Thue's Fundamentaltheorem, I: The general case

by

Paul M. Voutier (London)

1. Introduction

1.1. Background. In the 1840's, Liouville [16] established the existence of transcendental numbers by actually constructing one. His construction was based on his discovery that for any algebraic number α of degree $n \geq 2$, there exists a real number $c(\alpha) > 0$ such that

$$\left| \alpha - \frac{p}{q} \right| > \frac{c(\alpha)}{|q|^n}$$

for all integers p and q with $q \neq 0$. It was this work which first demonstrated the now well-established link between transcendence and diophantine problems.

In 1909, Thue [25] improved upon Liouville's diophantine result by introducing a method which eventually led, in 1955, to Roth's proof [20] that for any irrational algebraic number α and any $\epsilon > 0$, there exists $c(\alpha, \epsilon) > 0$ such that

$$\left| \alpha - \frac{p}{q} \right| > \frac{c(\alpha, \epsilon)}{|q|^{2+\epsilon}}$$

for all integers p and q with $q \neq 0$.

We call the exponents on $|q|$ in these inequalities *irrationality measures for α* and Roth's irrationality measures are essentially best possible.

But the reader should not be misled by this phrase "best possible", for here, as is often the case, there is more to be done. From Liouville's proof it is possible to explicitly determine the constant, $c(\alpha)$, but this is not true for the results of Thue or Roth. This is important as an irrationality measure even slightly less than n along with an explicit constant (such a result is called *effective*) can yield bounds on the size of solutions of many classes of diophantine equations.

[101]

At present, there are three methods available for obtaining such effective irrationality measures.

The first is due to Alan Baker, who, in 1964, published two papers [3, 4] in which he obtained such effective irrationality measures for certain algebraic numbers of the form $z^{m/n}$. As an example, he showed that for all integers p and q, with $q \neq 0$,

$$\left| 2^{1/3} - \frac{p}{q} \right| > \frac{10^{-6}}{|q|^{2.955}}.$$

Such results, via this technique, have since been improved, notably through Chudnovsky's analysis of denominators of the coefficients of certain hypergeometric functions [13]. The best result currently known, from [28], states that for any integers p and q, with $q \neq 0$,

$$\left| 2^{1/3} - \frac{p}{q} \right| > \frac{0.25}{|q|^{2.4325}}.$$

Baker also pioneered the second method. Later in the 1960's, he [5] established a remarkable result: lower bounds for linear forms in logarithms. Among the many applications of this result, in a refined form, are effective irrationality measures which are better than Liouville's for any algebraic number of degree at least three. The reader is invited to consult [6] where effective irrationality measures for numbers of the form $\sqrt[3]{n}$ with $n \in \mathbb{Z}$ are established.

Finally, in the early 1980's, Bombieri [8] combined elements of the non-effective method of Thue and Siegel with a result of Dyson, which was itself discovered for such diophantine approximation purposes, to create a method which under suitable conditions gives rise to effective irrationality measures much better than Liouville's. Along with van der Poorten and Vaaler, he [9] later refined this method in the case of numbers which are cubic irrationalities over number fields.

1.2. The present work. In this article, we shall consider ideas related to the first method, the basis of which lies in the work of Thue, his Fundamentaltheorem [26]. This work was a continuation of his earlier results [23, 24] in which he explicitly determined polynomials $P_r(x)$ and $Q_r(x)$ such that

$$Q_r(x)x^{1/n} - P_r(x) = (x-1)^{2r+1}\overline{S}_r(x),$$

where $\overline{S}_r(x)$ is regular at $x = 1$.

Siegel [21] recognised these $P_r(x)$ and $Q_r(x)$ as hypergeometric polynomials. He [22] also recognised that the polynomials, $F(x)$, satisfying the differential equation in Thue's Fundamentaltheorem are those given in our Lemma 3.2 for $m = 2$.

In earlier papers [11, 12, 15], Thue's Fundamentaltheorem was used to completely solve several families of Thue equations and inequalities. In this paper, we investigate the precise conditions under which Thue's Fundamentaltheorem yields effective irrationality measures for algebraic numbers.

As a result, we show that Thue's Fundamentaltheorem includes all the effective irrationality measures for numbers of the form $z^{1/n}$, which can be obtained by Baker's first method above and its refinements.

But, in addition to that, we also obtain effective irrationality measures for a new family of algebraic numbers. These results include all the previous ones ([11, 12, 15, 27]) derived from Thue's Fundamentaltheorem.

Furthermore, like Yuan [32], we are able to extend our results to diophantine approximation over imaginary quadratic fields (the only other number fields besides $\mathbb{Q}$ that possess the property of "discreteness" of its integers).

However, there are some related tools that are not dealt with here. In particular, it is possible to use Padé approximations to several functions simultaneously to obtain effective irrationality measures (see [13]). A striking example of applying this technique is Bennett's paper [7], in which it is used to obtain effective irrationality measures for numbers of the form $(b/a)^{1/n}$, where a and b are "small" rational integers. These cannot be treated by the usual "non-simultaneous" technique.

See also Wakabayashi's papers [30, 31] where simultaneous Padé approximations to the functions $\sqrt{1 - a_1 x}$ and $\sqrt{1 - a_2 x}$ are used to obtain effective irrationality measures for the real roots of some families of polynomials of the form $x^4 - a^2 x^2 + b$. These roots are not covered by our results here.

Finally, in a forthcoming paper [29], we show why Thue's Fundamentaltheorem holds and, as a consequence, generalise the results here.

1.3. Structure of this paper. We structure this paper as follows. After some notation in the next subsection, Section 2 contains the statements of our general theorems followed by two corollaries. In Section 3, we present Thue's original statement of his Fundamentaltheorem followed by our own simplified version. In Section 4, we establish the form of the polynomials to which Thue's Fundamentaltheorem applies. Section 5 contains information on the roots of these polynomials. Section 6 contains two diophantine lemmas. This is followed in Section 7 by some analytic results on the size of the numerators and denominators of the hypergeometric polynomials as well as bounds for the values of the polynomials. Section 8 contains the proof of Theorem 2.1, Section 9 contains the proof of Theorem 2.4; finally, we prove our two corollaries in Sections 10 and 11.

1.4. Notation. In order to state our results, we start with some notation.

For positive integers m and n with $(m, n) = 1$ and a non-negative integer r, we put

$$X_{m,n,r}(x) = {}_2F_1(-r, -r - m/n; 1 - m/n; x),$$

where ${}_2F_1$ denotes the classical hypergeometric function.

We use $X^*_{m,n,r}$ to denote the homogeneous polynomials derived from these polynomials, so that

$$X^*_{m,n,r}(x, y) = y^r X_{m,n,r}(x/y).$$

For Thue's Fundamentaltheorem itself, we will only use $X_{1,n,r}$, so for convenience we will write $X_{n,r}$ rather than $X_{1,n,r}$ in what follows.

We let $D_{m,n,r}$ be the smallest positive integer such that $D_{m,n,r}X_{m,n,r}(x)$ has rational integer coefficients (and again $D_{n,r}$ in place of $D_{1,n,r}$).

For a positive integer d, we define $N_{d,n,r}$ to be the greatest common divisor of the numerators of the coefficients of $X_{m,n,r}(1 - dx)$.

We will use $v_p(x)$ to denote the largest power of a prime p which divides into the rational number x. With this notation, for positive integers d and n, we put

$$\mathcal{N}_{d,n} = \prod_{p|n} p^{\min(v_p(d), v_p(n)+1/(p-1))}.$$

For any complex number w, we can write $w = se^{i\varphi}$, where $s \geq 0$ and $-\pi < \varphi \leq \pi$ (with $\varphi = 0$ if $s = 0$). With such a representation, unless otherwise stated, $w^{1/n}$ will signify $s^{1/n}e^{i\varphi/n}$ for a positive integer n, where $s^{1/n}$ is the unique non-negative nth root of s.

Lastly, following the function name in PARI, we define $\operatorname{core}(n)$ to be the unique square-free divisor, n_1, of n such that n/n_1 is a perfect square.

2. Results

THEOREM 2.1. *Let* $\mathbb{K}$ *be either* $\mathbb{Q}$ *or an imaginary quadratic field and let* β_1 *be an algebraic integer with* $[\mathbb{K}(\beta_1) : \mathbb{K}] \leq 2$.

If $\mathbb{K} = \mathbb{Q}$ *or* $\mathbb{K}(\beta_1) = \mathbb{K}$, *then let* $\tau = 1$, *else let* τ *be an algebraic integer in* $\mathbb{K}$ *such that* $\mathbb{K}(\beta_1) = \mathbb{K}(\sqrt{\tau})$.

If $\beta_1 \in \mathbb{K}$, *then let* $\beta_2, \gamma_1, \gamma_2 \in \mathbb{K}$ *with the* γ_i's *non-zero,* $\beta_2 \neq \beta_1$ *and* β_2 *an algebraic integer.*

If $[\mathbb{K}(\beta_1) : \mathbb{K}] = 2$, *then let* β_2 *be the algebraic conjugate of* β_1 *over* $\mathbb{K}$, $\gamma_1 \in \mathbb{K}(\beta_1)$ *and* γ_2 *be the algebraic conjugate of* γ_1 *over* $\mathbb{K}$ (*so* $\gamma_1 = \gamma_2$ *if they are elements of* $\mathbb{K}$).

For an algebraic integer $x \in \mathbb{K}$ *and a rational integer* $n \geq 3$, *put*

$$U(x) = -\gamma_2(x - \beta_2)^n, \quad Z(x) = \gamma_1(x - \beta_1)^n, \quad W(x) = \frac{Z(x)}{U(x)}$$

and

$$\mathcal{A}(x) = \frac{\beta_1(x - \beta_2)W(x)^{1/n} - \beta_2(x - \beta_1)}{(x - \beta_2)W(x)^{1/n} - (x - \beta_1)}.$$

Let g be an algebraic number such that $U(x)/g$ and $Z(x)/g$ are algebraic integers (not necessarily in $\mathbb{K}(\beta_1)$). For each non-negative integer r, let h_r be a non-zero algebraic integer with $h_r/g^r \in \mathbb{K}$ and $|h_r| \leq h$ for some fixed positive real number h.

Let d be the largest positive rational integer such that $(U(x) - Z(x))/(dg)$ is an algebraic integer and let $\mathcal{C}_n$ and $\mathcal{D}_n$ be positive real numbers such that

$$(2.1) \quad \max\left(1, \frac{\Gamma(1 - 1/n)r!}{\Gamma(r + 1 - 1/n)}, \frac{n\Gamma(r + 1 + 1/n)}{\Gamma(1/n)r!}\right)\frac{D_{n,r}}{N_{d,n,r}} < \mathcal{C}_n\left(\frac{\mathcal{D}_n}{\mathcal{N}_{d,n}}\right)^r$$

holds for all non-negative integers r.

Put

$$E = \frac{|g|\mathcal{N}_{d,n}}{\mathcal{D}_n}\{\min(|\sqrt{U(x)} - \sqrt{Z(x)}|, |\sqrt{U(x)} + \sqrt{Z(x)}|)\}^{-2},$$

$$Q = \frac{\mathcal{D}_n}{|g|\mathcal{N}_{d,n}}\{\max(|\sqrt{U(x)} - \sqrt{Z(x)}|, |\sqrt{U(x)} + \sqrt{Z(x)}|)\}^2,$$

$$\kappa = \frac{\log Q}{\log E},$$

$$c = 4h|\sqrt{\tau}|(|x - \beta_1| + |x - \beta_2|)\mathcal{C}_nQ$$
$$\times \max(1, 5h|\sqrt{\tau}| \, |1 - W(x)^{1/n}| \, |x - \beta_2| \, |\mathcal{A}(x) - \beta_1|\mathcal{C}_nE)^\kappa.$$

If $E > 1$ and either $0 < W(x) < 1$ or $|W(x)| = 1$ with $W(x) \neq -1$, then

$$(2.2) \qquad\qquad |\mathcal{A}(x) - p/q| > \frac{1}{c|q|^{\kappa+1}}$$

for all algebraic integers p and q in $\mathbb{K}$ with $q \neq 0$.

REMARK 2.2. As we will see in the proof of Corollary 2.7, the inclusion of the h_r's here can permit the use of a larger value of g and hence improved reduced values of κ.

REMARK 2.3. The inequality (2.1) does not impose any constraint, for, as we will demonstrate in Lemma 7.4, such an inequality always holds.

We can also obtain a similar, though slightly weaker, result for other values of $W(x)$ near 1. This allows us to extend and refine the results of Heuberger [14].

THEOREM 2.4. *Let $\mathbb{K}$ be an imaginary quadratic field and β_1, β_2, γ_1, γ_2, τ, x, n, $U(x)$, $Z(x)$, $W(x)$, $\mathcal{A}(x)$, d, g, h_r, h, $\mathcal{C}_n$, $\mathcal{D}_n$, $\mathcal{N}_{d,n}$ be as in Theorem 2.1. Put*

$$E = \frac{|g|\mathcal{N}_{d,n}}{\mathcal{D}_n} \frac{4(|U(x)| - |Z(x) - U(x)|)}{|Z(x) - U(x)|^2},$$

$$Q = \frac{\mathcal{D}_n}{|g|\mathcal{N}_{d,n}} 2(|U(x)| + |Z(x)|),$$

$$\kappa = \frac{\log Q}{\log E},$$

$$c = 4h|\sqrt{\tau}|(|x - \beta_1| + |x - \beta_2|)\mathcal{C}_n Q$$
$$\times \max(1, 2h|\sqrt{\tau}| \, |1 - W(x)^{1/n}| \, |x - \beta_2| \, |\mathcal{A}(x) - \beta_1|\mathcal{C}_n E)^{\kappa}.$$

If $E > 1$, $\max(|1 - W(x)|, |1 - 1/W(x)|) < 1$, then

$$(2.3) \qquad |\mathcal{A}(x) - p/q| > \frac{1}{c|q|^{\kappa+1}}$$

for all algebraic integers p and q in $\mathbb{K}$ with $q \neq 0$.

REMARK 2.5. The condition that $\mathbb{K}$ be an imaginary quadratic field is no restriction since the case of $\mathbb{K} = \mathbb{Q}$ is completely covered by Theorem 2.1.

We now give two corollaries of Theorem 2.1, showing how it contains, and extends, currently known results as well as providing new results. They cover all cases where $[\mathbb{K}(\beta_1) : \mathbb{Q}] \leq 2$.

In the first corollary, we establish effective irrationality measures for numbers of the form $z^{1/n}$. Together with Lemma 6.3, it also strengthens Theorem 2.1 in [32] and extends it to any algebraic number in an imaginary quadratic field which lies on the unit circle.

COROLLARY 2.6. *Let $\mathbb{K}$ be an imaginary quadratic field and $n \geq 3$ be a rational integer. Let a and b be algebraic integers in $\mathbb{K}$ with the ideal $(a, b) = \mathcal{O}_{\mathbb{K}}$ and either $a/b > 1$ a rational number or $|a/b| = 1$ with $a/b \neq -1$. Let d be the largest positive rational integer such that $(a - b)/d$ is an algebraic integer. Let $\mathcal{C}_n$, $\mathcal{D}_n$ and $\mathcal{N}_{d,n}$ be as in Theorem 2.1. Put*

$$E = \frac{\mathcal{N}_{d,n}}{\mathcal{D}_n} \{\min(|\sqrt{a} - \sqrt{b}|, |\sqrt{a} + \sqrt{b}|)\}^{-2},$$

$$Q = \frac{\mathcal{D}_n}{\mathcal{N}_{d,n}} \{\max(|\sqrt{a} - \sqrt{b}|, |\sqrt{a} + \sqrt{b}|)\}^2,$$

$$\kappa = \frac{\log Q}{\log E},$$

$$c = 4|a|\mathcal{C}_n Q \left(2.5 \left|\frac{a(a - b)}{b}\right| \mathcal{C}_n E\right)^{\kappa}.$$

If $E > 1$, then

$$(2.4) \qquad |(a/b)^{1/n} - p/q| > \frac{1}{c|q|^{\kappa+1}}$$

for all algebraic integers p and q in $\mathbb{K}$ with $q \neq 0$.

Our second corollary covers the cases when β_1 and β_2 lie in a quadratic extension of $\mathbb{Q}$. There is some overlap with Corollary 2.6, as we allow $\beta_1 \in \mathbb{Q}$ here, but the formulation here allows Corollary 2.7 to be readily applied to parametrised families of algebraic numbers.

COROLLARY 2.7. *Let n, t and x be rational integers with $n \geq 3$ and $t \neq 0$. Let $\beta_1 = a + b\sqrt{t}$ be an algebraic integer with $a, b \in \mathbb{Q}$ and $b \neq 0$ and let $\beta_2 = a - b\sqrt{t}$. Let γ_1 be an algebraic integer in $\mathbb{Q}(\sqrt{t})$ with γ_2 as its algebraic conjugate. We can write $U(x) = -\gamma_2(x - \beta_2)^n = (u_1 + u_2\sqrt{t})/2$ where $u_1, u_2 \in \mathbb{Z}$. Put*

$$g_1 = \gcd(u_1, u_2), \qquad g_2 = \gcd(u_1/g_1, t),$$

$$g_3 = \begin{cases} 1 & \text{if } t \equiv 1 \bmod 4 \text{ and } (u_1 - u_2)/g_1 \equiv 0 \bmod 2, \\ 2 & \text{if } t \equiv 3 \bmod 4 \text{ and } (u_1 - u_2)/g_1 \equiv 0 \bmod 2, \\ 4 & \text{otherwise,} \end{cases}$$

$$g_4 = \gcd\left(\operatorname{core}(g_2 g_3), \frac{\gcd(2, n)n}{\gcd(u_1/g_1, \gcd(2, n)n)}\right),$$

$$g = \frac{g_1\sqrt{g_2}}{\sqrt{g_3 g_4}},$$

$$E = \frac{|g|\mathcal{N}_{d,n}}{\mathcal{D}_n \min(|u_2\sqrt{t} \pm \sqrt{u_2^2 t - u_1^2}|)},$$

$$Q = \frac{\mathcal{D}_n \max(|u_2\sqrt{t} \pm \sqrt{u_2^2 t - u_1^2}|)}{|g|\mathcal{N}_{d,n}},$$

$$\kappa = \frac{\log Q}{\log E},$$

$$c = 4\sqrt{|2t|}(|x - \beta_1| + |x - \beta_2|)\mathcal{C}_n Q$$
$$\times (\max(1, 5\sqrt{|2t|}\,|1 - W(x)^{1/n}|\,|x - \beta_2|\,|\mathcal{A}(x) - \beta_1|\mathcal{C}_n E))^\kappa,$$

where d is the largest positive rational integer such that $u_1/(dg)$ is an algebraic integer and $\mathcal{A}(x)$, $\mathcal{C}_n$, $\mathcal{D}_n$, $\mathcal{N}_{d,n}$ and $W(x)$ are as in Theorem 2.1. If $E > 1$ and either $0 < W(x) < 1$ or $|W(x)| = 1$ with $W(x) \neq -1$, then

$$(2.5) \qquad |\mathcal{A}(x) - p/q| > \frac{1}{c|q|^{\kappa+1}}$$

for all rational integers p and q with $q \neq 0$.

REMARK 2.8. The factor g_4 here may appear wasteful as $(u/g_1)\sqrt{g_3/g_2}$ is already an algebraic integer. It arises from an interdependence between d and g here. The factor of $\sqrt{g_4}$ allows us to increase the size of d by a factor of g_4 and hence obtain a net benefit of $\sqrt{g_4}$. This can be important in practice (for example, filling the gap $1200 < t < 40\,000$ in [2]).

3. Thue's Fundamentaltheorem

LEMMA 3.1 (Thue [26]). *Let $F(x)$ be a polynomial of degree $n \geq 2$ and assume that there is a quadratic polynomial $G(x)$ with non-zero discriminant such that*

$$(3.1) \quad G(x) \frac{d^2}{dx^2}(F(x)) - (n-1) \frac{d}{dx}(G(x)) \frac{d}{dx}(F(x))$$
$$+ \frac{n(n-1)}{2} \frac{d^2}{dx^2}(G(x))F(x) = 0.$$

We write

$$Y(x) = 2G(x) \frac{d}{dx}(F(x)) - n \frac{d}{dx}(G(x))F(x),$$

$$h = \frac{n^2-1}{4}\left(\left(\frac{d}{dx}(G(x))\right)^2 - 2G(x)\frac{d^2}{dx^2}(G(x))\right),$$

$$\lambda = \frac{h}{n^2-1}.$$

Let us define two families of polynomials $P'_r(x)$ and $Q'_r(x)$ by the initial conditions

$$Q'_0(x) = \frac{2h}{3},$$

$$Q'_1(x) = \frac{2(n+1)}{3}\left(G(x)\frac{d}{dx}(F(x)) - \frac{n-1}{2}\frac{d}{dx}(G(x))F(x)\right),$$

$$P'_0(x) = \frac{2hx}{3},$$

$$P'_1(x) = xQ'_1(x) - \frac{2(n+1)G(x)F(x)}{3},$$

and, for $r \geq 1$, by the recurrence equations

$$\lambda(n(r+1)-1)Q'_{r+1}(x) = \left(r+\frac{1}{2}\right)Y(x)Q'_r(x) - (nr+1)F^2(x)Q'_{r-1}(x),$$

$$\lambda(n(r+1)-1)P'_{r+1}(x) = \left(r+\frac{1}{2}\right)Y(x)P'_r(x) - (nr+1)F^2(x)P'_{r-1}(x).$$

(a) *For any root α of $F(x)$,*

$$\alpha Q'_r(x) - P'_r(x) = S'_r(x),$$

where $S'_r(x)$ is a polynomial divisible by $(x-\alpha)^{2r+1}$.

(b) *Put*

$$Z(x) = \frac{1}{2}\left(\frac{Y(x)}{2n\sqrt{\lambda}} + F(x)\right) \quad and \quad U(x) = \frac{1}{2}\left(\frac{Y(x)}{2n\sqrt{\lambda}} - F(x)\right).$$

Then

$$(\sqrt{\lambda})^r Q_r'(x) = A(x) X_{n,r}^*(Z(x), U(x)) - B(x) X_{n,r}^*(U(x), Z(x)),$$

$$(\sqrt{\lambda})^r P_r'(x) = C(x) X_{n,r}^*(Z(x), U(x)) - D(x) X_{n,r}^*(U(x), Z(x)),$$

where

$$A(x) = \left(\frac{(n-1)\sqrt{\lambda}}{2F(x)}\right) Q_1'(x) - \left(\frac{Y(x)}{4\sqrt{\lambda}\,F(x)} - \frac{1}{2}\right) Q_0'(x),$$

$$B(x) = \left(\frac{(n-1)\sqrt{\lambda}}{2F(x)}\right) Q_1'(x) - \left(\frac{Y(x)}{4\sqrt{\lambda}\,F(x)} + \frac{1}{2}\right) Q_0'(x),$$

$$C(x) = \left(\frac{(n-1)\sqrt{\lambda}}{2F(x)}\right) P_1'(x) - \left(\frac{Y(x)}{4\sqrt{\lambda}\,F(x)} - \frac{1}{2}\right) P_0'(x),$$

$$D(x) = \left(\frac{(n-1)\sqrt{\lambda}}{2F(x)}\right) P_1'(x) - \left(\frac{Y(x)}{4\sqrt{\lambda}\,F(x)} + \frac{1}{2}\right) P_0'(x).$$

These results can be found in Thue [26, Theorem and equations (35)–(47)] or Chudnovsky [13] (see, in particular, Lemma 7.1 and the remarks that follow (pages 364–366)).

We have added two extra hypotheses, requiring that the degree of $F(x)$ be at least two and that the discriminant of $G(x)$ be non-zero. If $n = 1$, then $h = n - 1 = 0$, with the result that $A(x) = B(x) = C(x) = D(x) = 0$ and the relationship between the $P_r'(x)$'s and $Q_r'(x)$'s and the hypergeometric functions fails. When the discriminant of $G(x)$ is zero, the recurrence relationship for the $P_r'(x)$'s and $Q_r'(x)$'s does not hold.

Also notice that there are some differences in notation between the lemma above, which is similar to Chudnovsky's [13], and that of Thue. In particular, here,

- Thue's U is replaced by G here,
- our n and r are switched from [26],
- our $P_r'(x)$ is $2(r-1)B_n(x)/3$ and our $Q_r'(x)$ is $2(r-1)A_n(x)/3$ in Thue's notation (we use the superscript as we will simplify these polynomials further in what follows),
- we capitalise Thue's a, b, c, d, and z,
- what we call $Y(x)$ and $U(x)$, correspond to $2H(x)$ and $y(x)$ respectively in Thue's paper,
- we label Thue's $U_n(z, y)$ as $X_{n,r}^*(Z(x), U(x))$.

However, this lemma can be simplified considerably and that is the objective of this section.

We start with a result regarding the differential equation in (3.1).

LEMMA 3.2. *Let m and n be positive integers with $n \geq m$ and let $\beta_1, \ldots, \beta_m$ be distinct complex numbers. Put $G(x) = (x - \beta_1) \cdots (x - \beta_m)$. An analytic function $F(x)$ is a solution of the differential equation*

$$(3.2) \qquad \sum_{i=0}^{m} (-1)^i \binom{n - m + i}{i} \frac{d^i}{dx^i}(G(x)) \frac{d^{m-i}}{dx^{m-i}}(F(x)) = 0$$

if and only if it is of the form

$$F(x) = \sum_{i=1}^{m} \gamma_i (x - \beta_i)^n$$

for some choice of $\gamma_1, \ldots, \gamma_m \in \mathbb{C}$.

Proof. Note that (3.2) is a homogeneous linear differential equation of order m. The theory of these equations is well-understood (see, for example, Chapter 4 of [10]).

By Theorem 4.1.2 of [10], given m linearly independent solutions $(F_1(x), \ldots, F_m(x))$ of the differential equation, then any solution is given by $\gamma_1 F_1(x) + \cdots + \gamma_m F_m(x)$ for some constants $\gamma_1, \ldots, \gamma_m$. Here we show that $F_1(x) = (x - \beta_1)^n, \ldots, F_m(x) = (x - \beta_m)^n$ are such linearly independent solutions.

Putting $F(x) = F_j(x)$, we get

$$\frac{d^{m-i}}{dx^{m-i}}(F(x)) = \frac{n!}{(n - (m - i))!} (x - \beta_j)^{n-(m-i)},$$

so we can write (3.2) as

$$\sum_{i=0}^{m} (-1)^i \binom{n - m + i}{i} \frac{d^i}{dx^i}(G(x)) \frac{n!}{(n - (m - i))!} (x - \beta_j)^{n-(m-i)}$$

$$= \frac{n!}{(n - m)!} (x - \beta_j)^{n-m} \sum_{i=0}^{m} \frac{(-1)^i}{i!} \frac{d^i}{dx^i}(G(x))(x - \beta_j)^i.$$

Note that the sum in the last expression is in fact the Taylor series expansion of $G(\beta_j) = 0$, since $\deg G(x) = m$. Therefore, the entire expression is 0. Hence $(x - \beta_j)^n$ satisfies the required differential equation for each $j = 1, \ldots, m$ and it only remains to show that these m solutions are linearly independent.

This is equivalent to showing that their Wronskian is not always zero. We can write this Wronskian as

$$\det \begin{pmatrix} (x-\beta_1)^n & \cdots & (x-\beta_m)^n \\ n(x-\beta_1)^{n-1} & \cdots & n(x-\beta_m)^{n-1} \\ & \cdots & \\ \dfrac{n!(x-\beta_1)^{n-(m-1)}}{(n-m+1)!} & \cdots & \dfrac{n!(x-\beta_m)^{n-(m-1)}}{(n-m+1)!} \end{pmatrix}$$

$$= \left(\prod_{i=1}^m \frac{n!(x-\beta_i)^{n-(m-1)}}{(n-i+1)!} \right) \det \begin{pmatrix} (x-\beta_1)^{m-1} & \cdots & (x-\beta_m)^{m-1} \\ (x-\beta_1)^{m-2} & \cdots & (x-\beta_m)^{m-2} \\ & \cdots & \\ 1 & \cdots & 1 \end{pmatrix}$$

$$= \left(\prod_{i=1}^m \frac{n!(x-\beta_i)^{n-(m-1)}}{(n-i+1)!} \right) \prod_{1 \le i < j \le m} ((x-\beta_i) - (x-\beta_j)).$$

This function is identically zero only if the β_i's are not all distinct, a condition which we exclude here. ∎

We now present our simplified version of Lemma 3.1.

LEMMA 3.3. *Let* β_1, β_2, γ_1 *and* γ_2 *be complex numbers with* $\beta_1 \ne \beta_2$. *For any integer* $n \ge 2$, *we put*

$$U(x) = -\gamma_2(x-\beta_2)^n \quad and \quad Z(x) = \gamma_1(x-\beta_1)^n.$$

For all non-negative integers r, *we define*

$$Q_r(x) = (x-\beta_2)X_{n,r}^*(Z(x), U(x)) - (x-\beta_1)X_{n,r}^*(U(x), Z(x)),$$
$$P_r(x) = \beta_1(x-\beta_2)X_{n,r}^*(Z(x), U(x)) - \beta_2(x-\beta_1)X_{n,r}^*(U(x), Z(x)).$$

For any root, α, *of*

$$F(x) = \gamma_1(x-\beta_1)^n + \gamma_2(x-\beta_2)^n,$$

the polynomial

$$S_r(x) = \alpha Q_r(x) - P_r(x)$$

is divisible by $(x-\alpha)^{2r+1}$.

Proof. First note that we may assume that $G(x)$ is monic since wherever $G(x)$ is used in Lemma 3.1, the leading coefficient can be eliminated. Therefore, we can write $G(x) = (x-\beta_1)(x-\beta_2)$.

Applying Lemma 3.2 with $m = 2$, we see that a polynomial $F(x)$ satisfies the differential equation in (3.1) if and only if it is of the form above.

Also $h = (n^2 - 1)(\beta_1 - \beta_2)^2/4$ and $\lambda = (\beta_1 - \beta_2)^2/4$.

Next, we need to calculate Thue's $Y(x)$:

$$Y(x) = 2G(x)\frac{d}{dx}(F(x)) - n\frac{d}{dx}(G(x))F(x)$$
$$= 2(x-\beta_1)(x-\beta_2)(\gamma_1 n(x-\beta_1)^{n-1} + \gamma_2 n(x-\beta_2)^{n-1})$$
$$-n(2x-(\beta_1+\beta_2))(\gamma_1(x-\beta_1)^n + \gamma_2(x-\beta_2)^n)$$
$$= n(\beta_1-\beta_2)(\gamma_1(x-\beta_1)^n - \gamma_2(x-\beta_2)^n)$$
$$= 2n\sqrt{\lambda}\,(\gamma_1(x-\beta_1)^n - \gamma_2(x-\beta_2)^n).$$

Thus

$$Z(x) = \frac{1}{2}\left(\frac{Y(x)}{2n\sqrt{\lambda}} + F(x)\right)$$
$$= \frac{1}{2}\left(\gamma_1(x-\beta_1)^n - \gamma_2(x-\beta_2)^n + \gamma_1(x-\beta_1)^n + \gamma_2(x-\beta_2)^n\right)$$
$$= \gamma_1(x-\beta_1)^n.$$

Similarly, we find that $U(x) = -\gamma_2(x-\beta_2)^n$.

Now we determine the expressions for $A(x)$, $B(x)$, $C(x)$ and $D(x)$:

$$A(x) = \frac{2(n-1)\lambda Q_1(x) - Y(x)Q_0(x) + 2\sqrt{\lambda}\,F(x)Q_0(x)}{4\sqrt{\lambda}\,F(x)}$$
$$= \frac{h}{6\sqrt{\lambda}\,F(x)}\left(2G(x)\frac{d}{dx}(F(x))\right.$$
$$\left. -(n-1)\frac{d}{dx}(G(x))F(x) - Y(x) + 2\sqrt{\lambda}\,F(x)\right)$$
$$= \frac{h}{6\sqrt{\lambda}\,F(x)}\left(\frac{d}{dx}(G(x))F(x) + 2\sqrt{\lambda}\,F(x)\right)$$
$$= \frac{(n^2-1)\sqrt{\lambda}}{6}\left(\frac{d}{dx}(G(x)) + 2\sqrt{\lambda}\right)$$
$$= \frac{n^2-1}{6}(\beta_1-\beta_2)(x-\beta_2).$$

A similar argument establishes that

$$B(x) = \frac{n^2-1}{6}(\beta_1-\beta_2)(x-\beta_1),$$

as well as the relationships $C(x) = \beta_1 A(x)$ and $D(x) = \beta_2 B(x)$.

Therefore,

$$(\sqrt{\lambda})^r Q_r'(x) = A(x)X_{n,r}^*(Z(x),U(x)) - B(x)X_{n,r}^*(U(x),Z(x))$$
$$= \frac{n^2-1}{6}(\beta_1-\beta_2)$$
$$\times\{(x-\beta_2)X_{n,r}^*(Z(x),U(x)) - (x-\beta_1)X_{n,r}^*(U(x),Z(x))\}$$

and

$$(\sqrt{\lambda})^r P_r'(x) = C(x) X_{n,r}^*(Z(x), U(x)) - D(x) X_{n,r}^*(U(x), Z(x))$$

$$= \frac{n^2 - 1}{6} (\beta_1 - \beta_2)$$

$$\times \{\beta_1(x - \beta_2) X_{n,r}^*(Z(x), U(x)) - \beta_2(x - \beta_1) X_{n,r}^*(U(x), Z(x))\}.$$

We now set $P_r(x)$, $Q_r(x)$ and $S_r(x)$ to be $6/((n^2 - 1)(\beta_1 - \beta_2))$ times $(\sqrt{\lambda})^r P_r'(x)$, $(\sqrt{\lambda})^r Q_r'(x)$ and $(\sqrt{\lambda})^r S_r'(x)$, respectively.

From the statement of Thue's Fundamentaltheorem (Lemma 3.1(a)), for any root α of $F(x)$,

$$\alpha Q_r(x) - P_r(x) = S_r(x),$$

where $S_r(x)$ is a polynomial divisible by $(x - \alpha)^{2r+1}$. ∎

4. The form of the polynomials

LEMMA 4.1. *Let β_1, β_2, γ_1 and γ_2 be complex numbers with $\beta_1 \neq \beta_2$ and let n be an integer with $n \geq 3$. For any number field $\mathbb{K}$, we have*

$$0 \neq F(x) = \gamma_1(x - \beta_1)^n + \gamma_2(x - \beta_2)^n \in \mathbb{K}[x]$$

if and only if either

(a) *one of the γ_i's is zero (say γ_1), β_1 is any complex number, γ_2 is a non-zero element of $\mathbb{K}$ and β_2 is element of $\mathbb{K}$ other than β_1,*

(b) *$\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{K}$, or*

(c) *$[\mathbb{K}(\beta_1) : \mathbb{K}] = 2$ and β_2 is the algebraic conjugate of β_1 over $\mathbb{K}$, $\gamma_1 \in \mathbb{K}(\beta_1)$ and γ_2 is the algebraic conjugate of γ_1 over $\mathbb{K}$ (so $\gamma_1 = \gamma_2$ if they are elements of $\mathbb{K}$).*

REMARK 4.2. The condition $n \geq 3$ here is necessary. If $\beta_1 = \pi$, $\beta_2 = -1/\pi$, $\gamma_1 = 1/(\pi^2 + 1)$ and $\gamma_2 = \pi^2/(\pi^2 + 1)$ with $n = 2$, then $F(x) = x^2 + 1$. Here we have transcendental values for β_1, β_2, γ_1 and γ_2, yet $F(x) \in \mathbb{Q}[x]$.

Proof of Lemma 4.1. We will consider the four highest-order coefficients of $F(x)$:

(4.1)
$$\gamma_1 + \gamma_2 = a_1 \in \mathbb{K},$$
$$\gamma_1 \beta_1 + \gamma_2 \beta_2 = a_2 \in \mathbb{K},$$
$$\gamma_1 \beta_1^2 + \gamma_2 \beta_2^2 = a_3 \in \mathbb{K},$$
$$\gamma_1 \beta_1^3 + \gamma_2 \beta_2^3 = a_4 \in \mathbb{K}.$$

Using these expressions, we find that

$$\frac{a_3^2 - a_2 a_3 \beta_2 + (a_2^2 - a_1 a_3)\beta_2^2}{a_2 - a_1 \beta_2} = \frac{\beta_1^4 \gamma_1^2 - \beta_1^3 \beta_2 \gamma_1^2 + \beta_1 \beta_2^3 \gamma_1 \gamma_2 - \beta_2^4 \gamma_1 \gamma_2}{\gamma_1(\beta_1 - \beta_2)}$$

$$= \gamma_1 \beta_1^3 + \gamma_2 \beta_2^3.$$

If $a_2 - a_1\beta_2 = \gamma_1(\beta_1 - \beta_2) = 0$, then $\gamma_1 = 0$ (since we assumed $\beta_1 \neq \beta_2$). From the expression for our polynomial, this implies that β_1 can be any complex number and that γ_2 must be an element of $\mathbb{K}$. If $\gamma_2 = 0$, then β_2 can be any complex number ($\neq \beta_1$). And if $\gamma_2 \neq 0$, then β_2 must be an element of $\mathbb{K}$ (again, $\neq \beta_1$).

These cases constitute part (a) of the lemma, along with the assumption that $F(x) \neq 0$, so we can assume $a_2 - a_1\beta_2 \neq 0$ in the remainder of the proof.

From the first and last terms of the above relationship, we obtain a polynomial, $f(x)$, such that $f(\beta_2) = 0$. Namely,

$$(4.2) \qquad f(\beta_2) = (a_2^2 - a_1a_3)\beta_2^2 + (a_1a_4 - a_2a_3)\beta_2 + (a_3^2 - a_2a_4) = 0.$$

Therefore, β_2 is an algebraic number of degree at most 2 over $\mathbb{K}$.

From the expression in (4.1) for the a_i's, we find that

$$(4.3) \qquad \gamma_1 = \frac{a_2 - a_1\beta_2}{\beta_1 - \beta_2},$$

$$(4.4) \qquad \gamma_2 = \frac{a_1(\beta_1 - \beta_2) - (a_2 - a_1\beta_2)}{\beta_1 - \beta_2} = \frac{a_1\beta_1 - a_2}{\beta_1 - \beta_2},$$

$$(4.5) \qquad \beta_1 = \frac{a_3 - a_2\beta_2}{a_2 - a_1\beta_2}.$$

Let us consider the case of $\beta_2 \in \mathbb{K}$. From the expressions above, we see that $\beta_1, \gamma_1, \gamma_2 \in \mathbb{K}$. Hence we find ourselves in case (b).

Therefore, in what follows, we assume that $\beta_2 \notin \mathbb{K}$.

We now show that β_1 is the algebraic conjugate of β_2. To demonstrate this, we substitute the expression for β_1 in (4.5) into the polynomial $f(x)$. We find that

$$(a_2 - a_1\beta_2)^2 f(\beta_1)$$
$$= (a_2^2 - a_1a_3)(a_3 - a_2\beta_2)^2 + (a_1a_4 - a_2a_3)(a_3 - a_2\beta_2)(a_2 - a_1\beta_2)$$
$$\quad + (a_3^2 - a_2a_4)(a_2 - a_1\beta_2)^2$$
$$= (a_2^2 - a_1a_3)(a_3 - a_2\beta_2)^2 + (a_2 - a_1\beta_2)(a_1a_3a_4 - a_2^2a_4 + a_2^2a_3\beta_2 - a_1a_3^2\beta_2)$$
$$= (a_2^2 - a_1a_3)((a_3 - a_2\beta_2)^2 - (a_2 - a_1\beta_2)(a_4 - a_3\beta_2))$$
$$= (a_2^2 - a_1a_3)f(\beta_2) = 0.$$

Therefore β_1 is the algebraic conjugate of β_2. Hence, from (4.3), the algebraic conjugate of γ_1 is $(a_2 - a_1\beta_1)/(\beta_2 - \beta_1) = \gamma_2$, as required. ∎

REMARK 4.3. From a diophantine point of view, there is no interest in the cases of $\gamma_1 = 0$ or $\gamma_2 = 0$ (that is, part (a) of this lemma), since the resulting polynomial is a power of $x - \beta_2$, where $\beta_2 \in \mathbb{K}$. So in the following we shall not consider this case any further.

REMARK 4.4. This proof is quite detailed, but it does provide an explicit means to easily test if a given polynomial $F(x)$, of degree n, is of the required form.

Let A be the lead coefficient of $F(x)$, B be the coefficient of $F(x)$ of degree $n-1$, C be the coefficient of $F(x)$ of degree $n-2$ and D be the coefficient of $F(x)$ of degree $n-3$.

Set $a_1 = A$, $a_2 = -B/n$, $a_3 = C/\binom{n}{2}$ and $a_4 = -D/\binom{n}{3}$. Find β_1 and β_2 as the roots of $f(x)$ in (4.2) and then find γ_1 and γ_2 from (4.3) and (4.4).

5. Roots of these polynomials. We start with the following lemma describing the roots themselves.

LEMMA 5.1. *Let $n, \beta_1, \beta_2, \gamma_1, \gamma_2$ and $F(x)$ be as above. Then*

$$\alpha = \frac{\beta_1(-\gamma_1/\gamma_2)^{1/n} - \beta_2}{(-\gamma_1/\gamma_2)^{1/n} - 1}$$

is a root of $F(x)$ for each nth root of $-\gamma_1/\gamma_2$, except 1 in the case of $\gamma_1 = -\gamma_2$. Furthermore, for any two distinct nth roots of $-\gamma_1/\gamma_2$ (again excluding 1 in the case of $\gamma_1 = -\gamma_2$), the corresponding α's are distinct.

Proof. We start by substituting the above expression for α into $F(x)$:

$$F(\alpha) = \gamma_1 \left(\frac{\beta_1(-\gamma_1/\gamma_2)^{1/n} - \beta_2}{(-\gamma_1/\gamma_2)^{1/n} - 1} - \beta_1 \right)^n + \gamma_2 \left(\frac{\beta_1(-\gamma_1/\gamma_2)^{1/n} - \beta_2}{(-\gamma_1/\gamma_2)^{1/n} - 1} - \beta_2 \right)^n$$

$$= \gamma_1 \left(\frac{\beta_1 - \beta_2}{(-\gamma_1/\gamma_2)^{1/n} - 1} \right)^n + \gamma_2 \left(\frac{(\beta_1 - \beta_2)(-\gamma_1/\gamma_2)^{1/n}}{(-\gamma_1/\gamma_2)^{1/n} - 1} \right)^n$$

$$= \frac{(\beta_1 - \beta_2)^n (\gamma_1 + \gamma_2(-\gamma_1/\gamma_2))}{((-\gamma_1/\gamma_2)^{1/n} - 1)^n} = 0.$$

Next, we consider when two of these α's are equal. Let $(-\gamma_1/\gamma_2)^{1/n}$ be a fixed nth root of $-\gamma_1/\gamma_2$. Suppose that

$$\frac{\beta_1(-\gamma_1/\gamma_2)^{1/n} - \beta_2}{(-\gamma_1/\gamma_2)^{1/n} - 1} = \frac{\beta_1 \zeta_n^k (-\gamma_1/\gamma_2)^{1/n} - \beta_2}{\zeta_n^k (-\gamma_1/\gamma_2)^{1/n} - 1}$$

for some $\zeta_n^k = \exp(2\pi i k/n)$. Then

$$\beta_1 \zeta_n^k (-\gamma_1/\gamma_2)^{2/n} - \beta_1 (-\gamma_1/\gamma_2)^{1/n} - \beta_2 \zeta_n^k (-\gamma_1/\gamma_2)^{1/n} + \beta_2$$
$$= \beta_1 \zeta_n^k (-\gamma_1/\gamma_2)^{2/n} - \beta_2 (-\gamma_1/\gamma_2)^{1/n} - \beta_1 \zeta_n^k (-\gamma_1/\gamma_2)^{1/n} + \beta_2.$$

So

$$(\beta_1 - \beta_2) \zeta_n^k (-\gamma_1/\gamma_2)^{1/n} = (\beta_1 - \beta_2)(-\gamma_1/\gamma_2)^{1/n}.$$

This implies that either $\beta_1 = \beta_2$ (a condition which we exclude), $\gamma_1 = 0$ and $\gamma_2 \neq 0$ (which we have again excluded, see Remark 4.3) or $\zeta_n^k = 1$, which is to say that the two α's are equal. ∎

In the following lemma, we determine when the roots of the polynomials are real for polynomials with rational coefficients.

LEMMA 5.2. *Let $n, \beta_1, \beta_2, \gamma_1, \gamma_2$ and $F(x)$ be as above.*

(a) *If $\mathbb{K} = \mathbb{Q}$ and $\mathbb{K}(\beta_1)$ is an imaginary quadratic field, then $F(x)$ has n real roots.*

(b) *Suppose that $\mathbb{K} = \mathbb{Q}$ and $\mathbb{K}(\beta_1)$ is contained in a real quadratic field and write $\beta_1 = a + b\sqrt{t}$ with $a, b \in \mathbb{Q}$.*

If $-\gamma_1/\gamma_2 > 0$, then $F(x)$ has two real roots for n even and one real root for n odd. These roots are

$$(5.1) \qquad \alpha_1 = a + b\sqrt{t}\,\frac{(-\gamma_1/\gamma_2)^{1/n} + 1}{(-\gamma_1/\gamma_2)^{1/n} - 1}$$

and, for n even,

$$(5.2) \qquad \alpha_2 = a + \frac{tb^2}{\alpha_1 - a} = a + b\sqrt{t}\,\frac{(-\gamma_1/\gamma_2)^{1/n} - 1}{(-\gamma_1/\gamma_2)^{1/n} + 1},$$

where $(-\gamma_1/\gamma_2)^{1/n}$ denotes the unique positive real nth root of $-\gamma_1/\gamma_2$.

If $-\gamma_1/\gamma_2 < 0$, then $F(x)$ has no real roots for n even and one real root, α_1 above, for n odd, where $(-\gamma_1/\gamma_2)^{1/n}$ denotes the unique negative real nth root of $-\gamma_1/\gamma_2$.

Proof. When $\mathbb{K}(\beta_1) = \mathbb{Q}$, the result is well-known, so we restrict our attention to the case of $[\mathbb{K}(\beta_1) : \mathbb{Q}] = 2$. In this case, we can write $\beta_1 = a + b\sqrt{t}$ and $\beta_2 = a - b\sqrt{t}$, where $a, b \in \mathbb{Q}$.

(a) From Lemma 5.1, we know that as j runs through the integers from 0 to $n - 1$,

$$\frac{\beta_1 e^{2\pi i j/n}(-\gamma_1/\gamma_2)^{1/n} - \beta_2}{e^{2\pi i j/n}(-\gamma_1/\gamma_2)^{1/n} - 1}$$

runs through the roots, where $(-\gamma_1/\gamma_2)^{1/n}$ denotes a fixed root of $-\gamma_1/\gamma_2$.

Multiplying the numerator and denominator by the complex conjugate of the denominator and substituting the expressions for β_1, β_2 and $e^{2\pi i j/n}$, we find that the roots are of the form

$a + b\sqrt{t}$
$$\times \frac{|(-\gamma_1/\gamma_2)^{1/n}|^2 - 1 - 2i\{\sin(2\pi j/n)\Re((-\gamma_1/\gamma_2)^{1/n}) + \cos(2\pi j/n)\Im((-\gamma_1/\gamma_2)^{1/n})\}}{|(-\gamma_1/\gamma_2)^{1/n}|^2 + 1 + 2\sin(2\pi j/n)\Im((-\gamma_1/\gamma_2)^{1/n}) - 2\cos(2\pi j/n)\Re((-\gamma_1/\gamma_2)^{1/n})}.$$

If $t < 0$, then γ_1 and γ_2 are also complex conjugates, and $|(-\gamma_1/\gamma_2)^{1/n}|^2 = 1$, so the roots are of the form

$$a + b\sqrt{-t}\,\frac{\sin(2\pi j/n)\Re((-\gamma_1/\gamma_2)^{1/n}) + \cos(2\pi j/n)\Im((-\gamma_1/\gamma_2)^{1/n})}{1 + \sin(2\pi j/n)\Im((-\gamma_1/\gamma_2)^{1/n}) - \cos(2\pi j/n)\Re((-\gamma_1/\gamma_2)^{1/n})}.$$

So all the roots are real numbers.

(b) Now suppose that $t > 0$ and $-\gamma_1/\gamma_2 > 0$. Then $\Re((-\gamma_1/\gamma_2)^{1/n}) = (-\gamma_1/\gamma_2)^{1/n}$ and $\Im((-\gamma_1/\gamma_2)^{1/n}) = 0$, so we can write the roots as

$$a + b\sqrt{t}\,\frac{(-\gamma_1/\gamma_2)^{2/n} - 1 - 2i\sin(2\pi j/n)(-\gamma_1/\gamma_2)^{1/n}}{(-\gamma_1/\gamma_2)^{2/n} + 1 - 2\cos(2\pi j/n)(-\gamma_1/\gamma_2)^{1/n}}.$$

These roots are real if and only if their imaginary part is zero, which only happens if $2j$ is a multiple of n (i.e., $j = 0$ or $j = n/2$). Hence, there are precisely two real roots when n is even and precisely one real root when n is odd.

These roots are

$$a + \frac{b\sqrt{t}\,((-\gamma_1/\gamma_2)^{2/n} - 1)}{(-\gamma_1/\gamma_2)^{2/n} - 2(-\gamma_1/\gamma_2)^{1/n} + 1} = a + \frac{b\sqrt{t}\,((-\gamma_1/\gamma_2)^{2/n} - 1)}{((-\gamma_1/\gamma_2)^{1/n} - 1)^2}$$

$$= a + \frac{b\sqrt{t}\,((-\gamma_1/\gamma_2)^{1/n} + 1)}{(-\gamma_1/\gamma_2)^{1/n} - 1},$$

and similarly for n even,

$$a + \frac{b\sqrt{t}\,((-\gamma_1/\gamma_2)^{2/n} - 1)}{(-\gamma_1/\gamma_2)^{2/n} + 2(-\gamma_1/\gamma_2)^{1/n} + 1} = a + \frac{b\sqrt{t}\,((-\gamma_1/\gamma_2)^{1/n} - 1)}{(-\gamma_1/\gamma_2)^{1/n} + 1}.$$

If $-\gamma_1/\gamma_2 < 0$ and n is odd, then we let $(-\gamma_1/\gamma_2)^{1/n}$ denote the unique negative real nth root of $-\gamma_1/\gamma_2$ and by the same argument as above, there is one real root of $F(x)$ and it is of the form

$$a + \frac{b\sqrt{t}\,((-\gamma_1/\gamma_2)^{2/n} - 1)}{(-\gamma_1/\gamma_2)^{2/n} - 2(-\gamma_1/\gamma_2)^{1/n} + 1} = a + \frac{b\sqrt{t}\,((-\gamma_1/\gamma_2)^{1/n} + 1)}{((-\gamma_1/\gamma_2)^{1/n} - 1)}.$$

If $-\gamma_1/\gamma_2 < 0$ and n is even, then the roots are as above and can be real only if

$$(5.3) \qquad \sin(2\pi j/n)\Re((-\gamma_1/\gamma_2)^{1/n}) + \cos(2\pi j/n)\Im((-\gamma_1/\gamma_2)^{1/n})$$

is zero. For $n > 2$, both the real and imaginary parts of $(-\gamma_1/\gamma_2)^{1/n}$ are nonzero, which means that for (5.3) to be zero, both $\cos(2\pi j/n)$ and $\sin(2\pi j/n)$ must be 0. This is impossible, hence there are no real roots in this case. ∎

LEMMA 5.3. *Let $\mathcal{A}(x)$ and $W(x)$ be as in Theorem 2.1 and let $F(x)$ be as above. For any $x \in \mathbb{C}$ such that $W(x)$ is not a negative real number or zero, $F(\mathcal{A}(x)) = 0$.*

Furthermore, for each root, α, of $F(x)$, we can find a value of x such that $\mathcal{A}(x) = \alpha$ (in particular, $\mathcal{A}(\alpha) = \alpha$).

Proof. We can write $W(x)^{1/n}$ as $e^{2\pi i k/n}(x - \beta_1)(-\gamma_1/\gamma_2)^{1/n}/(x - \beta_2)$ for some integer k. Hence

$$\mathcal{A}(x) = \frac{e^{2\pi i k/n}\beta_1(-\gamma_1/\gamma_2)^{1/n} - \beta_2}{e^{2\pi i k/n}(-\gamma_1/\gamma_2)^{1/n} - 1}.$$

By Lemma 5.1, this quantity is a root of $F(x)$.

To show that $\mathcal{A}(\alpha) = \alpha$, observe that since α is a root of $F(x)$, we have $\gamma_1(\alpha - \beta_1)^n + \gamma_2(\alpha - \beta_2)^n = 0$ and hence

$$W(\alpha) = -\frac{\gamma_1(\alpha - \beta_1)^n}{\gamma_2(\alpha - \beta_2)^n} = 1.$$

Therefore, by our choice of nth root,

$$\mathcal{A}(\alpha) = \frac{\beta_1(\alpha-\beta_2)W(\alpha)^{1/n}-\beta_2(\alpha-\beta_1)}{(\alpha-\beta_2)W(\alpha)^{1/n}-(\alpha-\beta_1)} = \frac{\beta_1(\alpha-\beta_2)-\beta_2(\alpha-\beta_1)}{(\alpha-\beta_2)-(\alpha-\beta_1)} = \alpha. \; \blacksquare$$

6. Diophantine lemmas. The following lemma is used to obtain an effective approximation measure for a complex number θ from a sequence of "good" approximations in an imaginary quadratic field.

LEMMA 6.1. *Let $\theta \in \mathbb{C}$ and let $\mathbb{K}$ be either $\mathbb{Q}$ or an imaginary quadratic field. Suppose that for all non-negative integers r, there are algebraic integers p_r and q_r in $\mathbb{K}$ satisfying $p_r q_{r+1} \neq p_{r+1} q_r$ with $|q_r| < k_0 Q^r$ and $|q_r \theta - p_r| \leq \ell_0 E^{-r}$, for some real numbers $k_0, \ell_0 > 0$ and $E, Q > 1$. Then for any algebraic integers p and q in $\mathbb{K}$ with $|q| \geq 1/(2\ell_0)$, we have*

$$\left| \theta - \frac{p}{q} \right| > \frac{1}{c|q|^{\kappa+1}}, \quad \text{where} \quad c = 2k_0 Q(2\ell_0 E)^\kappa \quad \text{and} \quad \kappa = \frac{\log Q}{\log E}.$$

REMARK 6.2. This is a generalisation of Lemma 2.8 in [12] to quadratic imaginary fields.

Proof of Lemma 6.1. Let p, q be algebraic integers in $\mathbb{K}$ with $|q| \geq 1/(2\ell_0) > 0$. Choose

$$n_0 = \left\lfloor \frac{\log(2\ell_0 |q|)}{\log E} \right\rfloor + 1.$$

Since $E > 1$ and $2\ell_0 |q| \geq 1$, we have $n_0 \geq 1$.

It also follows that $\log(2\ell_0 |q|)/\log E < n_0$ and hence for all $n \geq n_0$,

(6.1) $$\ell_0 E^{-n} < \ell_0 E^{-\log(2\ell_0|q|)/\log E} = 1/(2|q|) < 1.$$

If we have $q_n = 0$ for some $n \geq n_0$, then from (6.1), $|p_n| = |q_n\theta - p_n| < 1$, which implies that $p_n = 0$, since all non-zero algebraic integers in these fields are of absolute value at least 1. This contradicts the supposition that $p_n q_{n+1} \neq p_{n+1} q_n$. Therefore, $q_n \neq 0$ for all $n \geq n_0$.

So, for any $n \geq n_0$ with $p/q \neq p_n/q_n$, we have

$$\left| \theta - \frac{p}{q} \right| \geq \left| \frac{p_n}{q_n} - \frac{p}{q} \right| - \left| \theta - \frac{p_n}{q_n} \right| \geq \frac{1}{|qq_n|} - \frac{\ell_0}{E^n|q_n|} > \frac{1}{2|qq_n|},$$

again using (6.1) and the fact that $p_n q - q_n p$ is a non-zero algebraic integer and hence of absolute value at least 1 in such fields.

The choice of n_0 yields

$$Q^{n_0} \leq \exp\left(\frac{\log(2\ell_0|q|) + \log E}{\log E} \log Q\right) = (2E\ell_0|q|)^\kappa.$$

If $p/q \neq p_{n_0}/q_{n_0}$, then

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{2|qq_{n_0}|} \geq \frac{1}{2|q|k_0 Q^{n_0}} \geq \frac{1}{2k_0(2E\ell_0)^\kappa |q|^{\kappa+1}}.$$

If $p/q = p_{n_0}/q_{n_0}$, then $p/q \neq p_{n_0+1}/q_{n_0+1}$ and we obtain

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{2|qq_{n_0+1}|} \geq \frac{1}{2|q|k_0 Q^{n_0+1}} \geq \frac{1}{2k_0 Q(2E\ell_0)^\kappa |q|^{\kappa+1}}. \blacksquare$$

LEMMA 6.3. *Let $\mathbb{K}$ be either $\mathbb{Q}$ or an imaginary quadratic field and let $\theta \in \mathbb{C}$. Suppose that*

$$|q\theta - p| > C|q|^{-\kappa},$$

for some $C, \kappa > 0$ and all $p, q \in \mathcal{O}_\mathbb{K}$, the ring of integers of $\mathbb{K}$, with $q \neq 0$. Let $a_1, a_2, a_3, a_4 \in \mathcal{O}_\mathbb{K}$ with $a_1 a_4 - a_2 a_3 \neq 0$ and put $\theta' = (a_1\theta + a_2)/(a_3\theta + a_4)$. Then

$$|q\theta' - p| > \frac{C}{|a_4 + a_3\theta|(|a_3|(1 + |\theta'|) + |a_1|)^\kappa} |q|^{-\kappa},$$

for the same $C, \kappa > 0$ and all $p, q \in \mathcal{O}_\mathbb{K}$ with $q \neq 0$.

REMARK 6.4. This is an explicit version of the results in Section 8 of [13], as well as an extension to include the imaginary quadratic fields. It can be used to obtain effective irrationality measures for numbers that can be obtained from θ by means of fractional transformations.

Proof of Lemma 6.3. We can write

(6.2) $$\theta = \frac{-a_4\theta' + a_2}{a_3\theta' - a_1}.$$

Suppose we have $q\theta' - p = \delta$ for some δ. Using this expression, we can write $\theta' = (\delta + p)/q$ and substituting this expression for θ' into (6.2), we find that

$$\theta(a_3 p - a_1 q) - (a_2 q - a_4 p) = -\delta(a_4 + a_3\theta).$$

From our hypothesis that

$$|Q\theta - P| > C|Q|^{-\kappa},$$

for some $C, \kappa > 0$ and all $P, Q \in \mathcal{O}_\mathbb{K}$ with $Q \neq 0$, we know that

$$|\delta(a_4 + a_3\theta)| > C|a_3 p - a_1 q|^{-\kappa}$$

or

$$|\delta| > \frac{C}{|a_4 + a_3\theta|} |a_3 p - a_1 q|^{-\kappa}.$$

We can assume that $|\delta| < 1$. Therefore, $|p| < |q\theta'| + 1$. So

$$|a_3 p - a_1 q| < |a_3|(1 + |\theta' q|) + |a_1 q|$$
$$\leq |a_3|(|q| + |\theta' q|) + |a_1 q| = |q|(|a_3|(1 + |\theta'|) + |a_1|).$$

Hence

$$|q\theta' - p| > \frac{C}{|a_4 + a_3\theta|(|a_3|(1 + |\theta'|) + |a_1|)^\kappa} \, |q|^{-\kappa},$$

completing the proof of our lemma. ∎

7. Analytic bounds. The following lemma is part of Lemma 2.3 in [12] with one important change. In Lemma 2.3 of [12], we only allowed non-zero values for x. We have removed this condition here as it is not used, or required, in the proof of Lemma 2.3 in [12].

This is important and fortunate, as $x = 0$ was actually used to obtain the theorems in [12, 15, 27]. Therefore, despite the statements in each of those papers of a result like that Lemma 2.3 which does exclude $x = 0$, the proofs of the theorems in those papers are still sound.

Note that the condition that $W(x)$ is not a negative real number or zero is required here with the current proof as it is used in the proof of Lemma 2.2 of [12], a lemma which is used as part of the proof of Lemma 2.3 of [12].

LEMMA 7.1. *Let r be a non-negative integer. If $W(x)$ is not a negative real number or zero, then*

(7.1) $S_r(x) = \{\alpha((x - \beta_2)W(x)^{1/n} - (x - \beta_1))$
$$-(\beta_1(x - \beta_2)W(x)^{1/n} - \beta_2(x - \beta_1))\}X^*_{n,r}(U(x), Z(x))$$
$$-(x - \beta_2)(\alpha - \beta_1)U(x)^r R_{1,n,r}(W(x)),$$

where

$$R_{m,n,r}(W(x)) = \frac{\Gamma(r + 1 + m/n)}{\Gamma(m/n)r!} \int\limits_1^{W(x)} ((1 - t)(t - W(x)))^r t^{m/n-r-1} \, dt.$$

Proof. We proved this result for r positive in [12]. It is part of Lemma 2.3 there upon noting that $x - \beta_2$, $x - \beta_1$, $\beta_1(x - \beta_2)$, $\beta_2(x - \beta_1)$ are $6/((n^2 - 1)(\beta_1 - \beta_2))$ times the $a(x)$, $b(x)$, $c(x)$ and $d(x)$ there respectively (see the proof of our Lemma 3.3 for details).

As noted above, we have removed the unnecessary condition that x be non-zero.

So it only remains to consider $r = 0$. Since

$$R_{m,n,0}(W(x)) = \frac{\Gamma(1 + m/n)}{\Gamma(m/n)} \int\limits_1^{W(x)} t^{m/n-1} \, dt = W(x)^{m/n} - 1,$$

we have

$$\{\alpha((x-\beta_2)W(x)^{1/n}-(x-\beta_1))-(\beta_1(x-\beta_2)W(x)^{1/n}-\beta_2(x-\beta_1))\}$$
$$\times X_{n,0}^*(U(x),Z(x))-(x-\beta_2)(\alpha-\beta_1)U(x)^0 R_{1,n,0}(W(x))$$
$$=\alpha\{(x-\beta_2)-(x-\beta_1)\}-\{\beta_1(x-\beta_2)-\beta_2(x-\beta_1)\}$$
$$=\alpha Q_0(x)-P_0(x)=S_0(x),$$

and hence (7.1) holds for $r=0$ too. ∎

Recall that Lemma 5.3 states that for any root, α, of $F(x)$, we can find a value of x such that the first quantity on the right-hand side of the expression for $S_r(x)$ is zero. This is very important for our needs as otherwise this term would actually grow exponentially with r, whereas we require $S_r(x)$ to decrease exponentially quickly to zero with r.

We will show next that the $U(x)^r R_{m,n,r}(W(x))$ term approaches 0 exponentially with r.

LEMMA 7.2. *Let m, n and r be non-negative integers with $0 < m < n$ and $(m,n)=1$.*

(a) *If either u and z are distinct positive real numbers, or u and z are complex numbers with $|u|=|z|\neq 0$ and $z/u\neq -1$, then*

$$|u^r R_{m,n,r}(w)| \leq 2.38|1-w^{m/n}|\frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}$$
$$\times \min(|\sqrt{u}-\sqrt{z}|,|\sqrt{u}+\sqrt{z}|)^{2r},$$

where $w=z/u$.

(b) *If u and z are complex numbers with $|1-z/u|<1$, then*

$$|u^r R_{m,n,r}(w)| < |w^{m/n}-1|\frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\left(\frac{|z-u|^2}{4(|u|-|z-u|)}\right)^r,$$

where $w=z/u$.

Proof. (a) We first consider the case when u and z are distinct positive real numbers. Using the definition of $R_{m,n,r}(w)$ from Lemma 7.1, we put

$$f(t)=\frac{(1-t)(t-w)}{t}.$$

We find that $(d/dt)f(t)=-(t^2-w)/t^2$ and that $(d/dt)f(t)=0$ precisely when $t=\pm\sqrt{w}$. Therefore, $|f(t)|\leq(1-\sqrt{w})^2$ for all t in the closed interval between w and 1.

As we saw in the proof of Lemma 7.1,

$$\int_1^w t^{m/n-1}\,dt=(n/m)(w^{m/n}-1),$$

and the lemma follows in this case.

We next consider the case when u and z are complex numbers with $|u| = |z|$. We proceed similarly to the proof of Lemma 2.5 in [12]. For $w = e^{i\varphi}$ with $0 < \varphi < \pi$ and $\sqrt{w} = e^{i\varphi/2}$, by Cauchy's theorem,

$$(7.2) \qquad R_{m,n,r}(w) = \frac{\Gamma(r+1+m/n)}{\Gamma(m/n)r!} \int_C ((1-t)(t-w))^r t^{m/n-r-1}\, dt,$$

where

$$C = \{t \mid t = e^{i\theta}, \, 0 \le \theta \le \varphi\}.$$

Put

$$f(t) = \frac{(1-t)(t-w)}{t} \quad \text{and} \quad g(t) = t^{m/n-1}.$$

Define $F(\theta) = |f(e^{i\theta})|^2$, so

$$F(\theta) = 4(1 - \cos\theta)(1 - \cos(\theta - \varphi)) \quad \text{for } 0 \le \theta \le \varphi.$$

A simple calculation shows that

$$F'(\theta) = -16 \sin\left(\theta - \frac{\varphi}{2}\right) \sin\frac{\theta}{2} \sin\frac{\varphi - \theta}{2}.$$

The only values of $0 \le \theta \le \varphi$ with $F'(\theta) = 0$ are $\theta = 0$, $\varphi/2$ and φ. It is easy to check that

$$F(\theta) \le F(\varphi/2) = 4\left(1 - \cos\frac{\varphi}{2}\right)^2 = |1 - \sqrt{w}|^4,$$

and hence

$$\left| \int_C f(t)^r g(t)\, dt \right| \le \int_0^\varphi |f(e^{i\theta})|^r |g(e^{i\theta})|\, d\theta \le \varphi |1 - \sqrt{w}|^{2r}.$$

Hence

$$|R_{m,n,r}(w)| \le \varphi \frac{\Gamma(r+1+m/n)}{\Gamma(m/n)r!} |1 - \sqrt{w}|^{2r}$$

for such w.

Note that since $|\varphi| < \pi$, the integrand used in (7.2) is continuous over the path of integration.

The same argument can be used to extend this result to all w on the unit circle using the same definition of the square root.

Notice that $|1 - \sqrt{w}| \le |1 + \sqrt{w}|$ for such w, as the real part of $\sqrt{w}$ is non-negative. Therefore,

$$|\sqrt{u}(1 - \sqrt{w})| \le \min(|\sqrt{u} - \sqrt{z}|, |\sqrt{u} + \sqrt{z}|).$$

Finally, observe that since

$$|\varphi|\sqrt{1 - (m\varphi/n)^2/12} < (n/m)\sqrt{2 - 2\cos(m\varphi/n)} = (n/m)|1 - w^{m/n}|,$$

we have

$$|\varphi| < \frac{(n/m)|1 - w^{m/n}|}{\sqrt{1 - \pi^2/12}} < 2.38(n/m)|1 - w^{m/n}|$$

since $|m\varphi/n| \leq \pi$, so the result holds in this case too.

(b) Following the proof of Lemma 2.4 in [14], we use the change of variables $t = (1 - \lambda) + \lambda w$ to obtain

$$R_{m,n,r}(w) = \frac{\Gamma(r + 1 + m/n)}{\Gamma(m/n)r!} (w - 1)^{2r+1}$$
$$\times \int_0^1 (\lambda(1 - \lambda))^r (1 + \lambda(w - 1))^{m/n-r-1} \, d\lambda.$$

With the estimates $\lambda(1 - \lambda) \leq 1/4$ and $|1 + \lambda(w - 1)| \geq 1 - |w - 1|$ for $0 \leq \lambda \leq 1$ and $|w - 1| < 1$, we find that

$$|R_{m,n,r}(w)| \leq \frac{\Gamma(r + 1 + m/n)}{\Gamma(m/n)r!} \left(\frac{|w - 1|^2}{4(1 - |w - 1|)}\right)^r$$
$$\times \left|\int_0^1 (w - 1)(1 + \lambda(w - 1))^{m/n-1} \, d\lambda\right|$$
$$= |w^{m/n} - 1| \frac{n\Gamma(r + 1 + m/n)}{m\Gamma(m/n)r!} \left(\frac{|w - 1|^2}{4(1 - |w - 1|)}\right)^r,$$

and conclude the proof by substituting $w = z/u$. ∎

LEMMA 7.3. *Let m, n and r be non-negative integers with $0 < m < n$ and $(m, n) = 1$.*

(a) *If either u and z are distinct positive real numbers, or u and z are complex numbers with $|u| = |z|$, then*

$$|X_{m,n,r}^*(z, u)|, |X_{m,n,r}^*(u, z)|$$
$$\leq 2\frac{\Gamma(1 - m/n)r!}{\Gamma(r + 1 - m/n)} \{\max(|\sqrt{u} + \sqrt{z}|, |\sqrt{u} - \sqrt{z}|)\}^{2r}.$$

(b) *If u and z are complex numbers with $\max(|1 - z/u|, |1 - u/z|) < 1$, then*

$$|X_{m,n,r}^*(z, u)|, |X_{m,n,r}^*(u, z)| \leq 2\frac{\Gamma(1 - m/n)r!}{\Gamma(r + 1 - m/n)} \{2(|u| + |z|)\}^r.$$

Proof. (a) We first consider the case when u and z are distinct positive real numbers.

For positive integers r, from Lemma 5.2 of [28], we have

$$|X_{m,n,r}^*(z, u)|, |X_{m,n,r}^*(u, z)| \leq (\sqrt{u} + \sqrt{z})^{2r}.$$

Since $X^*_{m,n,0}(u, z) = 1$, this also holds for $r = 0$. Since

$$(7.3) \qquad \frac{\Gamma(1 - m/n)\, r!}{\Gamma(r + 1 - m/n)} = \frac{r}{r - m/n} \cdots \frac{1}{1 - m/n} > 1,$$

the desired upper bound holds.

Now we turn to the case when u and z are complex numbers with $|u| = |z|$. This is an extension of Lemma 2.6 of [12] to non-negative r and to any u and z with $w = z/u = e^{i\varphi}$ where $-\pi < \varphi \leq \pi$. We proceed similarly here and determine the maximum of the function

$$F(\theta) = |f(e^{i\theta})|^2 = 4(1 - \cos \theta)(1 - \cos(\theta + \varphi))$$

defined there for $0 \leq \theta < 2\pi$ and fixed $-\pi < \varphi \leq \pi$, again observing that since r is a positive integer, f is continuous. Since

$$\frac{d}{d\theta} F(\theta) = -16 \sin\left(\theta + \frac{\varphi}{2}\right) \sin \frac{\theta}{2} \sin \frac{-\varphi - \theta}{2},$$

the only values of θ for which $(d/d\theta)F(\theta) = 0$ are $\theta = 0, 2\pi$ (so that $\sin(\theta/2) = 0$), $-\varphi/2, \pi - \varphi/2, 2\pi - \varphi/2$ (so that $\sin(\theta + \varphi/2) = 0$) and $-\varphi, 2\pi - \varphi$ (so that $\sin(-(\theta + \varphi)/2) = 0$).

- $\theta = 0, 2\pi$: $F(\theta) = 0$.
- $\theta = -\varphi/2$: $F(\theta) = 4(1 - \cos(-\varphi/2))(1 - \cos(\varphi/2)) = 4(1 - \cos(\varphi/2))^2$.
- $\theta = \pi - \varphi/2$: $F(\theta) = 4(1 - \cos(\pi - \varphi/2))(1 - \cos(\pi + \varphi/2))$
  $\qquad\qquad = 4(1 + \cos(\varphi/2))^2$.
- $\theta = 2\pi - \varphi/2$: $F(\theta) = 4(1 - \cos(2\pi - \varphi/2))(1 - \cos(2\pi + \varphi/2))$
  $\qquad\qquad = 4(1 - \cos(\varphi/2))^2$.
- $\theta = -\varphi$: $F(\theta) = 4(1 - \cos(-\varphi))(1 - \cos(0)) = 0$.
- $\theta = 2\pi - \varphi$: $F(\theta) = 4(1 - \cos(2\pi - \varphi))(1 - \cos(2\pi)) = 0$.

Since $-\pi/2 < \varphi/2 \leq \pi/2$, we have $0 \leq \cos(\varphi/2) \leq 1$ and hence the maximum value of $F(\theta)$ is $4(1 + \cos(\varphi/2))^2$. We can write $|1 + \sqrt{w}|^2 = (1 + \cos(\varphi/2))^2 + \sin^2(\varphi/2) = 1 + 2\cos(\varphi/2) + \cos^2(\varphi/2) + \sin^2(\varphi/2) = 2 + 2\cos(\varphi/2)$.

Hence $F(\theta) \leq |1 + \sqrt{w}|^4$ and following the same steps as in the remainder of the proof of Lemma 2.6 of [12], we find that

$$|X^*_{m,n,r}(z, u)| \leq 4|u|^r \frac{\Gamma(1 - m/n)\, r!}{\Gamma(r + 1 - m/n)} |1 + \sqrt{w}|^{2r-2}.$$

Since

$$|\sqrt{u}|\, |1 + \sqrt{w}| \leq \max(|\sqrt{u} + \sqrt{z}|, |\sqrt{u} - \sqrt{z}|),$$

we see that

$$|X^*_{m,n,r}(z, u)| \leq \frac{4}{|1 + \sqrt{w}|^2} \frac{\Gamma(1 - m/n) r!}{\Gamma(r + 1 - m/n)} \max(|\sqrt{u} + \sqrt{z}|, |\sqrt{u} - \sqrt{z}|)^{2r}.$$

Since w is on the unit circle, we can write $1 + \sqrt{w} = 1 + w_1 \pm \sqrt{1 - w_1^2}\, i$, where $0 \le w_1 \le 1$. Hence, $|1 + \sqrt{w}|^2 = 2 + 2w_1 \ge 2$, and so

$$\frac{4}{|1 + \sqrt{w}|^2} \le 2.$$

It follows that

$$|X_{m,n,r}^*(z,u)| \le 2 \frac{\Gamma(1 - m/n)\, r!}{\Gamma(r + 1 - m/n)} \max(|\sqrt{u} + \sqrt{z}|, |\sqrt{u} - \sqrt{z}|)^{2r}.$$

To bound $|X_{m,n,r}^*(u,z)|$ from above, we appeal to the fact that $_2F_1(-r, -r - m/n; 1 - m/n; w^{-1})$ is the complex conjugate of $_2F_1(-r, -r - m/n; 1 - m/n; w)$, as shown at the end of the proof of Lemma 2.6 of [12].

Finally, for $r = 0$, we have $X_{m,n,r}^*(z,u) = X_{m,n,r}^*(u,z) = 1$. From (7.3), the desired upper bound holds for $r = 0$.

(b) We prove the upper bound for $X_{m,n,r}^*(z,u)$, assuming that $|1 - z/u| < 1$. The proof for $X_{m,n,r}^*(u,z)$ is identical.

We can readily extend the proof of Lemma 2.5 of [14] to any $0 < m < n$, so the desired result holds for positive integers, r, since

$$\frac{4e^{2/n}}{\pi} \frac{1}{(2\sqrt{3})^{r+1}} |1 - z/u|^{2r+1} |w|^{m/n} < 1$$

for $r \ge 1$, $n \ge 2$, $|1 - z/u| < 1$, and $2^{r - m/n}(1 + |z/u|)^{r + m/n} < \{2(1 + |z/u|)\}^r$ for such u and z.

The proof for $r = 0$ is identical to that in (a). ■

LEMMA 7.4. *Suppose that d, m, n and r are non-negative integers with $d \ge 1$, $0 < m < n$ and $(m,n) = 1$.*

(a) *Let $D_{m,n,r}$ and $N_{d,n,r}$ be as in the Introduction. Then*

$$(D_{m,n,r}/N_{d,n,r})X_{m,n,r}(1 - dx) \in \mathbb{Z}[x].$$

Moreover, with $d_1 = \gcd(d,n)$ and $d_2 = \gcd(d/d_1, n)$, we have $(d_1^r \prod_{p \mid d_2} p^{v_p(r!)}) \mid N_{d,n,r}$.

(b) *Define*

$$\mu_n = \prod_{\substack{p \mid n \\ p\, prime}} p^{1/(p-1)}.$$

Then each of the coefficients of the polynomial

$$\binom{2r}{r} {_2F_1}(-r, -r \pm m/n; -2r; n\mu_n x)$$

is a rational integer times non-negative integer powers of μ_n. For $n \ge 3$, $\mu_n < 1.94 \log n$, and for $n > 420$, $\mu_n < 1.18 \log n$.

(c) *For n in Tables 1 and 2 and putting either $(\mathcal{C}_n, \mathcal{D}_n) = (\mathcal{C}_{1,n}, \mathcal{D}_{1,n})$ or $(\mathcal{C}_n, \mathcal{D}_n) = (100, \mathcal{D}_{2,n})$ in those tables, we have*

$$(7.4) \quad \max\left(1, \frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)}, \frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\right)\frac{D_{m,n,r}}{N_{d,n,r}} < \mathcal{C}_n\left(\frac{\mathcal{D}_n}{\mathcal{N}_{d,n}}\right)^r.$$

(d) *If $\mathcal{N}_{d,n} \mid n$, then (7.4) holds with $\mathcal{C}_n = 1$ and $\mathcal{D}_n = n\mu_n$ for all $n \geq 3$, and $\mathcal{C}_n = 1$ and $\mathcal{D}_n < 1.18n\log n$ for all $n \geq 3$, $n \neq 6$.*

REMARK 7.5. In practice, for a particular value of n one should use the results in Tables 1 and 2 or, for other values of n, calculate $n\mu_n$ explicitly. However, the values of $\mathcal{C}_n$ and $\mathcal{D}_n$ in part (d) will be useful in obtaining results for arbitrary n.

REMARK 7.6. As Wakabayashi states in Remark 3.1 in [31], it can sometimes be beneficial to have a smaller value of $\mathcal{C}_n$ even at the expense of a somewhat larger $\mathcal{D}_n$. This is the reason for providing $\mathcal{D}_{2,n}$ in Tables 1 and 2. For a given n, it is the smallest value of $\mathcal{D}_n \geq \mathcal{D}_{1,n}$ for which we can take $\mathcal{C}_n < 100$.

REMARK 7.7. It appears that $n\mu_n$ is approximately π/e^γ times the best possible value for $\mathcal{D}_n$. That is,

$$n\mu_n \approx \frac{\pi}{e^\gamma}\exp\left(\frac{\pi}{\phi(n)}\sum_{j=1,\,(j,n)=1}^{n/2}\cot\frac{\pi j}{n}\right).$$

REMARK 7.8. To check the calculations used as part of the proof of part (c), we checked the results for all n considered there and all $r \leq 400$ against calculations done in Maple 8. No differences were found. As well as providing a test for the correctness of the code used, this also provides further evidence that Proposition 3.2 of [28] yields exact information on the prime decomposition of $D_{m,n,r}$.

Proof of Lemma 7.4. (a) The fact that $(D_{m,n,r}/N_{d,n,r})X_{m,n,r}(1-dx) \in \mathbb{Z}[x]$ follows immediately from the definitions of these quantities.

The second statement is a more general version of Proposition 5.1 of [13] and we follow Chudnovsky's method of proof.

We can write

$$X_{m,n,r}(1-dx) = \frac{r!n^r}{(n-m)\cdots(rn-m)}P_{-m}(dx),$$

where

$$P_{-m}(x) = \binom{2r}{r}{}_2F_1(-r, -r-m/n; -2r; x)$$

$$= \sum_{i=0}^{r}\left(\prod_{k=r-i+1}^{r}(kn-m)\right)\frac{1}{i!n^i}\binom{2r-i}{r}(-x)^i.$$

Table 1. Denominator bounds: $3 \leq n \leq 80$

n	$\mathcal{C}_{1,n}$	$\log \mathcal{D}_{1,n}$	$\log \mathcal{D}_{2,n}$	n	$\mathcal{C}_{1,n}$	$\log \mathcal{D}_{1,n}$	$\log \mathcal{D}_{2,n}$
3	$2.0 \cdot 10^7$	0.93	0.97	41	$1.2 \cdot 10^6$	3.37	3.51
4	$4.9 \cdot 10^6$	1.60	1.64	42	2300	4.81	4.86
5	$8.8 \cdot 10^9$	1.37	1.42	43	$2.4 \cdot 10^6$	3.42	3.55
6	35 000	2.75	2.78	44	48 000	4.27	4.34
7	$3.8 \cdot 10^{11}$	1.66	1.75	45	31 000	4.33	4.42
8	$2.5 \cdot 10^8$	2.26	2.39	46	3800	4.26	4.32
9	$4.1 \cdot 10^{11}$	2.19	2.27	47	240 000	3.51	3.59
10	$2.6 \cdot 10^6$	3.02	3.11	48	$2.4 \cdot 10^6$	4.67	4.77
11	$9.7 \cdot 10^9$	2.06	2.19	49	6400	3.80	3.86
12	$3.9 \cdot 10^{11}$	3.18	3.27	50	540	4.58	4.62
13	$1.9 \cdot 10^{13}$	2.21	2.31	51	200 000	4.24	4.35
14	$6.9 \cdot 10^{10}$	3.24	3.37	52	210 000	4.42	4.46
15	94 000	3.21	3.31	53	13 000	3.64	3.70
16	3400	2.99	3.09	54	190 000	4.79	4.88
17	75 000	2.50	2.57	55	1400	4.25	4.34
18	$6.9 \cdot 10^7$	3.64	3.71	56	$2.6 \cdot 10^6$	4.61	4.71
19	$1.2 \cdot 10^6$	2.61	2.73	57	52 000	4.35	4.48
20	14 000	3.60	3.68	58	22 000	4.48	4.56
21	$2.2 \cdot 10^7$	3.47	3.55	59	$1.2 \cdot 10^7$	3.75	3.96
22	750 000	3.58	3.66	60	160 000	5.30	5.38
23	150 000	2.80	2.90	61	14 000	3.79	3.85
24	140 000	3.93	4.08	62	3500	4.54	4.60
25	29 000	3.16	3.28	63	14 000	4.61	4.70
26	$6.3 \cdot 10^6$	3.72	3.83	64	1900	4.44	4.49
27	840 000	3.38	3.48	65	41 000	4.41	4.51
28	16 000	3.87	4.00	66	1200	5.22	5.27
29	27 000	3.02	3.14	67	7400	3.89	3.94
30	$1.4 \cdot 10^6$	4.53	4.63	68	6800	4.67	4.74
31	$1.3 \cdot 10^7$	3.09	3.20	69	5100	4.54	4.63
32	$1.1 \cdot 10^6$	3.70	3.83	70	54 000	5.22	5.31
33	95 000	3.85	3.94	71	3500	3.95	4.03
34	4200	3.99	4.06	72	$1.2 \cdot 10^6$	5.09	5.16
35	890 000	3.85	4.00	74	2200	4.71	4.78
36	$1.8 \cdot 10^7$	4.36	4.41	75	240 000	4.87	4.99
37	3200	3.27	3.35	76	$1.8 \cdot 10^{10}$	4.78	4.86
38	1100	4.09	4.13	77	11 000	4.55	4.60
39	40 000	4.00	4.10	78	$8.1 \cdot 10^6$	5.37	5.50
40	16 000	4.33	4.37	80	39 000	5.07	5.13

Table 2. Denominator bounds: $81 \leq n \leq 486$

n	$\mathcal{C}_{1,n}$	$\log \mathcal{D}_{1,n}$	$\log \mathcal{D}_{2,n}$	n	$\mathcal{C}_{1,n}$	$\log \mathcal{D}_{1,n}$	$\log \mathcal{D}_{2,n}$
81	170 000	4.57	4.69	132	250	5.99	6.00
82	1000	4.82	4.86	134	50	5.33	5.33
84	35 000	5.58	5.65	138	3400	5.93	5.98
85	1400	4.67	4.70	140	270 000	6.00	6.14
86	2800	4.87	4.95	142	41	5.40	5.40
87	2300	4.77	4.85	143	42	5.17	5.17
88	1700	5.02	5.09	144	1200	5.85	5.90
90	11 000	5.72	5.80	150	$2.1 \cdot 10^6$	6.28	6.41
91	1200	4.71	4.75	154	130	5.95	5.96
92	720	4.97	5.01	156	3400	6.15	6.21
93	1600	4.84	4.90	162	1000	5.99	6.03
94	160	4.96	4.97	163	9.4	4.95	4.95
95	670	4.78	4.83	168	77	6.34	6.34
96	11 000	5.40	5.52	169	8.1	5.16	5.16
98	49 000	5.22	5.35	170	820	6.07	6.10
99	5900	5.03	5.10	174	91	6.18	6.18
100	4300	5.31	5.38	180	89	6.49	6.49
102	240	5.63	5.65	182	54	6.12	6.12
104	600	5.18	5.25	186	1100	6.25	6.29
105	3000	5.55	5.60	190	27	6.19	6.19
106	2400	5.08	5.14	198	7300	6.44	6.48
108	5200	5.53	5.58	210	1900	6.98	7.01
110	2400	5.64	5.70	216	510	6.32	6.34
111	200	5.03	5.05	222	9.5	6.44	6.44
112	1900	5.36	5.40	234	3.0	6.61	6.61
114	1000	5.74	5.78	242	8.7	6.20	6.20
116	360 000	5.21	5.33	243	2.0	5.91	5.91
117	700	5.20	5.23	250	3.5	6.38	6.38
118	7000	5.19	5.24	256	37	6.05	6.05
120	11 000	6.04	6.08	286	4.3	6.60	6.60
121	23	4.76	4.76	326	1.2	6.41	6.41
122	4400	5.23	5.30	338	1.0	6.61	6.61
124	1700	5.28	5.35	360	6.0	7.31	7.31
125	46	4.94	4.94	420	2.3	7.79	7.79
126	22 000	6.01	6.08	432	1.0	7.19	7.19
128	79 000	5.20	5.32	486	1.0	7.36	7.36
130	360	5.80	5.83				

(Notice that this differs from [13]. This is due to the fact that $X_r(z)$ and $Y_r(z)$ have been incorrectly switched in (4.3), (4.4), (5.2) and (5.4) of [13].) So

$$X_{m,n,r}(1-dx) = \sum_{i=0}^{r} \left(\prod_{k=1}^{r-i} \frac{1}{kn-m}\right) \frac{r!n^{r-i}d_1^i d_2^i d_3^i}{i!} \binom{2r-i}{r}(-x)^i,$$

where $d_3 = d/(d_1 d_2)$. Since $(kn-m, n) = 1$ for any integer k, it is clear that d_1^r is a divisor of the numerator of $X_{m,n,r}(1-dx)$.

Now suppose that $d_2 > 1$ and let p be a prime divisor of d_2. Then $p^i/p^{v_p(i!)}$ is an integer, since $v_p(i!) \le i/(p-1) \le i$. Hence we can remove a factor of $p^{v_p(r!)}$ from $r!$. Doing so for each prime divisor of d_2 completes the proof of part (a).

(b) The first statement is a slightly stronger and more general version of the statement of Lemma 2.4 of [12], but it is, in fact, what is proved there. Note that the restriction to $j = \pm 1$ is never used in the proof.

Let $f(x)$ be a positive non-decreasing function for $x \ge 2$ and suppose we want to show that $\mu_n \le f(n)$. If n_1 is the largest square-free divisor of n, then $\mu_{n_1} = \mu_n$. If $\mu_{n_1} \le f(n_1)$, then $\mu_n = \mu_{n_1} \le f(n_1) \le f(n)$. So we need only prove $\mu_n \le f(n)$ for square-free n.

Furthermore, $g(x) = x^{1/(x-1)}$ is a decreasing function for $x > 1$. Therefore, we can further reduce our consideration to $n = p_1 \cdots p_k$, where p_i is the ith prime. So we can write

$$\log \mu_n = \sum_{p \le p_k} \frac{\log p}{p-1} < \sum_{p \le p_k} \frac{\log p}{p} + \sum_p \left(\frac{\log p}{p-1} - \frac{\log p}{p}\right)$$

$$< \sum_{p \le p_k} \frac{\log p}{p} + \sum_{p < P} \frac{\log p}{p(p-1)} + \int_{P-1}^{\infty} \frac{\log p}{p-1} \, dp - \int_{P-1}^{\infty} \frac{\log p}{p} \, dp.$$

Following the notation of [1, §27.7] (i.e., letting $f(x) = -\int_1^x (\log t)/(t-1) \, dt$), we get

$$\int_{P-1}^{\infty} \frac{\log p}{p-1} \, dp - \int_{P-1}^{\infty} \frac{\log p}{p} \, dp = \frac{\log^2(P-1)}{2} + f(P-1) - \lim_{z \to \infty} \left(f(z) + \frac{\log^2 z}{2}\right).$$

Using the functional relationship $f(x) + f(1/x) = -(\log^2 x)/2$ (see (27.7.5) in [1]) with $x = 1/z$, we see that

$$\lim_{z \to \infty} f(z) + \frac{\log^2 z}{2} = -f(0) = -\frac{\pi^2}{6}.$$

Therefore,

$$\log \mu_n < \sum_{p \le p_k} \frac{\log p}{p} + \sum_{p < P} \frac{\log p}{p(p-1)} + \frac{\pi^2}{6} + \frac{\log^2(P-1)}{2} - \int_1^{P-1} \frac{\log t}{t-1} \, dt$$

for any prime $P \geq 3$. With $P = 107$, we find that

$$\log \mu_n < \sum_{p \leq p_k} \frac{\log p}{p} + 0.8.$$

For $p_k \geq 32$, by the Corollary to Theorem 6 of [19],

$$\log \mu_n < \sum_{p \leq p_k} \frac{\log p}{p} + 0.8$$
$$< \log p_k - 1.33258 + 1/\log p_k + 0.8 < \log p_k - 0.244.$$

Recalling that $n = p_1 \cdots p_k$, we have $\log n = \theta(p_k)$, where $\theta(x)$ is the logarithm of the product of all primes $\leq x$. Hence, from Theorem 10 of [19], for $p_k \geq 1427$, we have $0.95 p_k < \theta(p_k) = \log n$ and so $\log p_k < \log \log n - \log 0.95$. Thus $\log \mu_n < \log \log n - 0.1927$ and the result holds for such n.

A computation for $11 \leq p_k < 1427$ shows that $\log \mu_n < \log \log n + 0.162$, or $\mu_n < 1.18 \log n$, in this range.

By means of another computation, we find that for $3 \leq n < 2310$, $\mu_n < 1.18 \log n$ holds except for $n = 3, 4, 6, 10, 12, 18, 30, 42, 60, 210$ and 420 and that $\mu_n < 1.94 \log n$ for these n, completing the proof of part (b).

(c) The basis of the proof of this part of the lemma will be Lemma 3.3 from [28] and we shall proceed as in the proof of Lemma 5.1 there. However, to determine how much computation will be needed, we must first find a feasible value for $\mathcal{D}_n$, so we begin with the analytic bounds.

(c-i) Analytic estimates

Numerator estimates. We use d_1 and d_2 as in part (a).

If $d_2 = 1$, then $\mathcal{N}_{d,n} = d_1$ is a divisor of n and, from Lemma 3.5(a) of [28], $\mathcal{N}_{d,n}^r$ is a divisor of $N_{d,n,r}$. Hence $\mathcal{N}_{d,n}^r / N_{d,n,r} \leq 1$.

If $d_2 > 1$, then there exists at least one prime, p, such that p contributes $p^{v_p(n)+1/(p-1)}$ to $\mathcal{N}_{d,n}$. From part (a), we know that

$$(7.5) \qquad \frac{\mathcal{N}_{d,n}^r}{N_{d,n,r}} \leq \frac{\mathcal{N}_{d,n}^r}{d_1^r \prod_{p|d_2} p^{v_p(r!)}} = \frac{\prod_{p \nmid d_2} p^{r v_p(d)} \prod_{p|d_2} p^{r v_p(n)+r/(p-1)}}{d_1^r \prod_{p|d_2} p^{v_p(r!)}}$$
$$= \prod_{p|d_2} p^{r/(p-1)-v_p(r!)} \leq \prod_{p|n} p^{r/(p-1)-v_p(r!)},$$

the last equality holding since $\prod_{p \nmid d_2} p^{v_p(d)} \prod_{p|d_2} p^{v_p(n)} = d_1$.

Now $0 \leq r/(p-1) - v_p(r!) \leq (\log r)/\log p + 1/(p-1)$. Therefore,

$$(7.6) \qquad \frac{\mathcal{N}_{d,n}^r}{N_{d,n,r}} \leq r^{\omega(n)} \mu_n,$$

where $\omega(n)$ is the number of distinct prime factors of n.

Γ-term estimates. Observe that

$$\frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)} = \frac{r}{r-m/n} \cdots \frac{1}{1-m/n} > 1$$

for $n \geq 2$. Similarly,

$$\frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!} = \frac{r+m/n}{r} \cdots \frac{1+m/n}{1} > 1$$

for $n \geq 1$. Furthermore, since $(x+a)/x$ is a decreasing function of x for fixed positive a,

$$\frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!} < \frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)},$$

so

$$(7.7) \quad \max\left(1, \frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)}, \frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\right) = \frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)}.$$

Notice that $-\log(1-x) = x + x^2/2 + x^3/3 + \cdots$ for $|x| < 1$. Furthermore,

$$(x+x^2) - (x+x^2/2+x^3/3+\cdots) > x^2\left(\frac{1}{2} - \frac{x}{3}(1+x+x^2+\cdots)\right)$$

$$= x^2\left(\frac{1}{2} - \frac{x}{3(1-x)}\right) > 0$$

for $0 < x < 3/5$. Therefore, $-\log(1-x) < x + x^2$ for $0 < x < 3/5$, and so

$$\frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)} = \prod_{i=1}^{r} \frac{1}{1-m/(in)} = \frac{n}{n-m} \exp\left(\sum_{i=2}^{r} -\log\left(1-\frac{m}{in}\right)\right)$$

$$< \frac{n}{n-m} \exp\left(\sum_{i=2}^{r}\left(\frac{m}{in} + \frac{m^2}{(in)^2}\right)\right)$$

$$\leq \frac{n}{n-m} \exp\left(\int_{1}^{r}\left(\frac{m}{nx} + \frac{m^2}{(nx)^2}\right)dx\right)$$

$$= \frac{n}{n-m} \exp\left(\frac{mnr\log r - m^2 + m^2 r}{n^2 r}\right)$$

$$< ne^{m^2/n^2} r^{m/n} \leq (en)r^{(n-1)/n}$$

for $r \geq 1$, $n \geq 2$ and $n > m$. Hence

$$\max\left(1, \frac{\Gamma(1-m/n)\,r!}{\Gamma(r+1-m/n)}, \frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\right)\frac{\mathcal{N}_{d,n}^r}{N_{d,n,r}} < (en)r^{\omega(n)+(n-1)/n}\mu_n$$

for $n \geq 2$.

We saw in part (b) of this lemma that $\mu_n < 1.18\log n$ for $n > 420$; it follows that $e\mu_n < 3.21\log n$ for such n. Computing $e\mu_n$ for $3 \leq n \leq 420$, we find that $e\mu_n < 5.26\log n$ for all $n \geq 3$.

From Théorème 11 of [18], $\omega(n) < (1.3842 \log n)/\log \log n$ for $n \geq 3$, so for $n \geq 30$, we have $\omega(n)+(n-1)/n < 1.42 \log n$. Computing $\omega(n)+(n-1)/n$ for $3 \leq n < 29$, we find that $\omega(n) + (n-1)/n < 1.59 \log n$ for all $n \geq 3$.

Therefore,

$$(7.8) \quad \max\left(1, \frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)}, \frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\right) \frac{\mathcal{N}_{d,n}^r}{N_{d,n,r}}$$
$$< 5.26 r^{1.59 \log n} n \log n$$

for $n \geq 3$.

We divide the prime divisors of $D_{m,n,r}$ into two sets, according to their size. We let $D_{m,n,r}^{(S)}$ denote the contribution to $D_{m,n,r}$ from primes at most $(nr)^{1/2}$ and let $D_{m,n,r}^{(L)}$ denote the contribution from the remaining, larger, primes.

$D_{m,n,r}^{(S)}$ **estimates.** From Lemma 3.3(a) of [28], we know that

$$D_{m,n,r}^{(S)} \leq \prod_{p \leq (nr)^{1/2}} p^{\lfloor (\log nr)/\log p \rfloor}.$$

Now $\lfloor x \rfloor \leq 2\lfloor x/2 \rfloor + 1$, so

$$(7.9) \quad D_{m,n,r}^{(S)} \leq \exp\{2\psi(\sqrt{nr}) + \theta(\sqrt{nr})\}$$
$$< \exp\{(2.07766 + 1.01624)\sqrt{nr}\} = \exp\{3.1\sqrt{nr}\},$$

from Theorems 9 and 12 of [19].

From (7.8) and (7.9), we know that

$$(7.10) \quad \max\left(1, \frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)}, \frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\right) \frac{\mathcal{N}_{d,n}^r}{N_{d,n,r}} D_{m,n,r}^{(S)}$$
$$< 5.26 r^{1.59 \log n} n(\log n) \exp\{3.1\sqrt{nr}\}.$$

$D_{m,n,r}^{(L)}$ **estimates.** For each n in Tables 1 and 2, we let ϵ_n denote the analytic bound obtained from Table 1 of Ramaré and Rumely [17] such that $|\theta(x; n, k) - x/\phi(n)| < \epsilon_n x/\phi(n)$ for $x > 10^{10}$, where $\theta(x; n, k)$ is the logarithm of the product of all primes $p \leq x$ with $p \equiv k \bmod n$ and $\phi(n)$ is Euler's phi function.

From Table 2 of [17], we can also find ϵ'_n such that $|\theta(x; n, k) - x/\phi(n)| < \epsilon'_n \sqrt{x}$ for $x \leq 10^{10}$.

Combining these two results, we can find $X_0 = (\phi(n)\epsilon'_n/\epsilon_n)^2 < 10^{10}$ such that the analytic bound $|\theta(x; n, k) - x/\phi(n)| < \epsilon_n x/\phi(n)$ holds for $x \geq X_0$. We then compute $\theta(x; n, k)$ for all $x \leq X_0$ to find the last value X_1 that breaches the analytic bounds of Ramaré and Rumely for n.

Put

$$\mathcal{D}_{n,N} = \exp\left\{ \frac{n}{\phi(n)} \left(\sum_{A=0}^{N-1} \sum_{\ell=1,\,(\ell,n)=1}^{n/2} \left(\frac{1+\epsilon_n}{nA+\ell} - \frac{1-\epsilon_n}{nA+n-\ell} \right) \right. \right.$$
$$\left. \left. + \sum_{\ell=1,\,(\ell,n)=1}^{n/2} \frac{1+\epsilon_n}{nN+\ell} \right) \right\}$$

and compute $\mathcal{D}_{n,N}$ for $N \geq 1$ to find the value of $N_{\min}$ that minimises it. We use $\mathcal{D}_{n,\min}$ to denote this minimum value.

From Lemma 3.3(b) of [28], we see that for any positive integer N satisfying $nr/(nN+n/2) \geq (nr)^{1/2}$, we have

$$D_{m,n,r}^{(L)} \leq \exp\left\{ \sum_{A=0}^{N-1} \sum_{\ell=1,\,(\ell,n)=1}^{n/2} (\theta(nr/(nA+\ell);n,k_\ell) \right.$$
$$\left. - \theta(nr/(nA+n-\ell);n,k_\ell)) \right\}$$
$$\times \exp\left\{ \sum_{\ell=1,\,(\ell,n)=1}^{n/2} \theta(nr/(nN+\ell);n,k_\ell) \right\},$$

where $k_\ell \equiv (-m)\ell^{-1} \bmod n$.

So, for $r > X_1(N_{\min}+1/2) = r_{\mathrm{comp}}$, we have $D_{m,n,r}^{(L)} \leq \mathcal{D}_{n,\min}^r$. Combining this inequality with (7.10) yields

$$(7.11) \quad \max\left(1, \frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)}, \frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!} \right) \frac{\mathcal{N}_{d,n}^r}{N_{d,n,r}} D_{m,n,r}$$
$$< 5.26 r^{1.59\log n} n(\log n) \exp\{3.1\sqrt{nr} + r\log \mathcal{D}_{n,\min}\}$$

for $r > r_{\mathrm{comp}}$. Hence we can choose $\mathcal{D}_n$ to be any real number greater than or equal to

$$\exp\left\{ \frac{\log(5.26 r_{\mathrm{comp}}^{1.59\log n} n \log n)}{r_{\mathrm{comp}}} + 3.1\sqrt{\frac{n}{r_{\mathrm{comp}}}} \right\} \mathcal{D}_{n,\min}.$$

Therefore

$$\max\left(1, \frac{\Gamma(1-m/n)\,r!}{\Gamma(r+1-m/n)}, \frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!} \right) \frac{\mathcal{N}_{d,n}^r}{N_{d,n,r}} D_{m,n,r} < \mathcal{D}_n^r \leq \mathcal{C}_n \mathcal{D}_n^r$$

for all $r \geq r_{\mathrm{comp}}$, provided $\mathcal{C}_n \geq 1$. Note that as $\mathcal{D}_n$ is taken closer to the minimum possible value above, the associated value of $\mathcal{C}_n$ increases. We will try to strike a balance between the sizes of these two quantities. Therefore, we will often take $\mathcal{D}_n$ slightly larger than its minimum possible value here.

We now know $\mathcal{D}_n$ as well as how much computation is required to establish our desired inequalities for all $r \geq 0$ (a computation which will yield $\mathcal{C}_n$), so we are ready to describe the required computations.

(c-ii) Direct calculations. First, for each $1 \leq r \leq 1000$, we directly calculate

$$\max\left(1, \frac{\Gamma(1 - m/n)r!}{\Gamma(r + 1 - m/n)}, \frac{n\Gamma(r + 1 + m/n)}{m\Gamma(m/n)r!}\right)D_{m,n,r},$$

along with the product over all prime divisors of n of the maximum of 1 and $\mathcal{N}^r_{p^{v_p(n)+1},n}/N_{p^{v_p(n)+1},n,r}$.

(c-iii) Calculated estimates. For $1000 < r \leq r_{\text{comp}}$, we take the following steps.

(1) Computation of the Γ terms in the max term.

(2) Estimation of the numerator. We calculate the product over all prime divisors of n of $p^{r/(p-1)-v_p(r!)}$.

This provides an upper bound for $\mathcal{N}^r_{d,n}/N_{d,n,r}$ over all possible values of d.

This is much faster than calculating the maximum possible value of $\mathcal{N}^r_{d,n}/N_{d,n,r}$ precisely over all values of d. However, if, for a particular value of r, after the denominator steps that follow, this estimate leads to a large value of $\mathcal{C}_n$, then we do calculate the maximum possible value of $\mathcal{N}^r_{d,n}/N_{d,n,r}$ precisely.

(3) The computation of the contribution to $D_{m,n,r}$ from the small primes, that is, primes, p, satisfying $p \leq (nr)^{1/2}$, using Proposition 3.2 of [28].

We speed up this part of the calculation, and the following parts, by calculating and storing the first million primes (the last one being 32 441 957) and their logarithms before we start the calculations for any of the r's.

(4) The computation of the contribution to $D_{m,n,r}$ from all primes greater than $\sqrt{nr}$ and at most $(nr - 1)/(nA(r) + 1)$ for some non-negative integer $A(r)$, which depends only on r. We use Lemma 3.3(b) of [28] as well as the cached primes and their logarithms here.

(5) The computation of the contribution to $D_{m,n,r}$ from the remaining larger primes using the same technique as in [28] of using Lemma 3.3(b) there and calculating the contributions from each interval and congruence class via the endpoints of these intervals. The only difference is that here we grew $A(r)$ dynamically over the course of the calculation.

In this manner, we proceeded to estimate the size of the required quantities for all $r \leq r_{\text{comp}}$ to complete the proof of part (c) of the lemma.

All these calculations were performed using code written in the Java programming language (JDK 1.5.0.11). The code is available upon request.

(d) Following Chudnovsky [13] and defining $\mu_{n,r} = \prod_{p|n} p^{\lfloor r/(p-1)\rfloor}$ (note that we use a somewhat different notation from Chudnovsky to avoid confusion with $(\mu_n)^r$), from his Lemma 4.2, we know that

$$\frac{(n - m) \cdots (rn - m)}{r!}\mu_{n,r}$$

is an integer and that $\frac{(n-m)\cdots(rn-m)}{r!}\mu_{n,r}X_{m,n,r}(x)$ has integer coefficients. We will bound this integer from above to obtain our upper bound for $D_{m,n,r}$.

When considering the Γ terms in the proof of part (c), we saw that

$$\max\left(1,\frac{\Gamma(1-m/n)\,r!}{\Gamma(r+1-m/n)},\frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\right)=\frac{\Gamma(1-m/n)r!}{\Gamma(r+1-m/n)}.$$

Now

$$\frac{(n-m)\cdots(rn-m)}{r!}=n^r\frac{\Gamma(r+1-m/n)}{\Gamma(1-m/n)r!}.$$

Hence

$$\max\left(1,\frac{\Gamma(1-m/n)\,r!}{\Gamma(r+1-m/n)},\frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\right)D_{m,n,r}\le n^r\mu_{n,r}.$$

Since $\mathcal{N}_{d,n}\,|\,n$, we saw when considering the numerators in part (c) that $\mathcal{N}_{d,n}^r/N_{d,n,r}\le 1$ and so

$$\max\left(1,\frac{\Gamma(1-m/n)\,r!}{\Gamma(r+1-m/n)},\frac{n\Gamma(r+1+m/n)}{m\Gamma(m/n)r!}\right)\frac{\mathcal{N}_{d,n}^r D_{m,n,r}}{N_{d,n,r}}$$
$$\le n^r\mu_{n,r}\le(n\mu_n)^r<(1.18n\log n)^r$$

for all $n>420$ from part (b). In fact, we see that $n\mu_n<1.18n\log n$ holds for all $n\ge 3$, except $n=3,4,6,10,12,18,30,42,60,210$ and 420. For these excluded values of n, we can use the data in Tables 1 and 2 associated with part (c), along with some calculation, to show that the desired result holds and we can take $\mathcal{C}_n=1$ and $\mathcal{D}_n=1.18n\log n$ for all $n\ge 3$, $n\ne 6$. ∎

LEMMA 7.9. *Let* $\beta_1,\beta_2,P_r(x),Q_r(x)$ *and* $F(x)$ *be defined as in Lemma 3.3 and let* a,b,c *and* d *be complex numbers satisfying* $ad-bc\ne 0$. *Define*

$$K_r(x)=aP_r(x)+bQ_r(x)\quad\text{and}\quad L_r(x)=cP_r(x)+dQ_r(x).$$

If $(x-\beta_1)(x-\beta_2)F(x)\ne 0$, *then*

$$K_{r+1}(x)L_r(x)\ne K_r(x)L_{r+1}(x)$$

for all $r\ge 0$.

Proof. Lemma 2.7 of [12] states this with our $P_r'(x)$ and $Q_r'(x)$ in place of $P_r(x)$ and $Q_r(x)$. Upon noting that our $P_r(x)$ and $Q_r(x)$ are constant multiples of $P_r'(x)$ and $Q_r'(x)$, the result here holds. ∎

8. Proof of Theorem 2.1. We first determine the quantities defined in Lemma 3.3. We have

$$W(x)=\frac{Z(x)}{U(x)}=\frac{\gamma_1}{-\gamma_2}\left(\frac{x-\beta_1}{x-\beta_2}\right)^n.$$

Notice that

$$W(x) = 1 - \frac{U(x) - Z(x)}{U(x)} \quad \text{and} \quad \frac{1}{W(x)} = 1 - \frac{Z(x) - U(x)}{Z(x)}.$$

8.1. Construction of approximations. We now construct our sequences of approximations to $\mathcal{A}(x)$.

From Lemmas 3.3 and 7.1, for $r \geq 0$, we have

$$Q_r(x) = (x - \beta_2)X_{n,r}^*(Z(x), U(x)) - (x - \beta_1)X_{n,r}^*(U(x), Z(x)),$$
$$P_r(x) = \beta_1(x - \beta_2)X_{n,r}^*(Z(x), U(x)) - \beta_2(x - \beta_1)X_{n,r}^*(U(x), Z(x)),$$
$$S_r(x) = -(x - \beta_2)(\mathcal{A}(x) - \beta_1)U(x)^r R_{n,r}(W(x)).$$

These quantities will form the basis for our approximations.

Recalling the definitions of g and d from the statement of Theorem 2.1, we put $U_1(x) = U(x)/g$ and $Z_1(x) = Z(x)/g$ and have

$$X_{n,r}^*(U(x), Z(x)) = g^r X_{n,r}^*(U_1(x), Z_1(x))$$
$$= (gZ_1(x))^r X_{n,r}\left(1 - d\,\frac{Z_1(x) - U_1(x)}{dZ_1(x)}\right).$$

From Lemma 7.4(a),

$$\frac{D_{n,r}}{N_{d,n,r}}\,X_{n,r}\left(1 - d\,\frac{Z_1(x) - U_1(x)}{dZ_1(x)}\right) \in \mathbb{Z}\left[\frac{Z_1(x) - U_1(x)}{dZ_1(x)}\right]$$

and, as a consequence,

$$Z_1(x)^r\,\frac{D_{n,r}}{N_{d,n,r}}\,X_{n,r}\left(1 - d\,\frac{Z_1(x) - U_1(x)}{dZ_1(x)}\right) = \frac{D_{n,r}}{N_{d,n,r}}\,X_{n,r}^*(U_1(x), Z_1(x))$$

is an algebraic integer. Hence

$$\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\,X_{n,r}^*(U(x), Z(x)) = \frac{h_r D_{n,r}}{N_{d,n,r}}\,X_{n,r}^*(U_1(x), Z_1(x)),$$
$$\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\,X_{n,r}^*(Z(x), U(x)) = \frac{h_r D_{n,r}}{N_{d,n,r}}\,X_{n,r}^*(Z_1(x), U_1(x))$$

are algebraic integers in $\mathbb{K}(\beta_1)$ (switching the U's and Z's in the above argument to prove the latter). Since x, β_1 and β_2 are algebraic integers, it follows that

(8.1) $$\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\,P_r(x), \frac{h_r D_{n,r}}{g^r N_{d,n,r}}\,Q_r(x) \in \mathcal{O}_{\mathbb{K}(\beta_1)}.$$

If $[\mathbb{K}(\beta_1) : \mathbb{K}] = 1$, then we let

(8.2) $$p_r = \frac{h_r D_{n,r}}{g^r N_{d,n,r}}\,P_r(x) \quad \text{and} \quad q_r = \frac{h_r D_{n,r}}{g^r N_{d,n,r}}\,Q_r(x).$$

If $[\mathbb{K}(\beta_1) : \mathbb{K}] = 2$, then by hypothesis, β_1 and β_2 are algebraic conjugates over $\mathbb{K}$, as are γ_1 and γ_2, and since $x \in \mathbb{K}$, $U(x)$ is -1 times the algebraic

conjugate of $Z(x)$. Hence, $(x-\beta_1)X_{n,r}^*(U(x),Z(x))$ is the algebraic conjugate of $(-1)^r(x-\beta_2)X_{n,r}^*(Z(x),U(x))$. Similarly, $\beta_2(x-\beta_1)X_{n,r}^*(U(x),Z(x))$ is the algebraic conjugate of $(-1)^r\beta_1(x-\beta_2)X_{n,r}^*(Z(x),U(x))$.

So if $[\mathbb{K}(\beta_1):\mathbb{K}]=2$ and r is odd, then we let

$$(8.3) \qquad p_r = \frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, P_r(x) \quad\text{and}\quad q_r = \frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, Q_r(x).$$

If $\mathbb{K}=\mathbb{Q}$ and r is even, then

$$(x-\beta_1)\,\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, X_{n,r}^*(U(x),Z(x)) = \frac{a+b\sqrt{t}}{2}$$

for some choice of rational integers a, b, t with $t\neq 0$. Hence

$$\frac{h_r D_{n,r}}{\sqrt{t}\,g^r N_{d,n,r}}\, Q_r(x) = -b \in \mathbb{Z}.$$

Similarly,

$$\frac{h_r D_{n,r}}{\sqrt{t}\,g^r N_{d,n,r}}\, P_r(x) \in \mathbb{Z}.$$

So if $\mathbb{K}=\mathbb{Q}$, $[\mathbb{K}(\beta_1):\mathbb{K}]=2$ and r is even, then we let

$$(8.4) \qquad p_r = \frac{h_r D_{n,r}}{\sqrt{t}\,g^r N_{d,n,r}}\, P_r(x) \quad\text{and}\quad q_r = \frac{h_r D_{n,r}}{\sqrt{t}\,g^r N_{d,n,r}}\, Q_r(x).$$

If $\mathbb{K}$ is an imaginary quadratic field and r is even, then

$$(x-\beta_1)\,\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, X_{n,r}^*(U(x),Z(x)) = a+b\sqrt{\tau}$$

for some $a,b\in\mathbb{K}$ and where τ is as in the statement of the theorem. Hence

$$\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, Q_r(x) = -2b\sqrt{\tau} \quad\text{and}\quad \sqrt{\tau}\,\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, Q_r(x) \in \mathcal{O}_{\mathbb{K}}.$$

Similarly,

$$\sqrt{\tau}\,\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, P_r(x) \in \mathcal{O}_{\mathbb{K}}.$$

So if $\mathbb{K}$ is an imaginary quadratic field, $[\mathbb{K}(\beta_1):\mathbb{K}]=2$ and r is even, then we let

$$(8.5) \qquad p_r = \sqrt{\tau}\,\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, P_r(x) \quad\text{and}\quad q_r = \sqrt{\tau}\,\frac{h_r D_{n,r}}{g^r N_{d,n,r}}\, Q_r(x).$$

These are the numbers we shall use for our approximations. We have

$$q_r \mathcal{A}(x) - p_r = s_r,$$

where

$$(8.6) \qquad s_r = t_r \frac{h_r D_{n,r}}{g^r N_{d,n,r}} S_r$$

$$= -t_r \frac{h_r D_{n,r}}{N_{d,n,r}} (x - \beta_2)(\mathcal{A}(x) - \beta_1) U_1(x)^r R_{n,r}(W(x)),$$

where $t_r = 1$, $1/\sqrt{t}$ or $\sqrt{\tau}$ depending on values of p_r and q_r used above and the last equality holds due to the expression for $\mathcal{A}(x)$ in the statement of Theorem 2.1 and Lemma 7.1.

8.2. Estimates. We now want to show that these are "good" approximations; we do this by estimating $|q_r|$ and $|s_r|$ from above.

Since $|t|, |\sqrt{\tau}| \geq 1$, it follows that $|t_r| \leq |\sqrt{\tau}|$. Hence

$$(8.7) \quad |q_r| \leq h|\sqrt{\tau}| \frac{D_{n,r}}{N_{d,n,r}} \{|(x - \beta_1) X_{n,r}^*(U_1(x), Z_1(x))|$$

$$+ |(x - \beta_2) X_{n,r}^*(Z_1(x), U_1(x))|\}$$

$$\leq 2h|\sqrt{\tau}|(|x - \beta_1| + |x - \beta_2|)\mathcal{C}_n \left(\frac{\mathcal{D}_n}{\mathcal{N}_{d,n}}\right)^r$$

$$\times \{\max(|\sqrt{U_1(x)} + \sqrt{Z_1(x)}|, |\sqrt{U_1(x)} - \sqrt{Z_1(x)}|)\}^{2r}$$

from (8.2)–(8.5), the triangle inequality, the definitions of $\mathcal{C}_n$, $\mathcal{D}_n$, h, $\mathcal{N}_{d,n}$ and $Q_r(x)$, as well as Lemma 7.3(a).

Furthermore,

$$(8.8) \quad |s_r| = \left| \frac{t_r h_r D_{n,r}}{N_{d,n,r}} (x - \beta_2)(\mathcal{A}(x) - \beta_1) U_1(x)^r R_{n,r}(W(x)) \right|$$

$$\leq 2.4h|\sqrt{\tau}| |1 - W(x)^{1/n}| |x - \beta_2| |\mathcal{A}(x) - \beta_1|\mathcal{C}_n \left(\frac{\mathcal{D}_n}{\mathcal{N}_{d,n}}\right)^r$$

$$\times \{\min(|\sqrt{U_1(x)} + \sqrt{Z_1(x)}|, |\sqrt{U_1(x)} - \sqrt{Z_1(x)}|)\}^{2r}$$

from (8.6), the definition of h as well as Lemma 7.2(a).

Recall that we are only considering $0 < W(x) < 1$ or $|W(x)| = 1$ in Theorem 2.1, so only parts (a) of Lemmas 7.2 and 7.3 are required here.

We can apply Lemma 7.9 to see that $p_r q_{r+1} \neq p_{r+1} q_r$.

From (8.7) and (8.8), we can set

$$k_0 = 2h|\sqrt{\tau}|(|x - \beta_1| + |x - \beta_2|)\mathcal{C}_n,$$

$$\ell_0 = \max(0.5, 2.4h|\sqrt{\tau}| |1 - W(x)^{1/n}| |x - \beta_2| |\mathcal{A}(x) - \beta_1|\mathcal{C}_n),$$

$$E = \frac{\mathcal{N}_{d,n}}{\mathcal{D}_n} \{\min(|\sqrt{U_1(x)} + \sqrt{Z_1(x)}|, |\sqrt{U_1(x)} - \sqrt{Z_1(x)}|)\}^{-2},$$

$$Q = \frac{\mathcal{D}_n}{\mathcal{N}_{d,n}} \{\max(|\sqrt{U_1(x)} + \sqrt{Z_1(x)}|, |\sqrt{U_1(x)} - \sqrt{Z_1(x)}|)\}^2.$$

Hence we have $\kappa = (\log Q)/\log E$ and $c = 2k_0 Q (2\ell_0 E)^\kappa$ in Lemma 6.1. Since $1/(2\ell_0) \leq 1$, our result follows.

9. Proof of Theorem 2.4. The proof is identical to that of Theorem 2.1 except that we apply parts (b) of Lemmas 7.2 and 7.3, rather than parts (a). With this change, we have

$$k_0 = 2h|\sqrt{\tau}|(|x - \beta_1| + |x - \beta_2|)\mathcal{C}_n,$$
$$\ell_0 = \max(0.5, h|\sqrt{\tau}| |1 - W(x)^{1/n}| |x - \beta_2| |\mathcal{A}(x) - \beta_1|\mathcal{C}_n),$$
$$E = \frac{\mathcal{N}_{d,n}}{\mathcal{D}_n} \frac{4(|U_1(x)| - |Z_1(x) - U_1(x)|)}{|Z_1(x) - U_1(x)|^2},$$
$$Q = \frac{\mathcal{D}_n}{\mathcal{N}_{d,n}} 2(|U_1(x)| + |Z_1(x)|).$$

Hence we have $\kappa = (\log Q)/\log E$ and $c = 2k_0 Q (2\ell_0 E)^\kappa$ in Lemma 6.1. Since $1/(2\ell_0) \leq 1$, our result follows.

10. Proof of Corollary 2.6. We first determine the quantities defined in Lemma 3.3. Put $\beta_1 = 0$, $\beta_2 = b - a$, $\gamma_1 = 1$, $\gamma_2 = -(b/a)^{n-1}$ and $x = b$. We have

$$U(x) = -\gamma_2(x - \beta_2)^n = \frac{b^{n-1}}{a^{n-1}}(x - b + a)^n,$$
$$Z(x) = \gamma_1(x - \beta_1)^n = x^n,$$
$$W(x) = \frac{Z(x)}{U(x)} = \frac{a^{n-1}}{b^{n-1}}\left(\frac{x}{x - b + a}\right)^n.$$

Hence, since $U(b) = ab^{n-1}$, $Z(b) = b^n$ and $W(b) = b/a$, using the notation of Lemma 5.3,

$$\mathcal{A}(b) = \frac{\beta_1(b - \beta_2)W(b)^{1/n} + \beta_2(b - \beta_1)}{(b - \beta_2)W(b)^{1/n} + (b - \beta_1)}$$
$$= \frac{(b - a)b}{-a(b/a)^{1/n} + b} = -\frac{(b - a)(b/a)^{(n-1)/n}}{1 - (b/a)^{(n-1)/n}} = \alpha.$$

Since $(a, b) = \mathcal{O}_{\mathbb{K}}$, by assumption, we can take $g = b^{n-1}$ and $h_r = h = 1$. So we put $U_1(x) = a$, $Z_1(x) = b$ and take d to be the largest positive rational integer such that $(a - b)/d$ is an algebraic integer.

Observe that

$$\frac{b}{a}\left(\frac{b - a}{\alpha} - 1\right) = -\left(\frac{b}{a}\right)^{1/n},$$

so if

$$q_r \alpha - p_r = s_r,$$

then
$$ap_r(-(b/a)^{1/n}) - b((b-a)q_r - p_r) = -b(b-a)\frac{s_r}{\alpha}.$$

We use the p_r's and q_r's defined in the proof of Theorem 2.1 (note that they are members of $\mathcal{O}_\mathbb{K}$). In particular, with the expressions in this section for the relevant quantities,
$$p_r = \frac{h_r}{g^r}\frac{D_{n,r}}{N_{d,n,r}}\; P_r(b) = \frac{D_{n,r}}{N_{d,n,r}}\,(a-b)bX^*_{n,r}(a,b).$$

Note that p_r and $b((b-a)q_r - p_r)$ are both divisible by $b(b-a)$, so we have
$$\frac{ap_r}{b(b-a)}\,((b/a)^{1/n}) - \left(\frac{p_r}{b-a} - q_r\right) = \frac{s_r}{\alpha}.$$

Therefore, by Lemma 7.3(a) along with the definitions of $\mathcal{C}_n$, $\mathcal{D}_n$ and $\mathcal{N}_{d,n}$, we have
$$(10.1)\qquad \left|\frac{ap_r}{b(b-a)}\right| \le 2|a|\mathcal{C}_n\left(\frac{\mathcal{D}_n}{\mathcal{N}_{d,n}}\right)^r \{\max(|\sqrt{a}+\sqrt{b}|, |\sqrt{a}-\sqrt{b}|)\}^{2r}.$$

Similarly, by Lemma 7.2(a),
$$\left|\frac{s_r}{\alpha}\right| = \left|\frac{D_{n,r}}{N_{d,n,r}}\,aU_1(b)^r R_{n,r}(W(b))\right|$$
$$\le 2.38|1-(b/a)^{1/n}|\,|a|\mathcal{C}_n\left(\frac{\mathcal{D}_n}{\mathcal{N}_{d,n}}\right)^r \{\min(|\sqrt{a}+\sqrt{b}|, |\sqrt{a}-\sqrt{b}|)\}^{2r}.$$

Next, we require an upper bound for $|1-(b/a)^{1/n}|$.

If $b/a \in \mathbb{Q}$, then $0 < b/a < 1$ and $0 < (a-b)/a < 1$. From the binomial theorem, we have
$$|1-(b/a)^{1/n}|$$
$$= |1-(1-(a-b)/a)^{1/n}|$$
$$= \left|\frac{a-b}{na}\left\{1 + \frac{n-1}{2n}\left(\frac{a-b}{a}\right) + \frac{(n-1)(2n-1)}{6n^2}\left(\frac{a-b}{a}\right)^2 + \cdots\right\}\right|$$
$$< \frac{|a-b|}{n|a|}\left\{1 + \left(\frac{a-b}{a}\right) + \left(\frac{a-b}{a}\right)^2 + \cdots\right\} = \frac{a-b}{n|b|}.$$

If $|b/a| = 1$, then we can write $b/a = e^{i\varphi}$ for some $-\pi < \varphi \le \pi$. So we have
$$|1-(b/a)^{1/n}| = \sqrt{2 - 2\cos(\varphi/n)}.$$
Similarly,
$$|1-a/b| = \sqrt{2 - 2\cos\varphi}.$$

Now $(2/\pi)^2\varphi^2 \le 2 - 2\cos\varphi \le \varphi^2$ for all $-\pi < \varphi \le \pi$. Hence
$$|1-(b/a)^{1/n}| \le |\varphi/n| = \pi/(2n)(2/\pi)|\varphi| \le \pi/(2n)|1-(a/b)|.$$

Therefore,

$$(10.2) \qquad \left| \frac{s_r}{\alpha} \right| \le 1.25 \left| \frac{a(a-b)}{b} \right| \mathcal{C}_n \left(\frac{\mathcal{D}_n}{\mathcal{N}_{d,n}} \right)^r \{ \min(|\sqrt{a}+\sqrt{b}|, |\sqrt{a}-\sqrt{b}|) \}^{2r}$$

since $n \ge 3$.

From (10.1) and (10.2), we can set

$$k_0 = 2|a|\mathcal{C}_n,$$

$$\ell_0 = 1.25 \left| \frac{a(a-b)}{b} \right| \mathcal{C}_n,$$

$$E = \frac{\mathcal{N}_{d,n}}{\mathcal{D}_n} \{ \min(|\sqrt{a}+\sqrt{b}|, |\sqrt{a}-\sqrt{b}|) \}^{-2},$$

$$Q = \frac{\mathcal{D}_n}{\mathcal{N}_{d,n}} \{ \max(|\sqrt{a}+\sqrt{b}|, |\sqrt{a}-\sqrt{b}|) \}^2.$$

Hence $\kappa = (\log Q)/\log E$ and $c = 2k_0 Q(2\ell_0 E)^\kappa$ in Lemma 6.1.

We have $|a/b| \ge 1$ and $|a-b| \ge 1$, since the closest distance between two algebraic integers in an imaginary quadratic field is 1. In addition, $\mathcal{C}_n \ge 1$ (since $D_{n,0} = 1$). Therefore, $1/(2\ell_0) < 1$ and our result follows.

11. Proof of Corollary 2.7. We do not specify a value of x here, so we need only concern ourselves with determining d, g, h_r and h, and hence obtaining expressions for E, Q and c.

• g

Using the definitions of g and the g_i's in Corollary 2.7, we will show that $(U(x)\sqrt{g_3/g_2}/g_1)^2$ is an algebraic integer (and in $\mathbb{Q}(\sqrt{t})$). Since $g_4 \in \mathbb{Z}$, it will follow that $U(x)/g = \sqrt{g_4}\, U(x)\sqrt{g_3/g_2}/g_1$ is also an algebraic integer.

Writing

$$\frac{U^2(x)g_3}{g_1^2 g_2} = \frac{g_3}{4} \left\{ \left(\frac{u_1}{g_1 g_2} \right)^2 g_2 + \left(\frac{u_2}{g_1} \right)^2 \frac{t}{g_2} \right\} + \frac{u_1}{g_1 g_2} \frac{u_2}{g_1} \frac{g_3}{2} \sqrt{t} \in \mathbb{Q}(\sqrt{t}),$$

we have

$$\text{Trace}\left(\frac{U^2(x)g_3}{g_1^2 g_2} \right) = \frac{g_3(u_1^2 + u_2^2 t)}{2g_1^2 g_2}, \qquad \text{Norm}\left(\frac{U^2(x)g_3}{g_1^2 g_2} \right) = \frac{g_3^2(u_1^2 - u_2^2 t)^2}{16 g_1^4 g_2^2}.$$

If both of these quantities are rational integers, then the minimal polynomial of $U^2(x)g_3/(g_1^2 g_2)$ over $\mathbb{Q}$ will be monic with rational integer coefficients and hence $U^2(x)g_3/(g_1^2 g_2)$ is an algebraic integer.

From the definitions of g_1 and g_2, we see that t/g_2, $u_1/(g_1 g_2)$ and u_2/g_1 are all rational integers, so $(u_1^2 + u_2^2 t)/(g_1^2 g_2)$ and $(u_1^2 - u_2^2 t)^2/(g_1^4 g_2^2)$ are both rational integers.

If $t \equiv 1 \bmod 4$ and $(u_1 - u_2)/g_1 \equiv 0 \bmod 2$, then

$$\frac{u_1^2}{g_1^2} + \frac{u_2^2}{g_1^2} \, t = \begin{cases} 0 \bmod 4 & \text{if } u_1/g_1 \equiv u_2/g_1 \equiv 0 \bmod 2, \\ 2 \bmod 4 & \text{if } u_1/g_1 \equiv u_2/g_1 \equiv 1 \bmod 2, \end{cases}$$

while

$$\frac{u_1^2}{g_1^2} + \frac{u_2^2}{g_1^2} \, t = 0 \bmod 4$$

if $t \equiv 3 \bmod 4$ and $(u_1 - u_2)/g_1 \equiv 0 \bmod 2$.

In both cases, t is odd, so g_2 is also odd and thus $\mathrm{Trace}(U^2(x)g_3/(g_1^2 g_2)) \in \mathbb{Z}$.

If neither of these conditions holds (i.e., if we are in the "otherwise" case of the definition of g_3), then $g_3 = 4$ and again $\mathrm{Trace}(U^2(x)g_3/(g_1^2 g_2)) \in \mathbb{Z}$.

We proceed in a similar way to show that $\mathrm{Norm}(U^2(x)g_3/(g_1^2 g_2)) \in \mathbb{Z}$.

If $t \equiv 1 \bmod 4$ and $(u_1 - u_2)/g_1 \equiv 0 \bmod 2$, then

$$\frac{u_1^2}{g_1^2} - \frac{u_2^2}{g_1^2} \, t = 0 \bmod 4.$$

If $t \equiv 3 \bmod 4$ and $(u_1 - u_2)/g_1 \equiv 0 \bmod 2$, then

$$\frac{u_1^2}{g_1^2} - \frac{u_2^2}{g_1^2} \, t = \begin{cases} 0 \bmod 4 & \text{if } u_1/g_1 \equiv u_2/g_1 \equiv 0 \bmod 2, \\ 2 \bmod 4 & \text{if } u_1/g_1 \equiv u_2/g_1 \equiv 1 \bmod 2. \end{cases}$$

Since in both cases t is odd, g_2 is also odd, so $\mathrm{Norm}(U^2(x)g_3/(g_1^2 g_2)) \in \mathbb{Z}$. If neither of these conditions holds, then $g_3 = 4$ and again

$$\mathrm{Norm}(U^2(x)g_3/(g_1^2 g_2)) \in \mathbb{Z}.$$

Since $Z(x)$ is -1 times the algebraic conjugate of $U(x)$, $Z(x)/g$ is an algebraic integer as well.

- h_r

Since $g^2 \in \mathbb{Q}$, we can take $h_r = 1$ for r even. However, if, for example, g_2 is a proper divisor of t or if $g_3 = 2$, then g need not be a perfect square. Since $g_2 g_3 g_4/\mathrm{core}(g_2 g_3 g_4)$ is a perfect square, we can take $h_r = \sqrt{\mathrm{core}(g_2 g_3 g_4)}$ for r odd. From the definition of g_4 we see that $g_4 \mid \mathrm{core}(g_2 g_3)$, so $\mathrm{core}(g_2 g_3 g_4) \le \mathrm{core}(g_2 g_3)$. Since $g_2 \mid t$ and $g_3 = 1, 2$ or 4, we have $\mathrm{core}(g_2 g_3) \le 2t$. Hence $h_r \le \sqrt{2t}$ for r odd.

- d

Since $U(x) - Z(x) = u_1$, our definition of d is correct.

- E and Q

Since $U(x) = (u_1 + u_2\sqrt{t})/2$, we have $Z(x) = (-u_1 + u_2\sqrt{t})/2$. Hence,

$$(\sqrt{U(x)} \pm \sqrt{Z(x)})^2 = U(x) + Z(x) \pm 2\sqrt{U(x)Z(x)} = u_2\sqrt{t} \pm \sqrt{u_2^2 t - u_1^2},$$

giving rise to our expressions for E and Q.

- c

From our determination of h_r above, we can let $h = \sqrt{|2t|}$. Since $\mathbb{K} = \mathbb{Q}$ here, we have $\tau = 1$ and hence take c to be

$$4\sqrt{|2t|}\,(|x - \beta_1| + |x - \beta_2|)\mathcal{C}_n Q$$
$$\times (\max(1, 5\sqrt{|2t|}\,|1 - W(x)^{1/n}|\,|x - \beta_2|\,|\mathcal{A}(x) - \beta_1|\mathcal{C}_n E))^{\kappa}.$$

References

[1] M. Abramowitz and I. E. Stegun (eds.), *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, Nat. Bureau of Standards, Washington, 1964.

[2] S. Akhtari, A. Togbé and P. G. Walsh, *On the equation $aX^4 - bY^2 = 2$*, Acta Arith. 131 (2008), 145–169.

[3] A. Baker, *Rational approximations to certain algebraic numbers*, Proc. London Math. Soc. (3) 14 (1964), 385–398.

[4] —, *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers*, Quart. J. Math. Oxford 15 (1964), 375–383.

[5] —, *Linear forms in the logarithms of algebraic numbers I*, Mathematika 13 (1966), 204–216.

[6] A. Baker and C. L. Stewart, *On effective approximations to cubic irrationals*, in: New Advances in Transcendence Theory (Durham, 1986), Cambridge Univ. Press, 1988, 1–24.

[7] M. A. Bennett, *Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$*, J. Reine Angew. Math. 535 (2001), 1–49.

[8] E. Bombieri, *On the Thue–Siegel–Dyson Theorem*, Acta Math. 148 (1982), 255–296.

[9] E. Bombieri, A. L. van der Poorten and J. D. Vaaler, *Effective measures of irrationality for cubic extensions of number fields*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 23 (1996), 211–248.

[10] W. E. Boyce and R. C. DiPrima, *Elementary Differential Equations and Boundary Value Problems*, 6th ed., Wiley, 1996.

[11] J. H. Chen, *A new solution of the Diophantine equation $X^2 + 1 = 2Y^4$*, J. Number Theory 48 (1994), 62–74.

[12] J. H. Chen and P. M. Voutier, *Complete solution of the diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equations*, ibid. 62 (1997), 71–99.

[13] G. V. Chudnovsky, *On the method of Thue–Siegel*, Ann. of Math. 117 (1983), 325–382.

[14] C. Heuberger, *All solutions to Thomas' family of Thue equations over imaginary quadratic number fields*, J. Symbolic Comput. 41 (2006), 980–998.

[15] G. Lettl, A. Pethő and P. M. Voutier, *Simple families of Thue inequalities*, Trans. Amer. Math. Soc. 351 (1999), 1871–1894.

[16] J. Liouville, *Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques*, C. R. Acad. Sci. Paris Sér. A 18 (1844), 883–885.

[17] O. Ramaré and R. Rumely, *Primes in arithmetic progressions*, Math. Comp. 65 (1996), 397–425.

[18] G. Robin, *Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n*, Acta Arith. 42 (1983), 367–389.

[19] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[20] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1–20 and 168.

[21] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. 1 (1929), 41–69.

[22] —, *Einige Erläuterungen zu Thues Untersuchungen über Annäherungswerte algebraischer Zahlen und diophantische Gleichungen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II 1970, 169–195.

[23] A. Thue, *Bemerkungen über gewisse Näherungsbrüche algebraischer Zahlen*, Kra. Vidensk. Selsk. Skrifter I Mat. Nat. Kl. 1908, no. 3.

[24] —, *Über rationale Annäherungswerte der reellen Wurzel der ganzen Funktion dritten Grades $x^3 - ax - b$*, ibid. 1908, no. 6.

[25] —, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), 284–305.

[26] —, *Ein Fundamentaltheorem zur Bestimmung von Annäherungswerten aller Wurzeln gewisser ganzer Funktionen*, ibid. 138 (1910), 96–108.

[27] A. Togbé, P. M. Voutier and P. G. Walsh, *Solving a family of Thue equations with an application to the equation $x^2 - Dy^4 = 1$*, Acta Arith. 120 (2005), 39–58.

[28] P. M. Voutier, *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers revisited*, J. Théor. Nombres Bordeaux 19 (2007), 263–288.

[29] —, *Effective irrationality measures and approximations by algebraic conjugates*, Acta Arith., to appear.

[30] I. Wakabayashi, *On a family of quartic Thue inequalities I*, J. Number Theory 66 (1997), 70–84.

[31] —, *On a family of quartic Thue inequalities II*, ibid. 80 (2000), 60–88.

[32] P. Z. Yuan, *On algebraic approximations of certain algebraic numbers*, ibid. 102 (2003), 1–10.

Paul M. Voutier
London, UK
E-mail: Paul.Voutier@gmail.com