}(Q) \geq C_{E/K,\delta,\epsilon} \log m,
\]
where we are using the fact, noted earlier, that every point in \( \mathcal{P}_Q \) has canonical height equal to \( \hat{h}(Q) \).

\[\square\]

5. Other Congruence Conditions on the Coefficients

Cyclotomic polynomials play a key role in Lehmer’s conjecture, so the congruence condition \( (2) \) and the more general congruence divisibility condition \( (3) \) are natural ones to consider. However, there is no reason not to consider similar congruences in which the cyclotomic polynomial is replaced by some other polynomial. This was done in considerable generality by Samuels [17]. To illustrate, we reprove a special case of one of Samuels’ result and use it to make some remarks.

Definition. The length of a polynomial \( g(X) = \sum a_i X^i \in \mathbb{Z}[X] \) is the quantity
\[
L(g) = \sum |a_i|.
\]

Theorem 22. (Special Case of [17 Corollary 5.3]) Let \( m \geq 2 \) and let \( f(X) \in \mathbb{Z}[X] \) be a monic polynomial of degree \( D \) satisfying \( f(1) \neq 0 \). Further let \( u(X) \in \mathbb{Z}[X] \) be a polynomial of degree at most \( D - 1 \), and suppose that
\[
f(X) \equiv \Phi_D(X) + u(X) \pmod{m},
\]
but that \( f(X) \) has no roots in common with \( \Phi_D(X) + u(X) \). Then
\[
\sum_{f(\alpha) = 0} h(\alpha) \geq \frac{D}{D+1} \log \left( \frac{m}{L(X^{D+1} - 1 + (X - 1)u(X))} \right).
\]
Proof. We are given that

\[ f(X) = \Phi_D(X) + u(X) + mr(X) \quad \text{for some } r(X) \in \mathbb{Z}[X]. \]

Then

\[
\text{Res}\left(f(X), X^{D+1} - 1 + (X - 1)u(X)\right) \\
= \text{Res}\left(f(X), \Phi_D(X) + u(X)\right) \cdot \text{Res}\left(f(X), X - 1\right) \\
= \text{Res}\left(mr(X), \Phi_D(X) + u(X)\right) f(1) \\
= m^D \text{Res}\left(r(X), \Phi_D(X) + u(X)\right) f(1).
\]

By assumption, the resultants are nonzero integers, so we find that

\[ D \log m \leq \log |\text{Res}\left(f(X), X^{D+1} - 1 + (X - 1)u(X)\right)| \]

\[ = \sum_{f(\alpha) = 0} \sum_{v \in M_K^\infty} \log \|\alpha^{D+1} - 1 + (\alpha - 1)u(\alpha)\|_v \]

\[ = \sum_{v \in M_K^\infty} \sum_{\|\alpha\|_v > 1} \log \|\alpha^{D+1}\|_v \]

\[ + \sum_{v \in M_K^\infty} \sum_{\|\alpha\|_v > 1} \log \left\| \frac{\alpha^{D+1} - 1 + (\alpha - 1)u(\alpha)}{\alpha^{D+1}} \right\|_v \]

\[ + \sum_{v \in M_K^\infty} \sum_{\|\alpha\|_v \leq 1} \log \|\alpha^{D+1} - 1 + (\alpha - 1)u(\alpha)\|_v \]

\[ \leq h(\alpha^{D+1}) + D \sup_{|z| = 1} \log |z^{D+1} - 1 + (z - 1)u(z)| \quad (23) \]

\[ \leq (D + 1)h(\alpha) + D \log L\left(X^{D+1} - 1 + (X - 1)u(X)\right). \]

(We note that in (23), it suffices to take the supremum over |z| = 1, since log |w| is harmonic inside the unit disk.) \qed

Remark 23. The upshot of Theorem 22 is that if m is sufficiently large, then we obtain a Lehmer-type lower bound. However, in the cyclotomic case, i.e., u = 0, a Fourier averaging argument allowed us to prove nontrivial estimates for all values of m ≥ 2. We do not know how to perform such an averaging argument in the general case. It would also be interesting to prove a version of Theorem 22 under the weaker assumption that f(X) is divisible modulo m by \( \Phi_{n-1}(X) \) for, say, n ≥ \( \epsilon D \). Again we do not have the requisite averaging lemma.
Remark 24. If we take $u = 0$ in Theorem 22, we obtain the estimate
\[
\sum_{f(\alpha) = 0} h(\alpha) \geq \frac{D}{D + 1} \log \frac{m}{2}.
\]
This has the same form as Theorem 1, although the constant in Theorem 1 is a little bit better than ours (and our estimate is trivial for $m = 2$). On the other hand, it is interesting that such an elementary argument produces a lower bound that agrees with the best known lower bounds $[3, 4, 6, 10]$ up to an additional $O(1/m^2)$.

Remark 25. The estimate proven in Theorem 22 is nontrivial if and only if
\[
m > L(X^{D+1} - 1 + (X - 1)u(X)).
\]
As Samuels does in [17], it is sometimes possible to improve the estimate a little bit. We illustrate with the case $u(X) = -2$, so
\[
f(X) \equiv X^D + X^{D-1} + \cdots + X^2 + X - 1 \pmod{m}
\]
and
\[
L(X^{D+1} - 1 + (X - 1)u(X)) = L(X^{D+1} - 2X + 1) = 4.
\]
This gives a nontrivial height bound for $m \geq 5$. If $D$ is odd, then the supremum in (23) occurs at $z = -1$ and is equal to $\log 4$, but if $D$ is even, then the supremum is strictly smaller than $\log 4$ and we can obtain a small improvement in the theorem. However, for large (even) values of $D$ we have
\[
\sup_{|z| = 1} |z^{D+1} - 2z + 1| = 4 + O(D^{-2}) \quad \text{at } z \approx -e^{\pi i/(D+1)},
\]
so for $m = 4$ we only obtain $\sum h(\alpha) \gg D^{-2}$, which is weaker than Lehmer’s conjecture.

6. Proof of Proposition 12

In this section we give the proof of Proposition 12 for which we need the following standard lemma.

Lemma 26. For all $\theta \in \mathbb{R} \setminus 2\pi i\mathbb{Z}$ and all $t \geq 0$ we have
\[
\log |1 - e^{i\theta}| \leq \log |1 - e^{-t}e^{i\theta}| + \frac{1}{2} t.
\]

Proof. For notational convenience we let
\[
F_t(\theta) = \log |1 - e^{-t}e^{i\theta}| + \frac{1}{2} t - \log |1 - e^{i\theta}|,
\]
so we need to prove that $F_t(\theta) \geq 0$. We have
\[
F_0(\theta) = 0 \quad \text{for all } \theta \in \mathbb{R} \setminus 2\pi i\mathbb{Z}.
\]
For $t > 0$ we observe that
\[
\log |1 - e^{-t} e^{i\theta}| = \text{Re} \left( \sum_{n=1}^{\infty} -\frac{e^{-nt} e^{in\theta}}{n} \right)
\]
is given by an absolutely convergent series, so we may differentiate it term-by-term. Hence
\[
\frac{\partial F_t}{\partial t}(\theta) = \text{Re} \left( \sum_{n=1}^{\infty} \left( e^{-t} e^{i\theta} \right)^n \right) + \frac{1}{2} = \text{Re} \left( \frac{e^{-t+i\theta}}{1 - e^{-t+i\theta}} + \frac{1}{2} \right)
\]
\[
= \frac{e^{2t} - 1}{(e^t - \cos \theta)^2 + \sin^2 \theta} > 0 \quad \text{for all } t > 0.
\]
Thus for any fixed $\theta \in \mathbb{R} \setminus 2\pi i \mathbb{Z}$, the function $F_t(\theta)$ as a function of $t \geq 0$ satisfies $F_0(\theta) = 0$ and $(\partial F_t/\partial t)(\theta) \geq 0$. Hence $F_t(\theta) \geq 0$ for all $t \geq 0$.

Here is the elementary algebraic verification of the trigonometric identity that was used in the above calculation.
\[
\text{Re} \left( \frac{e^{-t+i\theta}}{1 - e^{-t+i\theta}} + \frac{1}{2} \right) = \text{Re} \left( \frac{e^{i\theta}}{e^t - e^{i\theta}} + \frac{1}{2} \right) = \text{Re} \left( \frac{e^{i\theta}(e^t - e^{-i\theta})}{e^{2t} - 2(e^{i\theta})e^t + 1} + \frac{1}{2} \right)
\]
\[
= \text{Re} \left( \frac{e^{i\theta} e^t - 1}{e^{2t} - 2(e^{i\theta})e^t + 1} + \frac{1}{2} \right) = \text{Re} \left( \frac{e^{i\theta} e^t - 1}{e^{2t} - 2(e^{i\theta})e^t + 1} + \frac{1}{2} \right)
\]
\[
= \frac{e^{2t} - 1}{(e^t - \cos \theta)^2 + \sin^2 \theta}.
\]

Proof of Proposition 12. The functions $\log |1 - z^j|$ are harmonic on the open unit disk $|z| < 1$, so the maximum occurs on the boundary. For $z = e^{i\theta}$ on the unit circle we estimate
\[
\sum_{j=1}^{J} \left( 1 - \frac{j}{J+1} \right) \log |1 - z^j|
\]
\[
\leq \sum_{j=1}^{J} \left( 1 - \frac{j}{J+1} \right) \left( \log |1 - e^{-t} e^{ij\theta}| + \frac{1}{2} t \right) \quad \text{from Lemma 26}
\]
\[
= \text{Re} \left( \sum_{j=1}^{J} \left( 1 - \frac{j}{J+1} \right) \sum_{k=1}^{\infty} -\frac{e^{-kt} e^{ijk\theta}}{k} \right) + \frac{Jt}{4}
\]
\[
= \text{Re} \left( \sum_{k=1}^{\infty} \frac{e^{-kt}}{k} \sum_{j=1}^{J} \left( 1 - \frac{j}{J+1} \right) e^{ijk\theta} \right) + \frac{Jt}{4}
\]
\[
= \sum_{k=1}^{\infty} \frac{e^{-kt}}{k} \left( \frac{1}{2} - \frac{1}{2J+2} \left| \sum_{j=0}^{J} e^{ijk\theta} \right|^2 \right) + \frac{Jt}{4}
\]
\[
\geq \sum_{k=1}^{\infty} \frac{e^{-kt}}{2k} + \frac{Jt}{4}
\]
\[
= -\frac{1}{2} \log(1 - e^{-t}) + \frac{Jt}{4}.
\]
This estimate holds for all \(t > 0\), so in particular we can set \(t = \log(1 + 2J^{-1})\), which (after some algebra) gives the estimate
\[
\sum_{j=1}^{J} f_j \log |1 - z^j| \leq \frac{1}{2} \log \left( \frac{J}{2} + 1 \right) + \frac{J}{4} \log \left( 1 + \frac{2}{J} \right).
\]
Finally we observe that \(x \log(1 + x^{-1}) \leq 1\) for all \(x \geq 0\), which gives the desired result. \(\square\)

References

[1] F. Amoroso and R. Dvornicich. A lower bound for the height in abelian extensions. \textit{J. Number Theory}, 80(2):260–272, 2000.
[2] P. E. Blanksby and H. L. Montgomery. Algebraic integers near the unit circle. \textit{Acta Arith.}, 18:355–369, 1971.
[3] P. Borwein, E. Dobrowolski, and M. J. Mossinghoff. Lehmer’s problem for polynomials with odd coefficients. \textit{Ann. of Math. (2)}, 166(2):347–366, 2007.
[4] P. Borwein, K. G. Hare, and M. J. Mossinghoff. The Mahler measure of polynomials with odd coefficients. \textit{Bull. London Math. Soc.}, 36(3):332–338, 2004.
[5] E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. \textit{Acta Arith.}, 34:391–401, 1979.
[6] A. Dubickas and M. J. Mossinghoff. Auxiliary polynomials for some problems regarding Mahler’s measure. \textit{Acta Arith.}, 119(1):65–79, 2005.
[7] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. \textit{Invent. Math.}, 93(2):419–450, 1988.
[8] M. Hindry and J. H. Silverman. On Lehmer’s conjecture for elliptic curves. In \textit{Séminaire de Théorie des Nombres, Paris 1988–1989}, volume 91 of \textit{Progr. Math.}, pages 103–116. Birkhäuser Boston, Boston, MA, 1990.
[9] M. Hindry and J. H. Silverman. \textit{Diophantine Geometry: An Introduction}, volume 201 of \textit{Graduate Texts in Mathematics}. Springer-Verlag, New York, 2000.
[10] M. I. M. Ishak, M. J. Mossinghoff, C. Pinner, and B. Wiles. Lower bounds for heights in cyclotomic extensions. \textit{J. Number Theory}, 130(6):1408–1424, 2010.
[11] S. Lang. \textit{Fundamentals of Diophantine Geometry}. Springer-Verlag, New York, 1983.
[12] S. Lang. \textit{Introduction to Arakelov Theory}. Springer-Verlag, New York, 1988.
[13] S. Lang. \textit{Algebra}, volume 211 of \textit{Graduate Texts in Mathematics}. Springer-Verlag, New York, third edition, 2002.
[14] M. Laurent. Minoration de la hauteur de Néron-Tate. In \textit{Séminaire de Théorie des Nombres}, Progress in Mathematics, pages 137–151. Birkhäuser, 1983. Paris 1981–1982.
[15] D. H. Lehmer. Factorization of certain cyclotomic functions. \textit{Ann. of Math. (2)}, 34(3):461–479, 1933.
[16] D. W. Masser. Counting points of small height on elliptic curves. Bull. Soc. Math. France, 117(2):247–265, 1989.
[17] C. L. Samuels. The Weil height in terms of an auxiliary polynomial. Acta Arith., 128(3):209–221, 2007.
[18] C. L. Samuels. Estimating heights using auxiliary functions. Acta Arith., 137(3):241–251, 2009.
[19] J. H. Silverman. Advanced Topics in the Arithmetic of Elliptic Curves, volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.
[20] J. H. Silverman. The Arithmetic of Elliptic Curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, second edition, 2009.
[21] C. Smyth. The Mahler measure of algebraic numbers: a survey. In Number theory and polynomials, volume 352 of London Math. Soc. Lecture Note Ser., pages 322–349. Cambridge Univ. Press, Cambridge, 2008.
[22] C. J. Smyth. On the product of the conjugates outside the unit circle of an algebraic integer. Bull. London Math. Soc., 3:169–175, 1971.
[23] C. L. Stewart. Algebraic integers whose conjugates lie near the unit circle. Bull. Soc. Math. France, 106(2):169–176, 1978.

E-mail address: jhs@math.brown.edu

Mathematics Department, Box 1917 Brown University, Providence, RI 02912 USA