1. Lehmer, Mahler and Jensen

1.1 Background: Lehmer's Paper

In 1933, D.H. Lehmer published a paper [Leh33] entitled 'Factorization of certain cyclotomic functions'. A by-product of his factorization method was a way of manufacturing large primes: 'large' should be interpreted in the light of available computing machinery in 1933 (see Section 1.6 below). The construction was to take a monic, integral polynomial

$$F(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x],$$

with factorization over $\mathbb{C}$

$$F(x) = \prod_{i=1}^{d}(x - \alpha_i).$$

Then, for every $n \in \mathbb{N}_{>0}$ define

$$\Delta_n(F) = \prod_{i=1}^{d}(\alpha_i^n - 1). \tag{1.1}$$

It is better to assume that no α_i is a root of unity (since if $\alpha_i^N = 1$ for some N, then $\Delta_n(F) = 0$ for all n divisible by N). In any case, the quantity $\Delta_n(F)$ is always an integer since the product (1.1) contains all the algebraic conjugates of all the zeros of F (see Remark A.5 in Appendix A for the details; alternatively, in Lemma 2.3 we show that $\Delta_n(F)$ is the cardinality of a finite group). Lehmer was able to produce some large primes as values of $\Delta_n(F)$. Substantial work on these sequences was also done by T.A. Pierce in his 1917 paper [Pie17], where the form of prime factors of $\Delta_n(F)$ was described.

Example 1.1. Let $F(x) = x^3 - x - 1$. Lehmer showed that

$$\Delta_{113}(F) = 63,088,004,325,217$$

and

$$\Delta_{127}(F) = 3,233,514,251,032,733$$

are primes.

The motivation in [Leh33] and [Pie17] may have been to generalize the classical notion of Mersenne number and Mersenne prime – Lehmer worked on related problems before and after this paper (see [BLS75], [BLS+83], [Leh30], [Leh32], [Leh47]). The Mersenne prime case is achieved by choosing the polynomial

$$F(x) = x - 2,$$

so that

$$\varDelta_n(F) = M_n = 2^n - 1.$$

In his paper, Lehmer demonstrated that $\varDelta_n(F)$ is more likely to produce primes if it does not grow too quickly, and measured the rate of growth by considering the ratio of successive terms,

$$\left|\frac{\varDelta_{n+1}(F)}{\varDelta_n(F)}\right|. \tag{1.2}$$

Lemma 1.2. *Provided no root α_i of F has $|\alpha_i| = 1$,*

$$\lim_{n\to\infty}\left|\frac{\varDelta_{n+1}(F)}{\varDelta_n(F)}\right| = \prod_{i=1}^{d} \max\{1, |\alpha_i|\}. \tag{1.3}$$

Proof. This is clear since we can treat each term in the product separately:

$$\lim_{n\to\infty}\left|\frac{\alpha^{n+1}-1}{\alpha^n - 1}\right| = \begin{cases} |\alpha| & \text{if } |\alpha| > 1, \\ 1 & \text{if } |\alpha| < 1. \end{cases}$$

Exercise 1.1. [1] Give examples to show that in general an integral polynomial may have zeros with unit modulus which are not unit roots.
[2] Show that a monic example of [1] can only occur in degree at least 4.

Exercise 1.2. Show that $\varDelta_n(F)$ is a *divisibility sequence*. That is, prove that if n divides m then $\varDelta_n(F)$ divides $\varDelta_m(F)$.

Remark 1.3. Lehmer made the following remark concerning the non-trivial problem of the convergence of (1.2) in the presence of possible unit modulus zeros (he assumed that F was irreducible, and defined $\varOmega$ to be the right-hand side of (1.3): 'It may happen that F has a root α on the unit circle. For $|\alpha| = 1$, (1.2) contributes an oscillating factor which, although it never vanishes or becomes infinite (since F is not a cyclotomic function), cannot be estimated readily. For lack of something better we use $\varOmega$ to measure the rate of increase of the sequence

$$\varDelta_1, \varDelta_2, \varDelta_3, \dots$$

even when some of the zeros of F lie on the unit circle.' In fact the expression (1.2) only converges if there are no unit modulus zeros, whereas the expression used in Lemma 1.10 below always converges.

1.2 Mahler's Measure

Thirty years later, Mahler used a generalization of the measure (1.3) of a polynomial in a quite different setting (see Remark 1.5 below).

Definition 1.4. For any non-zero polynomial

$$F(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 = a_d \prod_{i=1}^{d} (x - \alpha_i)$$

in $\mathbb{C}[x]$, define the *Mahler measure* of F to be

$$M(F) = |a_d| \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

In this definition, an empty product is assumed to be 1 so the Mahler measure of the non-zero constant polynomial $F(x) = a_0$ is $|a_0|$.

Write

$$m(F) = \log M(F)$$

for the *logarithmic Mahler measure*, and extend the definition to include $m(0) = \infty$. This convention looks a little strange, but makes sense in the dynamical interpretation: see Exercise 2.4 and Theorem 2.12 in Chapter 2. Since we often use $m(F)$, it will also be called the Mahler measure below.

Remark 1.5. This measure is called the Mahler measure because of two papers written by Mahler in the early 1960s – [Mah60] and [Mah62]. His interest in the quantity $M(F)$ was not to study it for its own merits, but instead to compare it with other kinds of measures – more natural ones in some sense. For a polynomial $F(x) = a_d x^d + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$, define

$$H(F) = \max_{0 \le 1 \le d} \{|a_i|\}, \qquad L(F) = \sum_{i=0}^{d} |a_i|,$$

the *height* and *length* of F respectively. Mahler proved that

$$|a_i| \le \binom{d}{i} M(F) \text{ for all } i = 0, \ldots, d \tag{1.4}$$

and also showed that all three measures are commensurate in the sense that

$$H(F) \ll M(F) \ll H(F) \tag{1.5}$$

and

$$L(F) \ll M(F) \ll L(F), \tag{1.6}$$

with the implied constants depending only on the degree d (see Appendix G for the notation $\ll$). Mahler [Mah64] also related the measure to the discriminant of the polynomial. The absolute value of the discriminant of F is defined to be

$$|\Delta(F)| = |a_d|^{2d-2} \prod_{i \neq j} |\alpha_i - \alpha_j|$$

where $F(x) = a_d \prod_{1 \leq i \leq d}(x - \alpha_i)$. Mahler showed that

$$|\Delta(F)| \leq d^d M(F)^{2d-2}. \tag{1.7}$$

Exercise 1.3. [1] Prove that

$$-d \log 2 + \ell(F) \leq m(F) \leq \ell(F),$$

where we write $\ell = \log L$. This is equivalent to an exact description of the implied constants in (1.6) above:

$$2^{-d} L(F) \leq M(F) \leq L(F).$$

[2] Give examples to show that the inequalities in part [1] and in (1.4) cannot be improved in general.
[3] Prove a weaker form of the inequality (1.7) as follows. Assume that

$$F(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0 = \prod_{1 \leq i \leq d} (x - \alpha_i)$$

is monic, so the absolute value of the discriminant is

$$|\Delta(F)| = \prod_{i \neq j} |\alpha_i - \alpha_j|.$$

Prove that

$$|\Delta(F)| \leq 2^{d(d-1)} M(F)^{2d-2}.$$

The inequality (1.5) requires some later material and is given in Exercise 1.11 below.

Definition 1.6. A polynomial is *cyclotomic* if all the zeros are roots of unity. The word cyclotomic means literally 'circle dividing' and it refers to the way that roots of unity divide up the unit circle.

Exercise 1.4. [1] Let $F \in \mathbb{Z}[x]$ denote a monic irreducible polynomial of degree d with zeros $\alpha_1, \ldots, \alpha_d$. Prove that, for any prime p,

$$p^d \leq \left| \prod_{i,j=1}^{d} (\alpha_i^p - \alpha_j) \right| \tag{1.8}$$

provided F is not cyclotomic.
[2] Let p denote a prime with

$$eL(F) < p < 2eL(F)$$

(which exists by Bertrand's postulate). Use this prime and (1.8) to deduce that

$$M(F) > 1 + \frac{\log 2e}{2e} \cdot \frac{1}{L(F)} \tag{1.9}$$

when F is irreducible and not cyclotomic. This exercise is based on Dobrowolski [Dob81, Lemma 2], where it is the first step towards a much deeper result. It follows from (1.9) that if F varies over a sequence of non-cyclotomic irreducible polynomials in $\mathbb{Z}[x]$ with $L(F)$ uniformly bounded *above*, the resulting non-zero values of $M(F)$ are uniformly bounded *below*.

Remark 1.7. [1] The polynomial $F(x) = x^3 - x - 1$ used in Example 1.1 has turned out to be very special. Among a certain infinite family of polynomials – the *non-reciprocal* polynomials – its measure is known to be minimal. See Smyth [Smy71] for the details and the survey paper by Boyd [Boy81] for an overview. We prove a weaker version of this result in Theorem 1.19 below.
[2] The quantity $|\Delta_n(F)|$ has an important interpretation in the theory of dynamical systems (see Section 2.1 below).
[3] In his paper, Lehmer mentioned that he could find no smaller measure of growth than that of the polynomial

$$G(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1, \tag{1.10}$$

and that is still the smallest known example. Of the ten zeros of (1.10), eight lie on the unit circle and just one lies outside.

The problem of verifying that integral polynomials have a smallest positive measure is now known as 'Lehmer's problem', and it seems to be a very deep problem. See Waldschmidt [Wal80], Boyd [Boy81] and Stewart [Ste78b] for surveys of this problem. In Sections 1.3, 1.4 and 1.5 below we show how versions of this problem may be solved for certain classes of polynomials. Lehmer's problem arises in many different areas. In algebraic dynamical systems it is related to the existence of algebraic models for certain abstract dynamical systems (see the discussions after Definition 2.7 and Theorem 4.2). Lehmer's problem also turns up in statistical mechanics (see Moussa [Mou83], [Mou90]; Barnsley, Bessis and Moussa [BBM79]) and in the study of iteration of complex functions (see Moussa [Mou86]; Moussa, Geronimo and Bessis [MGB84]).

The current best unconditional results on Lehmer's problem itself are probably the following. Blanksby and Montgomery [BM71] showed that if $F \in \mathbb{Z}[x]$ has $m(F) \neq 0$ and degree d, then

$$m(F) \geq \log\left(1 + \frac{1}{52d\log 6d}\right). \tag{1.11}$$

Dobrowolski, [Dob79] showed under the same hypotheses that

$$m(F) > \frac{1}{1200}\left(\frac{\log\log d}{\log d}\right)^3. \tag{1.12}$$

A similar estimate was also obtained independently by Cantor and Strauss [CS82], and Rausch [Rau85] improved the bound for large values of d. Louboutin [Lou83] strengthened the result, again for large d, and Voutier [?] has proved a similar result for *all* values of d. In a different direction, Dobrowolski [Dob81] proved that

$$m(F) > \frac{\log 2e}{2e(k+1)^k} \tag{1.13}$$

if F is a non-cyclotomic irreducible polynomial in $\mathbb{Z}[x]$ with k non-zero coefficients.

Dobrowolski, Lawton and Schinzel [DLS83] proved that if $F \in \mathbb{Z}[x]$ has $m(F) \neq 0$ and has k non-zero coefficients, then

$$m(F) > C = C(H(F), k), \tag{1.14}$$

where $H(F)$ is the maximum of the absolute values of the coefficients of F (cf. Remark 1.5). They also proved a bound of the form

$$m(F) > C(k) \tag{1.15}$$

involving only the number of non-zero cofficients. In Exercise 1.4 above some simple steps in the direction of the bounds involving only the number of non-zero coefficients are given. Dobrowolski [Dob91] gave an improved bound of the same form, showing that if F is a monic polynomial with $F(0) \neq 0$ that is not a product of cyclotomic factors then

$$M(F) \geq 1 + \frac{1}{a\exp(bk^k)}$$

where k is the number of non-zero coefficients of F and a, b are constants with $a \leq 13\,911$ and $b \leq 2.27$.

A beautiful and important observation from Mahler's paper [Mah60] is the following.

Lemma 1.8. [Mahler's lemma] *For any non-zero $F \in \mathbb{C}[x]$,*

$$m(F) = \int_0^1 \log|F(e^{2\pi i\theta})|d\theta.$$

Proof. This is a simple consequence of Jensen's formula: for any $\alpha \in \mathbb{C}$,

$$\int_0^1 \log |e^{2\pi i\theta} - \alpha| d\theta = \log \max\{1, |\alpha|\}.$$

That is, the (potentially improper) Riemann integral exists and has the stated value. This may be applied to each term in the factorization of F over $\mathbb{C}$.

For completeness, we include a proof of Jensen's formula. For the more interesting case (where $|\alpha| = 1$) we give a standard complex analysis proof and a short real analysis proof due to Young [You86].

Lemma 1.9. [Jensen's formula] *For any* $\alpha \in \mathbb{C}$,

$$\int_0^1 \log |\alpha - e^{2\pi i\theta}| d\theta = \log \max\{1, |\alpha|\}.$$

In the sequel it will be useful to write $\log^+ \lambda = \log \max\{1, \lambda\}$.

Proof. The statement is clear for $\alpha = 0$ so assume that $\alpha \neq 0$. First assume that $|\alpha| \neq 1$. Then

$$\int_0^1 \log |\alpha - e^{2\pi i\theta}| d\theta = \begin{cases} \log |\alpha| + \int_0^1 \log |1 - \alpha^{-1} e^{2\pi i\theta}| d\theta & \text{if } |\alpha| > 1; \\ \int_0^1 \log |1 - e^{-2\pi i\theta} \alpha| d\theta & \text{if } |\alpha| < 1. \end{cases}$$

The integral in the $|\alpha| < 1$ case may also be written (via the substitution $\theta \rightarrow -\theta$) as

$$\int_0^1 \log |1 - e^{2\pi i\theta} \alpha| d\theta.$$

It is therefore enough to prove that for any $\beta \in \mathbb{C}$ with $|\beta| < 1$,

$$\int_0^1 \log |1 - \beta e^{2\pi i\theta}| d\theta = 0.$$

Write $\Re(z)$, $\Im(z)$ for the real and imaginary parts of a complex number z. Notice that $\log |z| = \Re \log z$, so

$$\begin{aligned} \int_0^1 \log |1 - \beta e^{2\pi i\theta}| d\theta &= \Re \int_0^1 \log \left(1 - \beta e^{2\pi i\theta}\right) d\theta \\ &= \Re \int_0^1 \left(- \sum_{n=1}^{\infty} \frac{\beta^n}{n} e^{2\pi i\theta n} \right) d\theta \\ &= \Re \left(- \sum_{n=1}^{\infty} \frac{\beta^n}{n} \int_0^1 e^{2\pi i\theta n} d\theta \right) \\ &= 0, \end{aligned}$$

where the summation being taken out of the integral is justified because the sum is absolutely convergent.

We are left with the case $|\beta| = 1$, for which we give two proofs.

COMPLEX ANALYSIS PROOF. The integral is now singular, so we define

$$\int_0^1 \log|e^{2\pi i\theta} - \beta| d\theta = \lim_{\epsilon\to 0} \frac{1}{2\pi i} \int_{\Gamma(\beta,\epsilon)} \frac{1}{z} \log|z-\beta| dz$$

(if this limit exists), where $\Gamma(\beta, \epsilon)$ is the contour indicated in Figure 1.1.

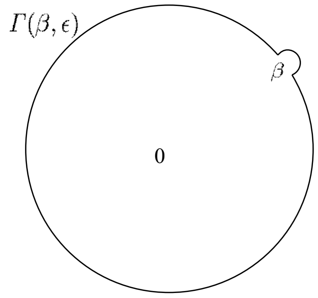

Fig. 1.1. The contour $\Gamma(\beta, \epsilon)$

Now $\frac{1}{z}\log|z-\beta| = \frac{1}{z}\Re\log(z-\beta)$, which is $\frac{1}{z}$ times the real part of a function which is analytic in the closed disc except for the point β. The residue from the singularity at 0 vanishes, so by Cauchy's theorem it does not contribute to the integral. It follows that

$$\frac{1}{2\pi i}\int_{\Gamma(\beta,\epsilon)} \frac{1}{z}\log(z-\beta)dz = \frac{1}{2\pi i}\int_{\gamma(\beta,\epsilon)} \frac{1}{z}\log(z-\beta)dz$$

where $\gamma(\beta, \epsilon)$ is the circle of radius ϵ around β. Parametrize $\gamma(\beta, \epsilon)$ by setting $z = \beta + \epsilon e^{2\pi i\theta}$ for $\theta \in [0, 1)$. Then $\frac{dz}{d\theta} = 2\pi i\epsilon e^{2\pi i\theta}$, so

$$\frac{1}{2\pi i}\int_{\gamma(\beta,\epsilon)} \frac{1}{z}\log(z-\beta)dz = \int_0^1 \frac{\epsilon e^{2\pi i\theta}}{\beta+\epsilon e^{2\pi i\theta}}\log(\epsilon e^{2\pi i\theta})d\theta.$$

Now

$$\left|\frac{\epsilon e^{2\pi i\theta}}{\beta+\epsilon e^{2\pi i\theta}}\right|$$

is bounded, so the integral is bounded in modulus by

$$C\cdot\epsilon|\log\epsilon|$$

which goes to zero as $\epsilon \to 0$.

Real analysis proof. Write the integral in the form

$$\frac{1}{2\pi}\int_0^{2\pi} \log|\alpha - e^{i\theta}|d\theta,$$

and assume that $|\alpha| = 1$; indeed, after translating by α^{-1} we may as well assume that $\alpha = 1$. Consider then

$$J = \int_0^{2\pi} \log|1 - e^{i\theta}|d\theta.$$

Since $|1 - e^{i\theta}| = 2\sin\frac{\theta}{2}$ for $\theta \in [0, 2\pi]$, it is enough to know that

$$J = \int_0^{\pi} \log\sin x dx = -\pi\log 2.$$

This exists as an improper Riemann integral since $\sin x \sim x$ for small x (see Appendix G for the meaning of $\sim$). Write $\sin x = 2\sin\frac{x}{2}\cos\frac{x}{2}$, then

$$J = \pi\log 2 + \int_0^{\pi}\log\sin\tfrac{x}{2}dx + \int_0^{\pi}\log\cos\tfrac{x}{2}dx.$$

Substituting $\frac{x}{2} = t$ in the first integral and $\frac{x}{2} = \frac{\pi}{2} - t$ in the second, we get

$$J = \pi\log 2 + 4\int_0^{\pi/2}\log\sin t dt = \pi\log 2 + 2J.$$

This ends the proof of Lemma 1.9.

Exercise 1.5. Justify the steps in the following alternative proof of the hard case in Lemma 1.9: $\int_0^1 \log|e^{2\pi i\theta} - 1|d\theta = \int_0^1 \log|e^{2\pi i\theta} + 1|d\theta$, so

$$\begin{aligned}\int_0^1 \log|e^{2\pi i\theta} - 1|d\theta &= \int_0^1 \log|e^{4\pi i\theta} - 1|d\theta \\ &= \int_0^1 \log|e^{2\pi i\theta} - 1|d\theta + \int_0^1 \log|e^{2\pi i\theta} + 1|d\theta,\end{aligned}$$

and therefore $\int_0^1 \log|e^{2\pi i\theta} + 1|d\theta = \int_0^1 \log|e^{2\pi i\theta} - 1|d\theta = 0$.

Another proof appears in the solution to Exercise 3.4[3].

A better (more robust) measure of the exponential growth rate of the quantity $|\Delta_n(F)|$ is

$$\lim_{n\to\infty}\frac{1}{n}\log|\Delta_n(F)|,$$

if this limit exists. The ratio (1.2) in fact *only* converges if there are no zeros with unit modulus – see Chothi, Everest and Ward [CEW97, Theorem 6.3] or Theorem 2.16 below for the details.

Lemma 1.10. *Provided no zero of F is a root of unity, the limit*

$$\lim_{n\to\infty} \frac{1}{n} \log |\Delta_n(F)|,$$

always exists for non-zero $F \in \mathbb{Z}[x]$, and the limit is $m(F)$.

Proof. First notice that

$$\log |\Delta_n(F)| = \sum_{i=1}^{d} \log |\alpha_i^n - 1|,$$

so each term can be treated separately. Recall that we write $\log^+ \lambda$ for $\log \max\{1, \lambda\}$.

If $|\alpha_i| > 1$, then

$$\frac{1}{n} \log |\alpha_i^n - 1| \longrightarrow \log |\alpha_i| = \log^+ |\alpha_i|.$$

If $|\alpha_i| < 1$, then

$$\frac{1}{n} \log |\alpha_i^n - 1| \longrightarrow 0 = \log^+ |\alpha_i|.$$

If $|\alpha_i| = 1$ then there is a subsequence $n_j \to \infty$ with the property that $\alpha_i^{n_j} \to 1$, so

$$\log |\alpha_i^{n_j} - 1| \longrightarrow -\infty.$$

The question is this: how fast does it happen? This is answered using a simple application of Baker's theorem (see Lemma 1.11 below). We claim that for any algebraic number α_i, not a unit root,

$$|\alpha_i^n - 1| > \frac{A}{n^B} \text{ for all } n, \tag{1.16}$$

for positive constants A and B, independent of n. It follows that

$$\log |\alpha_i^n - 1| = O(\log n),$$

so

$$\frac{1}{n} \log |\alpha_i^n - 1| \longrightarrow 0 = \log^+ |\alpha_i|$$

again (see Appendix G for the meaning of $O(\log n)$).

In fact the statement of Lemma 1.10 is much weaker than Baker's theorem – which is used to prove the estimate (1.16). An earlier estimate – due to Gelfond [Gel60] – is exactly equivalent to Lemma 1.10. This is pointed out in the context of the dynamical interpretation (cf. Chapter 2) in Lind's paper [Lin82, Section 4]. We have chosen to use Baker's theorem because it is more accessible in the literature and is more widely known.

We have left the proof of the estimate (1.16) to one side.

Lemma 1.11. *For $\alpha \in \bar{\mathbb{Q}}$, not a root of unity, $|\alpha| = 1$,*

$$|\alpha^n - 1| > \frac{A}{n^B}$$

for all $n \geq 1$ and constants A and B depending only on α.

Recall the notation $\ll$ (cf. Appendix G): (1.16) may be written

$$|\alpha^n - 1| \gg \frac{1}{n^B}.$$

For the proof we use Baker's theorem.

Theorem 1.12. [Baker's theorem] *Let $\alpha_1, \dots, \alpha_r$ be algebraic numbers, $\mathbf{n} \in \mathbb{Z}^r$ an integer vector, and write $|\mathbf{n}| = \max\{|n_i|\}$. Then for any choices of the logarithm branches, if $|n_1 \log \alpha_1 + \dots + n_r \log \alpha_r|$ is non-zero, it is bounded below by*

$$|n_1 \log \alpha_1 + \dots + n_r \log \alpha_r| \gg \frac{1}{|\mathbf{n}|^c}, \tag{1.17}$$

where c is a constant depending only on $\alpha_1, \dots, \alpha_r$.

Proof. Various versions of this were proved in Baker's series of papers [Bak66], [Bak67a], [Bak67b], [Bak68]. An expository treatment of the stronger inhomogeneous form of (1.17) is in [Bak75, Chapter 3].

Proof (of Lemma 1.11). We are only concerned with values of n for which α^n is very close to 1. Writing $\alpha = e^{i\theta}$ for some $\theta \in \mathbb{R}$, we see that α^n is close to 1 if and only if there is an $m \in \mathbb{Z}$ for which the real number $n\theta + 2\pi m$ is close to 0. Now

$$\alpha^n - 1 = e^{i(n\theta + 2\pi m)} - 1 \sim i(n\theta + 2\pi m) \tag{1.18}$$

for small values of $n\theta + 2\pi m$. It is sufficient therefore to find a lower bound of the right form for

$$in\theta + 2\pi i m. \tag{1.19}$$

Choosing any branch of the logarithm we may write $\alpha = e^{i\theta} = e^{\log \alpha}$, and choosing a non-principal branch we may write $1 = e^{2\pi i}$. Thus (1.19) can be written in the form

$$n \log \alpha + m \log 1.$$

Since this expression cannot be zero (recall that α is not a unit root), Theorem 1.12 says that

$$|in\theta + 2\pi i m| = |n \log \alpha + m \log 1| \gg \frac{1}{(\max\{|n|, |m|\})^c}.$$

On the other hand, $n\theta + 2\pi m$ is small, so n and m are close to constant multiples of each other, which shows that

$$|n \log \alpha + m \log 1| \gg \frac{1}{|n|^c}.$$

The desired estimate follows since $|z-1| > |\log z|$ for $|z-1| < 1$.

Exercise 1.6. [1] Prove that

$$m(F(x)) = m(F(x^n))$$

for all $n \geq 1$.
[2] Let $F \in \mathbb{C}[x]$ have degree d. Mahler proved in [Mah61] that

$$m(F') \leq m(F) + \log d.$$

Prove that this is equivalent to the statement that for any complex numbers $\alpha_1, \dots, \alpha_d$,

$$\int_0^1 \log \left| \sum_{j=1}^{d} \frac{1}{e^{2\pi i\theta} - \alpha_j} \right| d\theta \leq \log d. \tag{1.20}$$

Give examples to show that the estimate cannot be improved for all F.

A proof of (1.20) using complex analysis is given in Appendix D.

Question 1. Can you find an elementary proof of (1.20)?

Question 2. Is there a meaningful *lower* bound for $m(F')$? Any lower bound for $m(F')$ in terms of $m(F)$ must necessarily involve some dependence on the constant coefficient $F(0)$, as the example $F(x) = x - N$ shows. Experiment to find a sharp lower bound for $m(F')$. As a starting point, notice that $F(x) = x - N$ satisfies

$$m(F) + \log |d/F(0)| \leq m(F').$$

Lehmer calculated the following measures:

$$\begin{aligned} M(x^2 - x - 1) &= 1.618\dots, \\ M(x^3 - x - 1) &= 1.324\dots, \\ M(x^4 - x - 1) &= 1.380\dots, \\ M(x^5 - x^3 - 1) &= 1.362\dots, \\ M(x^6 - x - 1) &= 1.370\dots, \\ M(x^7 - x^3 - 1) &= 1.379\dots. \end{aligned}$$

He also studied the 'symmetric' polynomials (we now call these polynomials *reciprocal*, see Definition 1.17 below). Among these he found

$$M(x^6 - x^4 - x^3 - x^2 + 1) = 1.401\dots,$$

and

$$M(x^8 - x^5 - x^4 - x^3 + 1) = 1.280\dots,$$

but found no polynomials with smaller measure than

$$M(G) = 1.176\dots,$$

where

$$G(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1.$$

This polynomial does indeed generate some large primes: he found that

$$\sqrt{\Delta_{379}(G)} = 37{,}098{,}890{,}596{,}487$$

is prime (another prime appears in his paper, but it would appear this is what was intended). Notice that the values of Δ_n will be squares for a symmetric polynomial, so it is natural to look for prime values of the square root.

In the next few sections partial results in the direction of Lehmer's problem are described.

1.3 Lehmer's Problem I: Schinzel's Theorem

The result in this section concerns polynomials all of whose zeros are real. This is a special case of a more general result due to Schinzel, [Sch73] concerning heights of polynomials over totally real fields.

Lemma 1.13. *For any $d \geq 1$, let $y_1, \dots, y_d > 1$ be real numbers. Then*

$$(y_1 - 1)\dots(y_d - 1) \leq \left((y_1 \dots y_d)^{1/d} - 1\right)^d. \tag{1.21}$$

Proof. This is a well-known application of the convexity of $x \mapsto \log(e^x - 1)$; see Hardy, Littlewood and Polya [HLP34, Section 3.6].

Theorem 1.14. [Schinzel] *Suppose that $F \in \mathbb{Z}[x]$ is monic with degree d, $F(-1)F(1) \neq 0$ and $F(0) = \pm 1$. If the zeros of F are all real then*

$$M(F) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{d/2},$$

with equality if and only if F is a product of a power of $x^2 - x - 1$ and a power of $1 - x - x^2$.

Proof. Consider $E = \prod_{i=1}^{d} |\alpha_i^2 - 1|$; this is greater than or equal to 1 since F is monic. Now

$$E = \frac{1}{M(F)^2} \prod_{|\alpha_i|<1} |\alpha_i^{-2} - 1| \times \prod_{|\alpha_i|>1} |\alpha_i^2 - 1|.$$

By Lemma 1.13, it follows that

$$E \le \frac{1}{M(F)^2}\left(M(F)^{4/d}-1\right)^d = \left(M(F)^{2/d}-M(F)^{-2/d}\right)^d.$$

Since $1 \le E$, it follows that

$$M(F)^{2/d}-M(F)^{-2/d} \ge 1,$$

so

$$M(F) \ge \left(\frac{1+\sqrt{5}}{2}\right)^{d/2}.$$

Exercise 1.7. Explain why the condition $F(-1)F(1) \ne 0$ must be imposed for Theorem 1.14. Where is the real zeros condition used? Prove that equality can only occur as stated in the theorem.

Corollary 1.15. *If $F \in \mathbb{Z}[x]$ has real zeros then*

$$m(F) \ge \log\left(\frac{1+\sqrt{5}}{2}\right) = 0.481\ldots.$$

Proof. If F does not have ± 1 as leading and constant coefficient, then $m(F) \ge \log 2 = 0.693\ldots$ (cf. start of proof of Theorem 1.19), so this follows from Theorem 1.14.

Remark 1.16. For a general polynomial $F \in \mathbb{Z}[x]$ with real zeros and

$$F(0)F(-1)F(1) \ne 0$$

a similar result to Theorem 1.14 holds. Let

$$F(x) = a\prod_{i=1}^{d}(x-\alpha_i)$$

with constant coefficient $F(0) = c \ne 0$. Then $\prod_{|\alpha_i|>1}|\alpha_i| = \frac{M(F)}{a}$. Similarly $\prod_{|\alpha_i|<1}|\alpha_i| = \frac{c}{M(F)}$. Now consider

$$E = a^2\prod_{i=1}^{d}|\alpha_i^2-1|,$$

which is an integer greater than or equal to 1. Rearranging the product gives

$$E = a^2\prod_{|\alpha_i|<1}|\alpha_i|^2\left|1-\frac{1}{\alpha_i^2}\right| \times \prod_{|\alpha_i|>1}|\alpha_i^2-1|$$

$$
\begin{aligned}
&= \frac{a^2c^2}{M^2} \prod_{|\alpha_i|<1} \left|1 - \frac{1}{\alpha_i^2}\right| \times \prod_{|\alpha_i|>1} |\alpha_i^2 - 1| \\
&\leq \frac{a^2c^2}{M^2} \left(\left(\frac{M^2}{a^2} \cdot \frac{M^2}{c^2} \right)^{1/d} - 1 \right)^d \\
&= \left(M^{2/d} - \frac{(ac)^{2/d}}{M^{2/d}} \right)^d
\end{aligned}
$$

by Lemma 1.13. Hence, since $E \geq 1$,

$$1 \leq M^{2/d} - \frac{(ac)^{2/d}}{M^{2/d}},$$

so

$$M^{2/d} \geq 1 + \frac{(ac)^{2/d}}{M^{2/d}}.$$

Since $|ac| \geq 1$, this implies

$$1 + M^{-2/d} \leq M^{2/d}$$

and the result follows as before.

A short proof of Schinzel's theorem appears in the paper of Hoehn and Skoruppa [HS93]. Improved lower bounds appear in a paper of Flammang [Fla97]. See also Smyth's papers [**?**] and [**?**] for further results in the real case.

1.4 Lehmer's Problem II: Smyth's Theorem

The polynomials that are not 'symmetric' turn out to have a uniform lower bound for their Mahler measures, so candidates for smaller Mahler measures than Lehmer's example must be among the symmetric polynomials. Boyd has carried out extensive calculations of measures for reciprocal polynomials in [Boy80], [Boy89]. It is a remarkable fact that it is sufficient to look only at polynomials of height 1 (that is, with coefficients in $\{0, +1, -1\}$; for an explanation of why this is so see Mossinghoff [Mos98, Section 3.2]). Further calculations have been done by Mossinghoff [Mos95], [Mos98]; he has also found a new limit point near 1.309 in the set of (exponential) Mahler measures of integer polynomials. The paper [MPV98] by Mossinghoff, Pinner and Vaaler explores the polynomials obtained by adding a monomial to a product of cyclotomics, giving some small examples of Mahler measures. As they point out, Lehmer's best example (1.10) is given by such a procedure:

$$G(x) = (x-1)^2(x+1)^2(x^2+x+1)^2(x^2-x+1) - x^5.$$

Definition 1.17. Suppose $F \in \mathbb{C}[x]$ has degree d; write $F^*(x) = x^d F(x^{-1})$. Then F is *reciprocal* if $F = F^*$, and is *non-reciprocal* otherwise.

For example, Lehmer's best (smallest measure) example is reciprocal, while the polynomial $x^3 - x - 1$ is not.

In 1971 C.J. Smyth published the following remarkable theorem (see [Smy71]).

Theorem 1.18. [Smyth] *If $F(x) \in \mathbb{Z}[x]$ is a non-reciprocal polynomial, and $F(0)F(1) \neq 0$, then*

$$m(F) \geq m(x^3 - x - 1) = \log(1.324\ldots) = 0.281\ldots$$

The condition that $F(0) \neq 0$ simply means F is not divisible by x, and $F(1) \neq 0$ means F is not divisible by $x - 1$. Clearly some condition about divisibility by $x-1$ is required for if we multiply any reciprocal polynomial by $x-1$ the measure does not change but the polynomial becomes non-reciprocal.

In his thesis, Smyth also proved a stronger result:

$$M(F) > M(x^3 - x - 1) + 10^{-4}$$

unless F is reciprocal or is the minimum polynomial of $(\pm\theta_0)^{1/k}$ for some $k \geq 1$, where $\theta_0 = 1.324\ldots$ is the real zero of $x^3 - x - 1$.

We shall prove a weaker result, which is a good account of Smyth's basic method and gives a uniform lower bound for the measure of non-reciprocal polynomials. This result was known to Smyth before he proved Theorem 1.18 and has been proved independently by several people, including Stewart [Ste78a].

Theorem 1.19. *If $F \in \mathbb{Z}[x]$ is non-reciprocal and $F(0)F(1) \neq 0$, then*

$$m(F) \geq \tfrac{1}{2} \log \tfrac{5}{4} = 0.111\ldots.$$

In the proof we will need the following.

Exercise 1.8. Suppose $F \in \mathbb{Z}[x]$ is monic and irreducible, $F(1) \neq 0$, and F has a zero θ with $|\theta| = 1$. Show that F must be reciprocal. (Hint: $\bar{\theta}$ is also a root).

Proof (of Theorem 1.19). We can assume that F is irreducible, monic (since if $F(x) = a\prod(x - \alpha_i)$ then $m(F) \geq \log|a|$), $F(0)F(1) \neq 0$, and $F(0) = \pm 1$: if $F(0) \neq \pm 1$, then

$$2 \leq |F(0)| = \prod |\alpha_i| \leq M(F),$$

so $m(F) \geq \log 2 > \frac{1}{2} \log \frac{5}{4}$ (here and below write $\prod$ to denote the product taken over all the roots of F).

Notice that

$$G(z) = \frac{F(0)F(z)}{F^*(z)} = \frac{F(0)\prod(z-\alpha_j)}{\prod(1-z\alpha_j)}$$
$$= \frac{F(0)\prod(z-\alpha_j)}{\prod(1-z\bar{\alpha_j})}$$

since $\{\alpha_j\} = \{\bar{\alpha_j}\}$.

It is clear that $F(1) = F^*(1)$, so if $F^* = -F$ then $F^*(1) = -F(1)$ hence $F(1) = 0$, which is impossible. We deduce that F is not identically equal to $-F^*$.

We now claim that

$$G(z) = 1 + a_k z^k + \ldots \in \mathbb{Z}[[z]],$$

convergent in some neighbourhood of zero (that $G(0) = 1$ is clear). This remark (due to Raphael Salem [Sal45]) is seen as follows. Since F is monic,

$$F^*(z) = 1 + \ldots \pm z^d,$$

so

$$\frac{1}{F^*(z)} = 1 + \ldots \in \mathbb{Z}[[z]]$$

by the binomial theorem.

Now by Exercise 1.8 we may write

$$G(z) = \frac{F(0)\prod_{|\alpha_j|<1}\left(\frac{z-\alpha_j}{1-\bar{\alpha_j}z}\right)}{\prod_{|\alpha_j|>1}\left(\frac{1-\bar{\alpha_j}z}{z-\alpha_j}\right)} = \frac{f(z)}{g(z)}$$

where f and g are holomorphic functions in an open region containing the closed unit disc.

Notice that $|z| = 1$ if and only if $\bar{z} = \frac{1}{z}$. Assume that $|z| = 1$ and consider a typical factor $\left(\frac{z-\alpha_j}{1-\bar{\alpha_j}z}\right)$ of $f(z)$:

$$\left(\frac{z-\alpha_j}{1-\bar{\alpha_j}z}\right)\overline{\left(\frac{z-\alpha_j}{1-\bar{\alpha_j}z}\right)} = \left(\frac{z-\alpha_j}{1-\bar{\alpha_j}z}\right)\left(\frac{\bar{z}-\bar{\alpha_j}}{1-\alpha_j\bar{z}}\right)$$
$$= \left(\frac{z-\alpha_j}{1-\bar{\alpha_j}z}\right)\left(\frac{1-\bar{\alpha_j}z}{z-\alpha_j}\right) = 1$$

so

$$\left|\frac{z-\alpha_j}{1-\bar{\alpha_j}z}\right| = 1$$

for all j, and therefore $|f(z)| = 1$.

A similar argument applies to g. We deduce that

$$|f(z)| = |g(z)| = 1 \text{ for } |z| = 1. \tag{1.22}$$

Now write

$$f(z) = b + b_1 z + \dots$$

and

$$g(z) = c + c_1 z + \dots$$

absolutely convergent in the closed unit disc. It follows that

$$G(z) = 1 + a_k z^k + \dots = \frac{b + b_1 z + \dots}{c + c_1 z + \dots} \tag{1.23}$$

in some (smaller) disc. Now b and c are real and (without loss of generality) positive; moreover

$$b = |f(0)| = \prod_{|\alpha_j|<1} |\alpha_j| = \frac{1}{M(F)}$$

(since $\prod |\alpha_j| = 1$) and similarly $g(0) = \frac{1}{M(F)}$ so $b = c > 0$. Now compare terms in (1.23) to see that

$$\begin{aligned} b = c = &\ \frac{1}{M(F)}, \\ b_1 = &\ c_1, \\ &\ \vdots \\ b_{k-1} = &\ c_{k-1} \\ ca_k + c_k = &\ b_k \end{aligned}$$

If $\max\{|c_k|, |b_k|\} < \frac{b}{2} = \frac{c}{2}$, then

$$c \le |ca_k| = |b_k - c_k| \le |b_k| + |c_k| < b,$$

which contradicts $b = c$. It follows that

$$\max\{|c_k|, |b_k|\} \ge \frac{b}{2} = \frac{c}{2}. \tag{1.24}$$

Assume without loss of generality that (1.24) holds with

$$|b_k| \ge \frac{b}{2}$$

(if not, repeat the argument that follows with g replacing f, noting that $|c_k| \ge \frac{c}{2}$). Consider

$$f(z) = b + b_1(z) + \ldots + b_k z^k + \ldots$$

(where k is the power appearing in $G(z)$in equation (1.23)). We know by (1.22) that $|f(z)| = 1$ on $|z| = 1$, so

$$\int_0^1 |f(e^{2\pi i\theta})|^2 d\theta = 1. \tag{1.25}$$

Lemma 1.20. [Parseval's formula] *Suppose that $\phi : \mathbb{C} \to \mathbb{C}$ is holomorphic in an open region containing the closed unit disc, with Taylor expansion*

$$\phi(z) = e_0 + e_1 z + \ldots,$$

$e_i \in \mathbb{C}$. *Then*

$$\int_0^1 |\phi(e^{2\pi i\theta})|^2 d\theta = \sum_{i=0}^{\infty} |e_i|^2.$$

Applying Parseval's formula to f we see that

$$b^2 + |b_1|^2 + \ldots + |b_k|^2 + \ldots = 1,$$

so

$$b^2 + |b_k|^2 \leq 1.$$

On the other hand

$$|b_k| \geq \frac{b}{2},$$

so

$$\tfrac{5}{4} b^2 \leq 1.$$

Since $b = \frac{1}{M(F)}$, we deduce that

$$M(F)^2 \geq \tfrac{5}{4},$$

proving Theorem 1.19.

Remark 1.21. Smyth uses the third coefficient of G, together with a more sophisticated use of Parseval's formula to arrive at his definitive result, Theorem 1.18.

It remains to prove Parseval's formula. This is a simple application of the standard orthogonality relations for the family of functions $\{e^{2\pi int}\}$.

Proof (of Lemma 1.20). Notice that

$$|\phi(e^{2\pi i\theta})|^2 = \phi(e^{2\pi i\theta}) \cdot \overline{\phi(e^{2\pi i\theta})},$$

so

$$\begin{aligned}\int_0^1 |\phi(e^{2\pi i\theta})|^2 d\theta &= \int_0^1 \left(\sum_{m=0}^{\infty} e_m e^{2\pi i m\theta}\right)\left(\sum_{n=0}^{\infty} \bar{e_n} e^{-2\pi i n\theta}\right) d\theta \\ &= \int_0^1 \left(\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} e_m \bar{e_n} e^{2\pi i(m-n)\theta}\right) d\theta \\ &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\left(\int_0^1 e_m \bar{e_n} e^{2\pi i(m-n)\theta} d\theta\right)\end{aligned}$$

by the absolute convergence of the Taylor series on $|z| = 1$. On the other hand

$$\int_0^1 e^{2\pi i(m-n)\theta} d\theta = \begin{cases} 1 & \text{if } m = n; \\ 0 & \text{if not.}\end{cases}$$

So the integral reduces to

$$\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\left(\int_0^1 e_m \bar{e_n} e^{2\pi i(m-n)\theta} d\theta\right) = \sum_{m=0}^{\infty} |e_m|^2$$

as required.

To close this section we give another application of Parseval's formula by proving Gonçalves' formula.

Theorem 1.22. [Gonçalves' formula] *Let $F \in \mathbb{R}[z]$ be a monic polynomial with $|F(0)| \geq 1$. Then*

$$M(F)^2 + M(F)^{-2} \leq \sum_{j=0}^{d} a_j^2, \tag{1.26}$$

where $F(z) = z^d + a_{d-1}z^{d-1} + \ldots + a_0$.

Proof. Write

$$F(z) = \prod_{j=1}^{d}(z - \alpha_j).$$

By Parseval's formula (Lemma 1.20)

$$\begin{aligned}\sum_{j=0}^{d} a_j^2 &= \int_0^1 |F(e^{2\pi i\theta})| d\theta \\ &= \int_0^1 \left(\prod_{|\alpha_j|>1} |e^{2\pi i\theta} - \alpha_j|^2 \cdot \prod_{|\alpha_j|\leq 1} |e^{2\pi i\theta} - \alpha_j|^2\right) d\theta \\ &= M(F)^2 \int_0^1 \left(\prod_{|\alpha_j|>1} |e^{2\pi i\theta} - \alpha_j^{-1}|^2 \cdot \prod_{|\alpha_j|\leq 1} |e^{2\pi i\theta} - \alpha_j|^2\right) d\theta \\ &= M(F)^2 \int_0^1 |G(e^{2\pi i\theta})|^2 d\theta,\end{aligned}$$

where

$$G(z) = \prod_{|\alpha_j|>1} (z - \alpha_j^{-1}) \cdot \prod_{|\alpha_j|\le 1} (z - \alpha_j) = z^d + \ldots \pm \left(a_0/M(F)^2\right).$$

Apply Parseval's formula to G to get

$$\sum_{j=0}^{d} a_j^2 \geq M(F)^2 \left(1 + \frac{a_0^2}{M(F)^4}\right) \geq M(F)^2 + M(F)^{-2}.$$

Remark 1.23. [1] The original proof is due to Gonçalves [Gon50]. The proof presented here is taken from Smyth's doctoral thesis.
[2] Schinzel [Sch82] gives a different proof starting from the observation that $F(z)F(z^{-1})$ has constant coefficient $\sum_{j=1}^{d} a_j^2$.

Exercise 1.9. Prove the complex version of Gonçalves' formula: if $F \in \mathbb{C}[z]$ has $|a_0| \geq 1$, prove that

$$M(F)^2 + M(F)^{-2} \leq \sum_{j=0}^{d} |a_j|^2.$$

The next two exercises show how lower bounds for Mahler's measure may be used to deduce irreducibility results for certain trinomials. Let $H(x)$ denote the polynomial $x^m \pm x^n \pm 1$.

Exercise 1.10. [1] Prove that H has at most one non-reciprocal factor over $\mathbb{Q}$. (Hint: use Theorems 1.18 and 1.22).
[2] Show that the reciprocal factors of H are cyclotomic.

Exercise 1.11. Prove the inequality (1.5) by finding the best possible values for the implied constants.

1.5 Lehmer's Problem III: Zhang's Theorem

In the previous section, the involution $F \mapsto F^*$ on the ring of integral polynomials was used to make non-trivial estimates for the measure of polynomials not fixed by the involution (Definition 1.17 and Theorem 1.18). In a similar spirit, we introduce another involution: for $F \in \mathbb{Z}[x]$ define

$$F_*(x) = F(1 - x). \tag{1.27}$$

It is clear that $F \mapsto F_*$ is an involution on the set of polynomials.

Theorem 1.24. [Zhang, Zagier] *Let ω denote a primitive 6th root of unity. Suppose $F \in \mathbb{Z}[x]$ has degree d, and $F(0)F(1)F(\omega) \neq 0$. Then*

$$m(F) + m(F_*) \geq \frac{d}{2} \log\left(\frac{1+\sqrt{5}}{2}\right) \tag{1.28}$$

with equality if and only if F or F_* is a power of $x^4 - x^3 + x^2 - x + 1$.

Exercise 1.12. Explain why the condition $F(0)F(1)F(\omega) \neq 0$ must be imposed for Theorem 1.24.

This theorem was proved originally as an application of a theorem of Zhang [Zha92] in the context of heights of algebraic numbers (cf. Section 5.8). His proof used Arakelov theory and did not give the optimal lower bound in (1.28). Zagier [Zag93] gave a beautiful elementary proof, also in the context of heights, yielding the optimal bound. We follow Zagier's proof, although phrased in terms of Mahler's measure. The proof is similar in spirit to the proof of Theorem 1.19.

Let $\omega, \bar{\omega}$ denote the roots of $x^2 - x + 1 = 0$. Theorem 1.24 will follow directly from Lemma 1.27 below. To motivate this, we first consider the special case where F and F_* are monic and both have constant term ±1. An example is $F(x) = x^2 - x - 1$.

Lemma 1.25. *There is a constant $A \geq 1$ such that for every complex number $z \notin \{0, 1, \omega, \bar{\omega}\}$,*

$$\log|z^2 - z + 1| + 1 \leq A\,(|\log|z|| + |\log|1-z||).$$

Corollary 1.26. *Suppose F and F_* in $\mathbb{Z}[x]$ are both monic with constant term ±1 and $F(0)F(1)F(\omega) \neq 0$. Then*

$$m(F) + m(F_*) \geq \frac{d}{2A}.$$

Proof. Apply Lemma 1.25 to each $z = \alpha_i$ to obtain

$$\sum_{i=1}^{d} \log|\alpha_i^2 - \alpha_i + 1| + d \leq A\sum_{i=1}^{d} |\log|\alpha_i|| + A\sum_{i=1}^{d} |\log|1-\alpha_i||.$$

Since F and F_* are monic, $m(F) = \sum \log^+|\alpha_i|$ and $m(F_*) = \sum \log^+|1-\alpha_i|$. On the other hand, the assumption on the constant terms means that

$$|\prod_{i=1}^{d} \alpha_i| = |\prod_{i=1}^{d}(1-\alpha_i)| = 1$$

so

$$m(F) = \tfrac{1}{2}\textstyle\sum_{i=1}^{d} |\log|\alpha_i||$$

and

$$m(F_*) = \tfrac{1}{2}\textstyle\sum_{i=1}^{d} |\log|1-\alpha_i||.$$

Thus

$$\begin{aligned} d \le \sum_{i=1}^{d} \log|\alpha_i^2 - \alpha_i + 1| + d &\le A\sum_{i=1}^{d} |\log|\alpha_i|| + A\sum_{i=1}^{d} |\log|1-\alpha_i|| \\ &\le 2A\left(m(F) + m(F_*)\right) \end{aligned}$$

giving the required inequality.

Proof (of Lemma 1.25). Consider the function

$$f(z) = \frac{\log\left|z^2 - z + 1\right| + 1}{\left|\log|z|\right| + \left|\log|1-z|\right|}$$

for $z \in \mathbb{C}\backslash\{0, 1, \omega, \bar{\omega}\}$. As $|z| \to \infty$, $f(z) \to 1$. For values of z near the points $z = \omega$ or $\bar{\omega}$, $f(z)$ is large and negative. Finally, the function is continuous everywhere except at the intersection of the circles $|z| = |1-z| = 1$, where it is large and negative. It follows that the function is bounded above uniformly on all of $\mathbb{C}$.

Theorem 1.24 follows from a refined version of Lemma 1.25 that makes the constant explicit and uses $\log^+|\cdot|$ instead of $\left|\log|\cdot|\right|$.

Lemma 1.27. *For any $z \in \mathbb{C}\backslash\{0, 1, \omega, \bar{\omega}\}$,*

$$\begin{aligned} \log^+|z| + \log^+|1-z| \ge \frac{\sqrt{5}-1}{2\sqrt{5}} &\log|z^2 - z| \\ &+\frac{1}{2\sqrt{5}}\log|z^2 - z + 1| + \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right), \end{aligned}$$

with equality holding if and only if z or $1-z$ equals $e^{\pm\pi i/5}$ or $e^{\pm 3\pi i/5}$.

Proof (of Theorem 1.24). First notice that $e^{\pm\pi i/5}$, $e^{\pm 3\pi i/5}$ are the roots of $x^4 - x^3 + x^2 - x + 1 = 0$.

If F is monic, then applying Lemma 1.27 to each zero α_i in turn gives

$$\begin{aligned} m(F) + m(F_*) &\ge \frac{\sqrt{5}-1}{2\sqrt{5}}\sum_{i=1}^{d}\log|\alpha_i^2 - \alpha_i| \\ &\quad+\frac{1}{2\sqrt{5}}\sum_{i=1}^{d}\log|\alpha_i^2 - \alpha_i + 1| + \frac{d}{2}\log\left(\frac{1+\sqrt{5}}{2}\right) \\ &\ge \frac{d}{2}\log\left(\frac{1+\sqrt{5}}{2}\right) \end{aligned}$$

since

$$|\prod_{i=1}^{d}\left(\alpha_i^2-\alpha_i\right)| \text{ and } |\prod_{i=1}^{d}\left(\alpha_i^2-\alpha_i+1\right)|$$

are positive integers.

If F has leading coefficient a then add $2\log|a|$ to the left-hand side of Lemma 1.24, which then becomes $m(F)+m(F_*)$. Add $\log|a|$ to the right-hand side to obtain, after writing $\log|a| = \frac{\sqrt{5}-1}{2\sqrt{5}}\log|a|^2+\frac{1}{2\sqrt{5}}\log|a|^2$,

$$\frac{\sqrt{5}-1}{2\sqrt{5}}\log|a^2\prod_{i=1}^{d}(\alpha_i^2-\alpha_i)|+\frac{1}{2\sqrt{5}}\log|a^2\prod_{i=1}^{d}(\alpha_i^2-\alpha_i+1)| \\ +\frac{d}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)\geq\frac{d}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)$$

since $|a^2\prod_{i=1}^{d}(\alpha_i^2-\alpha_i)|$ and $|a^2\prod_{i=1}^{d}(\alpha_i^2-\alpha_i+1)|$ are positive integers.

Proof (of Lemma 1.27). Define a function g by

$$g(z)=\frac{\sqrt{5}-1}{2\sqrt{5}}\log|z^2-z|+\frac{1}{2\sqrt{5}}\log|z^2-z+1|+\frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right) \\ -\log^+|z|-\log^+|1-z|.$$

If $|z|$ is large then $g(z)$ behaves like $-\log|z|$ and, in particular, $g(z)\to-\infty$ as $|z|\to\infty$. Similarly, if z is close to one of the points $0,1,\omega,\bar{\omega}$ then $g(z)$ is large and negative. Away from these points, g is continuous, and so attains its maximum on some finite point or points. Off the circles $|z|=1$ and $|1-z|=1$ the function is the real part of a holomorphic function, so by the maximum principle for harmonic functions (see [CKP83, p. 46] for example) the maxima must be attained on these circles (cf. Appendix D). The involutions $z\mapsto 1-z$ and $z\mapsto\bar{z}$ preserve g, so it is enough to restrict attention to $z=e^{i\theta}$ for $0\leq\theta\leq\pi$.

First suppose that $0\leq\theta\leq\frac{\pi}{3}$, so $|1-z|\leq 1$. Then

$$g(z)=\tfrac{\sqrt{5}-1}{2\sqrt{5}}\log\left(2\sin\tfrac{\theta}{2}\right)+\tfrac{1}{2\sqrt{5}}\log\left(2\cos\theta-1\right)+\tfrac{1}{2}\log\left(\tfrac{1+\sqrt{5}}{2}\right).$$

Write $S=4\sin^2\frac{\theta}{2}$ (so that $0\leq S\leq 1$ for $0\leq\theta\leq\frac{\pi}{3}$). Then

$$g(z)=\tfrac{\sqrt{5}-1}{4\sqrt{5}}\log S+\tfrac{1}{2\sqrt{5}}\log(1-S)+\tfrac{1}{2}\log\left(\tfrac{1+\sqrt{5}}{2}\right).$$

Differentiating with respect to S shows that the unique maximum of g for $S\in(0,1)$ is attained at $S=\frac{3-\sqrt{5}}{2}$, where $g=0$ and $\theta=\frac{\pi}{5}$.

A similar argument holds for $\frac{\pi}{3}\leq\theta\leq\pi$; here $1\leq S\leq 4$ and

$$\begin{aligned} g(z) &= \tfrac{-\sqrt{5}-1}{2\sqrt{5}} \log\left(2\sin\tfrac{\theta}{2}\right) + \tfrac{1}{2\sqrt{5}} \log\left(1-2\cos\theta\right) + \tfrac{1}{2}\log\left(\tfrac{1+\sqrt{5}}{2}\right) \\ &= \tfrac{-\sqrt{5}-1}{4\sqrt{5}} \log S + \tfrac{1}{2\sqrt{5}} \log(S-1) + \tfrac{1}{2}\log\left(\tfrac{1+\sqrt{5}}{2}\right). \end{aligned}$$

The unique maximum of g is attained at $S = \frac{3+\sqrt{5}}{2}$, where $g = 0$ and $\theta = \frac{3\pi}{5}$.

To close this section, we mention some related results. Rhin and Smyth [RS97] showed that if $H \in \mathbb{Z}[x]$ is divisible by x but is not $\pm x^n$ for any n, and $G \in \mathbb{Z}[x]$ is irreducible, then

$$m(G(H(x))) > Cd$$

for some constant C, where d is the degree of the composition $G(H(x))$.

Exercise 1.13. Prove that for any polynomial $F \in \mathbb{Z}[x]$, the polynomial FF_* can be written in the form

$$F(x)F_*(x) = G(x(1-x))$$

for some polynomial $G \in \mathbb{Z}[x]$.

Dresden [Dre98] has extended Theorem 1.24 in a different direction. If α is an algebraic integer, and F_1 is the minimum polynomial of α, F_2 the minimum polynomial of $\frac{1}{1-\alpha}$ and F_3 the minimum polynomial of $1 - \frac{1}{1-\alpha}$, then he shows that the two smallest values of

$$\frac{1}{d}\left(m(F_1) + m(F_2) + m(F_3)\right)$$

are 0 and 0.4218..., where d is the degree of α. As he points out (p. 819, *ibid.*) this has the following consequence: if $F \in \mathbb{Z}[x]$ is a polynomial of degree d with the property that the cyclic group of order three generated by the map $z \mapsto 1 - \frac{1}{z}$ is a subgroup of its Galois group, then

$$m(F) \geq \frac{d}{3}(0.4218\ldots).$$

1.6 Large Primes in 1933

Lehmer's calculations, including the 16-digit prime 3 233 514 251 032 733 were not aimed at generating record-breaking primes, but rather at understanding primes appearing in a novel fashion. Appendix E contains some extensions of Lehmer's calculations (and their elliptic analogues).

Essentially all large primes arise from the sequences $2^n \pm 1$, for which there are special primality tests. The famous Mersenne problem asks if $M_n = 2^n - 1$ is prime for infinitely many values of n. It is well-known that $2^n + 1$ can only be prime when n is a power of 2 and very few instances of $2^{2^k}+1$ being prime are known; however 2^n+1 is sometimes a product of a small factor and a large prime. For comparison, Table 1.1 shows some record primes, breaking off with the largest prime to be found without the use of electronic computing machines and ending with the current largest known prime, found by Clarkson, Woltman and Kurowski as part of GIMPS. Some of the information in this section is taken with permission from Chris Caldwell's Prime Page on the world wide web at `http://www.utm.edu/research/primes/`.

Notice that Robinson's – and all subsequent – calculations were performed on a computer. The computer age, far from killing the subject off, seems to have caused a revival. Laura Nickel and Curt Noll were at high-school when they discovered their record-breaking prime. The Euler–Fermat theorem, which was generalized by Pierce [Pie17] and Lehmer [Leh33], is described below. Table 1.1 is far from complete – see Ribenboim [Rib95b] for more details. Large primes of other forms (notably $(2^n+1)/3$) continue to be studied using methods from Elliptic Curve theory (see Bateman *et al.* [BSW89] and Morain [Mor90]).

Number	**Digits**	**Year**	**Prover and Method**
$2^{17}-1$	6	1588	Cataldi; trial division
$2^{19}-1$	6	1588	Cataldi; trial division
$2^{31}-1$	10	1722	Euler; Euler–Fermat theorem
$(2^{59}-1)/179\,951$	13	1867	Landry; Euler–Fermat theorem
$2^{127}-1$	39	1876	Lucas; Lucas–Lehmer test
$(2^{148}+1)/17$	44	1951	Ferrier; Proth's theorem
$\vdots$	$\vdots$	$\vdots$	$\vdots$
M_{2281}	687	1952	Robinson; Lucas–Lehmer test
M_{11213}	3376	1963	Gillies; Lucas–Lehmer test
M_{21701}	6533	1978	Nickel & Noll; Lucas–Lehmer test
M_{86243}	25 962	1982	Slowinski; Lucas–Lehmer etc.
M_{216091}	65 050	1985	Slowinski; Lucas–Lehmer etc.
M_{859433}	258 716	1994	Slowinski & Gage; Lucas–Lehmer etc.
$M_{3021377}$	909 526	1998	Clarkson, Woltman & Kurowski; GIMPS

Table 1.1. A brief history of large primes.

Lemma 1.28. [Euler–Fermat theorem] *If p and q are odd primes, and p divides 2^q-1, then $p\equiv 1$ (mod q) and $p\equiv\pm1$ (mod 8).*

Exercise 1.14. Prove the Euler–Fermat theorem.

The Lucas–Lehmer test is the following.

Theorem 1.29. [Lucas–Lehmer test] *Let p be an odd prime. Then the Mersenne number $2^p - 1$ is prime if and only if $2^p - 1$ divides S_{p-1}, where $S_{n+1} = S_n^2 - 2$ and $S_1 = 4$.*

Exercise 1.15. Prove Theorem 1.29.

The last result mentioned above is part of a long list of results for numbers of special forms.

Theorem 1.30. [Proth's theorem, 1878] *Let $n = h \cdot 2^k + 1$ with $2^k > h$. If there is an integer a such that $a^{(n-1)/2}$ is congruent to -1 (mod n), then n is prime.*

This is a special case of a more general result; see Ribenboim [Rib95b] for the whole story.

GIMPS (the Great Internet Mersenne Prime Search), founded by George Woltman and others, is a very efficient system for using idle time on many different computers scattered all over the world to perform a coordinated search for Mersenne primes.

Question 3. Let $F(x) = x^3 - x - 1$. Are there infinitely many primes in the sequence $\Delta_n(F)$? For some calculations in this direction, see Appendix E.

Question 4. Can the arithmetic properties of the sequences considered by Lehmer be developed in the same way that the arithmetic properties of binary sequences have? See Ribenboim [Rib95a], Stewart [Ste77] for background, and van der Poorten [Poo89] and references therein for an introduction to the large body of results on recurrence sequences in general.

1.7 When Does the Measure Vanish?

Lehmer's problem asks about small positive values of $m(F)$. In this section we show that the situation where $m(F) = 0$ can be completely understood using Kronecker's lemma.

Theorem 1.31. [Kronecker] *Suppose that $\alpha \neq 0$ is an algebraic integer and the algebraic conjugates $\alpha_1 = \alpha, \dots, \alpha_d$ of α all have modulus $|\alpha_j| \leq 1$. Then α is a root of unity.*

Proof. Consider the polynomial

$$F_n(x) = \prod_{i=1}^{d} (x - \alpha_i^n), \tag{1.29}$$

where F_1 is the minimal polynomial for α. The coefficients of F_n are symmetric functions in the algebraic integers α_j^n so they are (rational) integers.

Each of the coefficients is uniformly bounded as n varies because $|\alpha_j| \leq 1$ for all j, so the set

$$\{F_n\}_{n\in\mathbb{N}}$$

must be finite. It follows that there is a pair $n_1 \neq n_2$ for which

$$F_{n_1} = F_{n_2},$$

so

$$\{\alpha_1^{n_1}, \dots, \alpha_d^{n_1}\} = \{\alpha_1^{n_2}, \dots, \alpha_d^{n_2}\}.$$

For each permutation $\tau \in S_d$ (the permutation group on d symbols), define an action of τ on the set of roots by

$$\alpha_i^{n_1} = \alpha_{\tau(i)}^{n_2}.$$

Then if τ has order r in S_d,

$$\alpha_i^{n_1^r} = \alpha_i^{n_2^r},$$

so

$$\alpha_i^{n_1^r}\left(\alpha_i^{n_2^r - n_1^r} - 1\right) = 0,$$

which shows that α_i must be a unit root since $\alpha_i \neq 0$.

Remark 1.32. Kronecker's lemma relates an analytic property of algebraic numbers (a condition on the modulus of the zeros) to an algebraic property (that the zeros must be torsion points in the group of complex numbers of modulus one).

A polynomial in $\mathbb{Z}[x]$ is called *primitive* if the coefficients have no non-trivial common factor.

Theorem 1.33. *Suppose $F \in \mathbb{Z}[x]$ is non-zero, primitive and $F(0) \neq 0$. Then $m(F) = 0$ if and only if all the zeros of F are roots of unity.*

Proof. Assume that all the zeros of F are roots of unity. Then the leading coefficient of F must be ± 1 since F divides $x^N - 1$ for some $N \geq 1$. So, from the definition, $m(F) = 0$.

Conversely, if $m(F) = 0$ then it is clear that F must be (plus or minus) a monic polynomial, so all the zeros are algebraic integers, and all must have modulus less than or equal to 1. Apply Kronecker's lemma to see they must all be unit roots.

Remark 1.34. We could restate this by saying that for primitive F, $m(F) = 0$ if and only if F is a monomial times a cyclotomic polynomial.

Exercise 1.16. If $F \in \mathbb{Z}[x]$ is cyclotomic, prove that $F^* = \pm F$.