Bull. Aust. Math. Soc. (First published online 2023), page 1 of 12*
doi:10.1017/S0004972723000278
*Provisional—final page numbers to be inserted when paper edition is published

ON DISCRIMINANTS OF MINIMAL POLYNOMIALS OF THE RAMANUJAN t_n CLASS INVARIANTS

SARTH CHAVAN

(Received 1 October 2022; accepted 12 February 2023)

Dedicated to all my Rickoid friends who turned into a family

Abstract

We study the discriminants of the minimal polynomials $\mathcal{P}_n$ of the Ramanujan t_n class invariants, which are defined for positive $n \equiv 11 \pmod{24}$. We show that $\Delta(\mathcal{P}_n)$ divides $\Delta(H_n)$, where H_n is the ring class polynomial, with quotient a perfect square and determine the sign of $\Delta(\mathcal{P}_n)$ based on the ideal class group structure of the order of discriminant $-n$. We also show that the discriminant of the number field generated by $j((-1+\sqrt{-n})/2)$, where j is the j-invariant, divides $\Delta(\mathcal{P}_n)$. Moreover, using Ye's computation of $\log|\Delta(H_n)|$ ['Revisiting the Gross–Zagier discriminant formula', *Math. Nachr.* **293** (2020), 1801–1826], we show that 3 never divides $\Delta(H_n)$, and thus $\Delta(\mathcal{P}_n)$, for all squarefree $n \equiv 11 \pmod{24}$.

2020 *Mathematics subject classification*: primary 11R29; secondary 11F03, 11G07, 11R09, 11R37.

Keywords and phrases: elliptic curves, ring class polynomials, class invariant, j-invariant, discriminant.

1. Introduction and main results

Let E be an elliptic curve over $\mathbb{C}$ that has *complex multiplication* (CM) by an imaginary quadratic order $\mathcal{O}$, by which we mean that the endomorphism ring $\mathrm{End}(E)$ is isomorphic to $\mathcal{O}$. Let K denote the fraction field of $\mathcal{O}$. The j-invariant of E is an algebraic integer whose minimal polynomial over K is the *ring class polynomial* H_n, where $-n$ is the discriminant of $\mathcal{O}$. (When $\mathcal{O}$ is a maximal order, H_n is often called the *Hilbert class polynomial*.) The ring class polynomial H_n is defined by

$$H_n(x) := \prod_{j(E)\in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (x - j(E)),$$

where $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E) : \mathrm{End}(E) \cong \mathcal{O}\}$ is the set of j-invariants of elliptic curves E over $\mathbb{C}$ with CM by the imaginary quadratic order $\mathcal{O}$ with discriminant $\mathrm{disc}(\mathcal{O}) = -n$.

Moreover, $H_n \in \mathbb{Z}[x]$ and its splitting field over the imaginary quadratic field K is the *ring class field* $K_{\mathcal{O}}$, which is an abelian extension of K whose Galois group $\mathrm{Gal}(K_{\mathcal{O}}/K)$

The author was supported by The 2022 Spirit of Ramanujan Fellowship and The 2022 Mehta Fellowship.

TABLE 1. Ramanujan's table of $\mathcal{P}_n$ for $n = 11, 35, 59, 83, 107$.

n	$\mathcal{P}_n(z)$
11	$z - 1$
35	$z^2 + z - 1$
59	$z^3 + 2z - 1$
83	$z^3 + 2z^2 + 2z - 1$
107	$z^3 - 2z^2 + 4z - 1$

is isomorphic to the class group $\mathrm{Cl}(\mathcal{O})$, via the Artin map. This is indeed a remarkable result as it implies that of uncountably many isomorphism classes of elliptic curves over $\mathbb{C}$, only countably many have CM.

In his third notebook [11, pages 392–393], Ramanujan defined the values

$$t_n := \frac{f(\sqrt[3]{q_n})f(q_n^3)}{f^2(q_n)}\sqrt{3}q_n^{1/18},$$

where $q_n = \exp(-\pi\sqrt{n})$ and $f(-q) = \prod_{n\geqslant 1}(1 - q^n)$. For all positive $n \equiv 11 \pmod{24}$, let $\mathcal{P}_n$ be the minimal polynomial of t_n over $\mathbb{Q}$. Without any further explanation on how he found them, Ramanujan gave the polynomials $\mathcal{P}_n$ based on t_n for the first five values of $n \equiv 11 \pmod{24}$ (see Table 1).

Berndt and Chan [2, Theorem 1.2] later verified these claims, using laborious computations involving Greenhill polynomials and Weber class invariants, and proved that each $\mathcal{P}_n$ has t_n as a root. Because of its computational complexity, their method could not be applied for higher values of n. However, they proved the following result.

THEOREM 1.1 [2, Theorem 4.1]. *Let $n \equiv 11 \pmod{24}$ be a squarefree positive integer, and suppose that the class number of the associated imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$ is odd. Then, t_n is a real unit generating the ring class field over $\mathbb{Q}(\sqrt{-n})$ with respect to the order of discriminant $-n$.*

Ten years later, Konstantinou and Kontogeorgis [7] generalised this result by removing the constraint that the class number be odd and also provided an efficient method for constructing the minimal polynomials $\mathcal{P}_n$ of t_n over $\mathbb{Q}$ from the Ramanujan values t_n for $n \equiv 11 \pmod{24}$, using the Shimura reciprocity law. They also proved that the Ramanujan value t_n is a class invariant for $n \equiv 11 \pmod{24}$ [7, Theorem 3.4]. It follows that the degree of $\mathcal{P}_n$ equals the class number of the order of discriminant $-n$ for all positive integers $n \equiv 11 \pmod{24}$.

Let $\mathfrak{j}_n = j((-1 + \sqrt{-n})/2)$, for all $n \in \mathbb{N}$, where j denotes the j-invariant as defined in Section 2.1. In a follow-up paper in 2010, Konstantinou and Kontogeorgis proved the following important result.

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

PROPOSITION 1.2 [8, Lemma 3]. *Suppose $R_{\mathcal{P}}$ is a real root of a Ramanujan polynomial $\mathcal{P}_n$. Then, the real number $R_H = (R_{\mathcal{P}}^6 - 27R_{\mathcal{P}}^{-6} - 6)^3$ is a real root of the corresponding ring class polynomial H_n.*

In their proof, they show that, letting $R_{\mathcal{P}} = t_n$ gives $\mathrm{j}_n = (t_n^6 - 27t_n^{-6} - 6)^3$ [8, page 12]. Moreover, notice that $\mathbb{Z}[\mathrm{j}_n] \subseteq \mathbb{Z}[t_n]$, which also follows from Section 3.1.

The coefficients of the polynomial $\mathcal{P}_n$ have remarkably smaller size compared to the coefficients of the corresponding ring class polynomial H_n, suggesting that they may be useful for generating elliptic curves over prime fields by the CM method. Proposition 1.2 supports this because it shows that the roots of the polynomials $\mathcal{P}_n$ can be transformed to the roots of H_n. For more details on constructing elliptic curves with the CM method, see [1, 4].

We study the discriminant of $\mathcal{P}_n$. The historical precedent for doing so comes from [6] in which the prime factorisations of certain resultants of ring class polynomials are computed. In [6], Gross and Zagier computed the prime factorisation of the discriminant of the ring class polynomial associated to the fundamental discriminant $-p$, where $p \equiv 3 \pmod 4$ is a prime. This result was later generalised by Dorman [5] to ring class polynomials associated to arbitrary fundamental discriminants and by Ye [14] to ring class polynomials associated to certain nonfundamental discriminants.

1.1. Notation. Fix a positive integer $n \equiv 11 \pmod{24}$ and let $K = \mathbb{Q}(\sqrt{-n})$ denote the associated imaginary quadratic field. Let h_n and $\mathrm{Cl}(n)$ denote the class number and ideal class group of the order of discriminant $-n$, respectively, and let $\mathrm{Cl}(n)[2]$ be the subgroup of $\mathrm{Cl}(n)$ consisting of elements of order at most 2.

1.2. Main results. Our first main result relates $\Delta(H_n)$ to $\Delta(\mathcal{P}_n)$.

THEOREM 1.3. *For all positive $n \equiv 11 \pmod{24}$,*

$$\Delta(H_n) = \Delta(\mathcal{P}_n)[\mathbb{Z}[t_n] : \mathbb{Z}[\mathrm{j}_n]]^2,$$

where $[\mathbb{Z}[t_n] : \mathbb{Z}[\mathrm{j}_n]]$ is the index of $\mathbb{Z}[\mathrm{j}_n]$ in $\mathbb{Z}[t_n]$.

REMARK 1.4. Since the quotient $[\mathbb{Z}[t_n] : \mathbb{Z}[\mathrm{j}_n]]^2$ is a perfect square, we deduce that $\Delta(H_n)$ and $\Delta(\mathcal{P}_n)$ have the same sign for all positive integers $n \equiv 11 \pmod{24}$.

Let $\mathcal{D}(\mathfrak{F})$ denote the discriminant of an algebraic number field $\mathfrak{F}$. Our next main result is the following result.

THEOREM 1.5. *For all positive integers $n \equiv 11 \pmod{24}$,*

$$\Delta(\mathcal{P}_n) = \mathcal{D}(\mathbb{Q}(\mathrm{j}_n))[\mathcal{O}_{\mathbb{Q}(\mathrm{j}_n)} : \mathbb{Z}[t_n]]^2,$$

where $[\mathcal{O}_{\mathbb{Q}(\mathrm{j}_n)} : \mathbb{Z}[t_n]]$ is the index of $\mathbb{Z}[t_n]$ inside $\mathcal{O}_{\mathbb{Q}(\mathrm{j}_n)}$.

REMARK 1.6. Dorman explicitly computed $\mathcal{D}(\mathbb{Q}(\mathrm{j}_n))$ in [5]. More precisely, he proved in [5, Proposition 5.1] that, for a squarefree positive integer $n \equiv 11 \pmod{24}$,

$$\mathcal{D}(\mathbb{Q}(\mathrm{j}_n)) = \pm \mathfrak{D}_0^{h_n/2} \cdot \mathfrak{D}_1^{(h_n - 2^{t-1})/2}, \tag{1.1}$$

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

where $\mathfrak{t}$ is the number of distinct prime factors of n and $n = \mathfrak{D}_0\mathfrak{D}_1$ with

$$\mathfrak{D}_1 = \begin{cases} 1 & \text{if at least 2 primes congruent to 3 mod 4 divide } n, \\ p & \text{if } p \text{ is the unique prime congruent to 3 mod 4 dividing } n. \end{cases}$$

Note that there is a factor of ± 1 in (1.1), although this factor does not appear in [5, Proposition 5.1], because Dorman computes the absolute value of $\mathcal{D}(\mathbb{Q}(\mathfrak{j}_n))$.

Next, we explicitly determine the sign of $\Delta(\mathcal{P}_n)$.

THEOREM 1.7. *For all positive* $n \equiv 11 \pmod{24}$, $\Delta(\mathcal{P}_n) > 0$ *if and only if*

$$h_n \equiv |\mathrm{Cl}(n)[2]| \pmod 4,$$

where $\mathrm{Cl}(n)[2]$ *is the subgroup of* $\mathrm{Cl}(n)$ *consisting of elements of order at most* 2.

Using the ambiguous class number formula from genus theory, we find that for all positive squarefree integers $n \equiv 11 \pmod{24}$,

$$|\mathrm{Cl}(n)[2]| = 2^{\mathfrak{t}-1},$$

where $\mathfrak{t}$ is the number of distinct prime factors of n. Therefore, we have the following corollary.

COROLLARY 1.8. *For all positive squarefree* $n \equiv 11 \pmod{24}$, $\Delta(\mathcal{P}_n) > 0$ *if and only if*

$$h_n \equiv 2^{\mathfrak{t}-1} \pmod 4,$$

where, as usual, $\mathfrak{t}$ *denotes the number of distinct prime factors of* n.

Moreover, when the ideal class group is a cyclic group, that is $\mathrm{Cl}(n) \cong (\mathbb{Z}/h_n\mathbb{Z})$, which is true for all $n \equiv 11 \pmod{24}$, with $11 \leqslant n \leqslant 995$ as illustrated in Table 2, it is easy to see that

$$|\mathrm{Cl}(n)[2]| = \begin{cases} 1 & \text{if } h_n \text{ is odd}, \\ 2 & \text{if } h_n \text{ is even}. \end{cases}$$

Thus, we have the following corollary.

COROLLARY 1.9. *For all positive* $n \equiv 11 \pmod{24}$, *if* $\mathrm{Cl}(n) \cong (\mathbb{Z}/h_n\mathbb{Z})$, *then* $\Delta(\mathcal{P}_n) > 0$ *if and only if*

$$h_n \equiv 1, 2 \pmod 4.$$

REMARK 1.10. For example, two positive values of $n \equiv 11 \pmod{24}$ for which the ideal class group $\mathrm{Cl}(n) \ncong \mathbb{Z}/h_n\mathbb{Z}$ are 1235 and 2555. In particular, we find that $\mathrm{Cl}(1235) \cong \mathrm{Cl}(2555) \cong (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. The structure of the ideal class group $\mathrm{Cl}(n)$ for positive $n \equiv 11 \pmod{24}$ was computed using Sage [13].

In Table 2, it can be observed that 3 seems to be the only prime that never appears in the prime factorisation of $\Delta(\mathcal{P}_n)$ for positive $n \equiv 11 \pmod{24}$. To prove this, we show that 3 never divides $\Delta(H_n)$, and thus $\Delta(\mathcal{P}_n)$, using Ye's explicit computation of $\Delta(H_n)$

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

TABLE 2. Computation of the class number h_n, the sign $\operatorname{sgn}(\Delta)$ of $\Delta(\mathcal{P}_n)$, the structure of the ideal class group $\mathrm{Cl}(n)$ and the prime factorisation of $|\Delta(\mathcal{P}_n)|$ for all $n \equiv 11 \pmod{24}$ with $11 \leqslant n \leqslant 995$.

n	h_n	$\operatorname{sgn}(\Delta)$	Prime factorisation of $\lvert\Delta(\mathcal{P}_n)\rvert$	$\mathrm{Cl}(n)$
11	1	+	1	$\mathbb{Z}/1\mathbb{Z}$
35	2	+	5	$\mathbb{Z}/2\mathbb{Z}$
59	3	−	59	$\mathbb{Z}/3\mathbb{Z}$
83	3	−	83	$\mathbb{Z}/3\mathbb{Z}$
107	3	−	107	$\mathbb{Z}/3\mathbb{Z}$
131	5	+	$2^4 \times 131^2$	$\mathbb{Z}/5\mathbb{Z}$
155	4	−	$2^4 \times 5^2 \times 31$	$\mathbb{Z}/4\mathbb{Z}$
179	5	+	$2^6 \times 179^2$	$\mathbb{Z}/5\mathbb{Z}$
203	4	−	$2^2 \times 7 \times 29^2$	$\mathbb{Z}/4\mathbb{Z}$
227	5	+	$2^4 \times 227^2$	$\mathbb{Z}/5\mathbb{Z}$
251	7	−	$2^{10} \times 251^3$	$\mathbb{Z}/7\mathbb{Z}$
275	4	−	$2^2 \times 5^3 \times 7^2 \times 11$	$\mathbb{Z}/4\mathbb{Z}$
299	8	−	$2^{14} \times 13^4 \times 23^3 \times 47^2$	$\mathbb{Z}/8\mathbb{Z}$
323	4	−	$2^2 \times 7^2 \times 17^2 \times 19$	$\mathbb{Z}/4\mathbb{Z}$
347	5	+	$2^4 \times 347^2$	$\mathbb{Z}/5\mathbb{Z}$
371	8	−	$2^{20} \times 7^3 \times 17^2 \times 53^4$	$\mathbb{Z}/8\mathbb{Z}$
395	8	−	$2^{18} \times 5^4 \times 13^4 \times 79^3$	$\mathbb{Z}/8\mathbb{Z}$
419	9	+	$2^{22} \times 167^2 \times 419^4$	$\mathbb{Z}/9\mathbb{Z}$
443	5	+	$2^6 \times 7^2 \times 443^2$	$\mathbb{Z}/5\mathbb{Z}$
467	7	−	$2^{12} \times 5^4 \times 467^3$	$\mathbb{Z}/7\mathbb{Z}$
491	9	+	$2^{28} \times 7^2 \times 23^2 \times 491^4$	$\mathbb{Z}/9\mathbb{Z}$
515	6	+	$2^6 \times 5^3 \times 7^2 \times 13^2 \times 103^2$	$\mathbb{Z}/6\mathbb{Z}$
539	8	−	$2^{28} \times 7^7 \times 11^4 \times 13^2$	$\mathbb{Z}/8\mathbb{Z}$
563	9	+	$2^{18} \times 5^4 \times 311^2 \times 563^4$	$\mathbb{Z}/9\mathbb{Z}$
587	7	−	$2^{10} \times 5^4 \times 13^4 \times 587^3$	$\mathbb{Z}/7\mathbb{Z}$
611	10	+	$2^{30} \times 7^2 \times 13^9 \times 47^4$	$\mathbb{Z}/10\mathbb{Z}$
635	10	+	$2^{28} \times 5^5 \times 13^2 \times 127^4 \times 383^2$	$\mathbb{Z}/10\mathbb{Z}$
659	11	−	$2^{40} \times 7^4 \times 191^2 \times 659^5$	$\mathbb{Z}/11\mathbb{Z}$
683	5	+	$2^6 \times 7^2 \times 683^2$	$\mathbb{Z}/5\mathbb{Z}$
707	6	+	$2^8 \times 7^2 \times 13^2 \times 19^2 \times 101^3$	$\mathbb{Z}/6\mathbb{Z}$
731	12	−	$2^{52} \times 17^6 \times 19^2 \times 43^5 \times 263^2 \times 479^2$	$\mathbb{Z}/12\mathbb{Z}$
755	12	−	$2^{38} \times 5^6 \times 41^4 \times 71^2 \times 151^5 \times 503^2$	$\mathbb{Z}/12$
779	10	+	$2^{40} \times 19^8 \times 41^5 \times 311^2$	$\mathbb{Z}/10\mathbb{Z}$
803	10	+	$2^{26} \times 5^4 \times 11^4 \times 19^8 \times 73^5$	$\mathbb{Z}/10\mathbb{Z}$
827	7	−	$2^{12} \times 7^2 \times 13^6 \times 827^3$	$\mathbb{Z}/7\mathbb{Z}$
851	10	+	$2^{44} \times 7^2 \times 13^2 \times 23^4 \times 37^5 \times 167^2$	$\mathbb{Z}/10\mathbb{Z}$
875	10	+	$2^{32} \times 5^{13} \times 7^4 \times 19^2 \times 37^4 \times 89^2$	$\mathbb{Z}/10\mathbb{Z}$
899	14	+	$2^{72} \times 13^2 \times 19^4 \times 29^7 \times 31^6 \times 647^2$	$\mathbb{Z}/14\mathbb{Z}$
923	10	+	$2^{30} \times 5^4 \times 13^5 \times 19^2 \times 61^4 \times 71^4$	$\mathbb{Z}/10\mathbb{Z}$
947	5	+	$2^4 \times 13^2 \times 19^2 \times 947^2$	$\mathbb{Z}/5\mathbb{Z}$
971	15	−	$2^{78} \times 41^4 \times 71^2 \times 503^2 \times 719^2 \times 971^7$	$\mathbb{Z}/15\mathbb{Z}$
995	8	−	$2^{22} \times 5^4 \times 7^2 \times 13^4 \times 19^2 \times 23^2 \times 199^3$	$\mathbb{Z}/8\mathbb{Z}$

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

[14, Corollary 1.2] for squarefree positive integers $n \equiv 11 \pmod{24}$. For more details, see Section 3.4. Therefore, we have the following important theorem.

THEOREM 1.11. *For all positive squarefree $n \equiv 11 \pmod{24}$, we have $3 \nmid \Delta(\mathcal{P}_n)$.*

1.3. Organisation of the manuscript. We start with a section on the necessary preliminaries and prove some important results that will later play a crucial role in the proofs of our main results. Proofs of Theorems 1.3, 1.5, 1.7 and 1.11 are provided in Sections 3.1, 3.2, 3.3 and 3.4, respectively. In Table 2, we have computed the class number and the ideal class group structure of $\mathbb{Q}(\sqrt{-n})$, the prime factorisation and sign of $\Delta(\mathcal{P}_n)$ for all positive integers $n \equiv 11 \pmod{24}$, $11 \leqslant n \leqslant 995$, as an illustration of our main results. Finally, in Section 4, we show that all our main results hold for $n = 227$, as an example. The computations were performed using Sage [13].

2. Preliminaries: nuts and bolts

2.1. The *j*-invariant of a lattice. A *lattice* is an additive subgroup L of $\mathbb{C}$ which is generated by two complex numbers ω_1 and ω_2 that are linearly independent over $\mathbb{R}$. We express this by writing $L = [\omega_1, \omega_2]$. The j-invariant $j(L)$ of a lattice L is the complex number

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2},$$

where

$$g_2(L) = 60 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^4} = 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m\tau + n)^4}$$

and

$$g_3(L) = 140 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^6} = 140 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m\tau + n)^6},$$

where $L = [1, \tau]$ with $\tau \in \mathbb{H}$, the upper-half plane.

PROPOSITION 2.1. *Let L be a lattice, and let $\overline{L}$ denote the lattice obtained by complex conjugation. Then $g_2(\overline{L}) = \overline{g_2(L)}$, $g_3(\overline{L}) = \overline{g_3(L)}$ and $j(\overline{L}) = \overline{j(L)}$.*

PROOF. From the definition of $g_2(L)$,

$$g_2(\overline{L}) = 60 \sum_{\omega \in \overline{L}\setminus\{0\}} \frac{1}{\omega^4} = 60 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\overline{\omega}^4} = \overline{60 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^4}} = \overline{g_2(L)}.$$

A similar argument shows that $g_3(\overline{L}) = \overline{g_3(L)}$ and then the result for j follows from its definition. □

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

We say that two lattices L and L' are *homothetic* if there is a nonzero complex number λ such that $L' = \lambda L$. Note that homothetic lattices have the same j-invariant.

LEMMA 2.2 [4, Theorem 10.9]. *If L and L' are lattices in $\mathbb{C}$, then $j(L) = j(L')$ if and only if the lattices L and L' are homothetic.*

Next, we prove an important result that will later play a crucial role in the proof of Theorem 1.7.

PROPOSITION 2.3. *Let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal, where $\mathcal{O}$ is an order in an imaginary quadratic number field. Then $j(\mathfrak{a})$ is a real number if and only if the class of $\mathfrak{a}$ has order at most 2 in the ideal class group $\mathrm{Cl}(\mathcal{O})$.*

PROOF. Let $\mathfrak{b}$ be the complex conjugate of the ideal $\mathfrak{a}$. From Proposition 2.1, $j(\mathfrak{a})$ is a real number if and only if $j(\mathfrak{a}) = j(\mathfrak{b})$. Now Lemma 2.2 tells us that this is only possible when $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic or, equivalently, when they represent the same ideal classes in the ideal class group $\mathrm{Cl}(\mathcal{O})$. Let $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ denote the ideal class of a proper fractional $\mathcal{O}$-ideal $\mathfrak{c}$. Now using [4, Lemma 7.14(iii)], $[\mathfrak{b}] = [\mathfrak{a}]^{-1}$ for all $\mathfrak{a}$. Therefore,

$$[\mathfrak{a}] = [\mathfrak{b}] \Longleftrightarrow [\mathfrak{a}] = [\mathfrak{a}]^{-1} \Longleftrightarrow [\mathfrak{a}]^2 = [(1)].$$

Note that this is not true as a statement about ideals; here we are explicitly referring to ideal classes, that is, elements of $\mathrm{Cl}(\mathcal{O})$. □

The proposition has the following important corollary.

COROLLARY 2.4. *The j-invariant $j(\mathcal{O})$ is a real number for any order $\mathcal{O}$.*

2.2. Discriminant of an algebraic number field. Let $\mathcal{D}(K)$ denote the discriminant of an algebraic number field K. The discriminant of a nonzero finitely generated $\mathbb{Z}$-submodule $\mathfrak{M}$ of a number field K is defined as

$$\mathcal{D}(\mathfrak{M}) = \mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

where $\mathfrak{M} = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$ and spans K as a $\mathbb{Q}$-vector space.

PROPOSITION 2.5 [10, Proposition 2.12]. *If $\mathfrak{M} \subset \mathfrak{M}'$ are two nonzero finitely generated $\mathbb{Z}$-submodules of a number field K that span K as a $\mathbb{Q}$-vector space, then the index $[\mathfrak{M}' : \mathfrak{M}]$ is finite and*

$$\mathcal{D}(\mathfrak{M}) = [\mathfrak{M}' : \mathfrak{M}]^2 \mathcal{D}(\mathfrak{M}').$$

REMARK 2.6. Although Neukirch [10, Proposition 2.12] only states Proposition 2.5 for finitely generated $\mathcal{O}_K$-submodules, the same result and proof also hold more generally for finitely generated $\mathbb{Z}$-submodules.

2.3. Number fields $\mathbb{Q}(\mathfrak{j}_n)$ and $\mathbb{Q}(t_n)$. The main goal of this section is to show that the fields $\mathbb{Q}(\mathfrak{j}_n)$ and $\mathbb{Q}(t_n)$ are the same. This important result enables us to prove our main theorem, Theorem 1.5, in a very efficient way, as explained in Section 3.2.

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

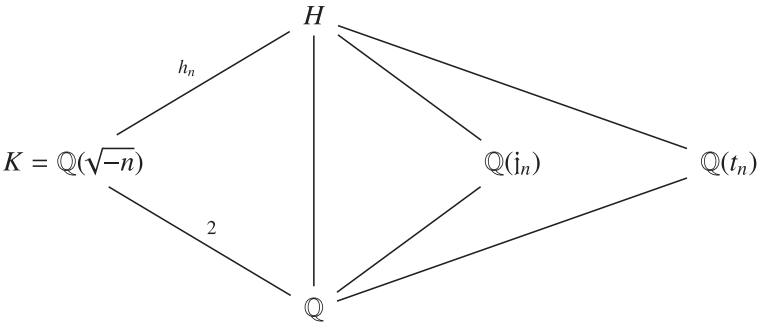

FIGURE 1. Field diagram 1.

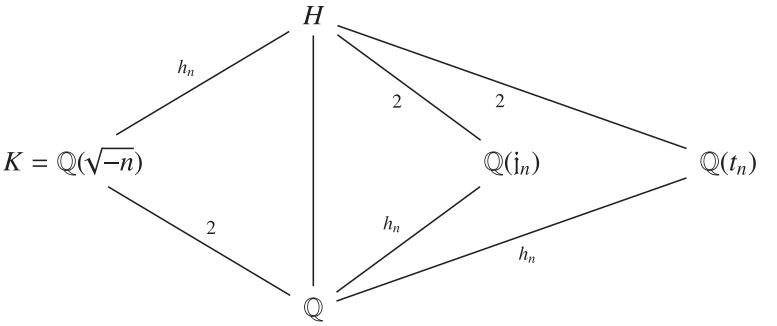

FIGURE 2. Field diagram 2.

PROPOSITION 2.7. *For all positive integers* $n \equiv 11 \pmod{24}$, *we have* $\mathbb{Q}(\mathfrak{j}_n) = \mathbb{Q}(t_n)$.

PROOF. To start with, consider the field diagram in Figure 1. We freely use some standard facts about the ring class fields of K throughout the proof. From class field theory, recall that if H is the ring class field associated to the discriminant of order $-n$, then H is a finite Galois extension of K and $[H : K] = h_n$, where h_n denotes the class number of the order of discriminant $-n$. Therefore, we have $[H : K] = [H : \mathbb{Q}(\sqrt{-n})] = h_n$. Next, it is easy to see that $[K : \mathbb{Q}] = 2$ since $\{1, i\sqrt{n}\}$ forms a basis. Moreover, since $H = (\mathbb{Q}(\mathfrak{j}_n))(\sqrt{-n})$, we have $[H : \mathbb{Q}(\mathfrak{j}_n)] \leqslant 2$. Therefore, using the tower law, either $[\mathbb{Q}(\mathfrak{j}_n) : \mathbb{Q}] = h_n$ or $[\mathbb{Q}(\mathfrak{j}_n) : \mathbb{Q}] = 2h_n$. Now let $\mathfrak{f}$ be the minimal polynomial of $\mathfrak{j}_n \in H$ over K. Note that $\mathfrak{f} \in K[x]$ has degree h_n. From Corollary 2.4, $\mathfrak{j}_n \in \mathbb{R}$, that is, $\overline{\mathfrak{j}_n} = \mathfrak{j}_n$. Thus, $\bar{\mathfrak{f}} = \mathfrak{f}$, which implies $\mathfrak{f} \in \mathbb{Q}[x]$, and we deduce that $[\mathbb{Q}(\mathfrak{j}_n) : \mathbb{Q}] \leqslant h_n$.

Putting all this together finally produces $[\mathbb{Q}(\mathfrak{j}_n) : \mathbb{Q}] = h_n$ and $[H : \mathbb{Q}(\mathfrak{j}_n)] = 2$. Since $t_n \in \mathbb{R}$, which easily follows from Ramanujan's definition of t_n, a similar argument can be applied to show that $[\mathbb{Q}(t_n) : \mathbb{Q}] = h_n$ and $[H : \mathbb{Q}(t_n)] = 2$.

The above discussion can be summarised by Figure 2.

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

Now observe that we have the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\mathfrak{j}_n) \subseteq \mathbb{Q}(t_n) \subseteq H$, where $\mathbb{Q}(\mathfrak{j}_n) \subseteq \mathbb{Q}(t_n)$ follows from Proposition 1.2. Therefore, by the tower law,

$$[\mathbb{Q}(t_n) : \mathbb{Q}(\mathfrak{j}_n)][H : \mathbb{Q}(t_n)] = [H : \mathbb{Q}(\mathfrak{j}_n)] \Longrightarrow [\mathbb{Q}(t_n) : \mathbb{Q}(\mathfrak{j}_n)] = 1,$$

which is only possible when $\mathbb{Q}(\mathfrak{j}_n) = \mathbb{Q}(t_n)$. This completes the proof. □

3. Proofs of the main results

3.1. Proof of Theorem 1.3. Since $t_n \in \mathbb{Z}[t_n]$ and the constant term of $\mathcal{P}_n$ is always ± 1 (see [8, Section 3], where it is shown that t_n is a unit), it follows that $t_n^{-1} \in \mathbb{Z}[t_n]$. From Proposition 1.2,

$$\mathfrak{j}_n = (t_n^6 - 27t_n^{-6} - 6)^3.$$

Therefore, $\mathfrak{j}_n \in \mathbb{Z}[t_n]$ and thus $\mathbb{Z}[\mathfrak{j}_n] \subseteq \mathbb{Z}[t_n]$. Substituting $\mathfrak{M} = \mathbb{Z}[\mathfrak{j}_n]$ and $\mathfrak{M}' = \mathbb{Z}[t_n]$ in Proposition 2.5 produces

$$\mathcal{D}(\mathbb{Z}[\mathfrak{j}_n]) = \mathcal{D}(\mathbb{Z}[t_n])[\mathbb{Z}[t_n] : \mathbb{Z}[\mathfrak{j}_n]]^2$$

or, equivalently,

$$\Delta(H_n) = \Delta(\mathcal{P}_n)[\mathbb{Z}[t_n] : \mathbb{Z}[\mathfrak{j}_n]]^2,$$

which is the desired result.

3.2. Proof of Theorem 1.5. First, simply notice that

$$\mathbb{Z}[t_n] \subseteq O_{\mathbb{Q}(t_n)} = O_{\mathbb{Q}(\mathfrak{j}_n)} \subseteq \mathbb{Q}(\mathfrak{j}_n),$$

where $O_{\mathbb{Q}(t_n)} = O_{\mathbb{Q}(\mathfrak{j}_n)}$ follows from the fact that $\mathbb{Q}(\mathfrak{j}_n) = \mathbb{Q}(t_n)$, as shown in Proposition 2.7. As in the previous proof, substituting $\mathfrak{M} = \mathbb{Z}[t_n]$ and $\mathfrak{M}' = O_{\mathbb{Q}(\mathfrak{j}_n)}$ in Proposition 2.5 gives the desired result.

3.3. Proof of Theorem 1.7. From the definition of the ring class polynomial, its roots are

$$\{j(\mathfrak{a}) \mid \mathfrak{a} \in \mathrm{Cl}(n)\}.$$

From Proposition 2.3, we deduce that the real roots of the ring class polynomial H_n are given by

$$\{j(\mathfrak{a}) \mid \mathfrak{a} \in \mathrm{Cl}(n), \text{order of } \mathfrak{a} \text{ at most } 2\},$$

which is in bijection with $\mathrm{Cl}(n)[2]$.

Therefore, the number of nonreal roots of H_n is given by $|\mathrm{Cl}(n)| - |\mathrm{Cl}(n)[2]| = h_n - |\mathrm{Cl}(n)[2]|$. The discriminant of a polynomial in $\mathbb{Q}$ is positive if and only if the

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

number of nonreal roots of the polynomial is divisible by 4. Putting all this together completes the proof.

3.4. Proof of Theorem 1.11. Assume that n is a positive squarefree integer. Ye [14, Corollary 1.2] computed the discriminant of the ring class polynomials H_n as

$$\log|\Delta(H_n)| = -\frac{h_K}{4}\sum_{\substack{[\mathfrak{a}]\in \mathrm{Cl}_K\\ [\mathfrak{a}]\neq[O_K]}}\sum_{\ell=0}^{n-1}\sum_{X,Y=-\infty}^{\infty}\kappa\Big(1-\frac{n(2AX+BY)^2+(nY-2A\ell)^2}{4An}, \frac{B\ell}{n}f_1^{(\mathfrak{a})}-\frac{2A\ell}{n}f_2^{(\mathfrak{a})}+L_-^{(\mathfrak{a})}\Big),$$

where h_K denotes the class number of $K=\mathbb{Q}(\sqrt{-n})$, $L_-^{(\mathfrak{a})}$ denotes the lattice $\mathbb{Z}f_1^{(\mathfrak{a})}+\mathbb{Z}f_2^{(\mathfrak{a})}$,

$$\mathfrak{a}=\Big[A,\frac{B+\sqrt{-n}}{2}\Big],\quad f_1^{(\mathfrak{a})}=\begin{pmatrix}-1 & B\\ 0 & A\end{pmatrix},\quad f_2^{(\mathfrak{a})}=\begin{pmatrix}0 & C\\ 1 & 0\end{pmatrix},$$

$$\kappa(m,\mu)=-\frac{1}{h_K}\sum_{q\,\text{inert}}\xi_q(m,\mu)(\mathrm{ord}_q(m)+1)\rho_K\Big(\frac{mn}{q}\Big)\log q - \frac{\rho_K(mn)}{h_K}\sum_{q|n}\xi_q(m,\mu)\,\mathrm{ord}_q(mn)\log q, \tag{3.1}$$

and ξ_q and ρ_K are the functions defined in [14, Corollary 1.2].

To prove Theorem 1.11, we will show that $\log 3$ never appears in $\kappa(m,\mu)$ for any choice of parameters m and μ. From the definition of $\kappa(m,\mu)$, it suffices to prove that 3 always splits in $\mathbb{Q}(\sqrt{-n})$ and does not divide n for all positive squarefree $n\equiv 11 \pmod{24}$.

Recall that a prime number $\mathfrak{p}$ splits in the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$ if and only if $-n$ is a nonzero quadratic residue mod $\mathfrak{p}$. The quadratic residues mod 3 are 0 and 1, and it is easy to see that when $n\equiv 11 \pmod{24}$, we have $-n\equiv 1 \pmod 3$. Thus $-n$ is a nonzero quadratic residue mod 3 for all positive squarefree integers $n\equiv 11 \pmod{24}$. This completes the proof.

4. An illustration of the main results

EXAMPLE 4.1. Take $n=227$. From [7, Table 1],

$$\mathcal{P}_{227}(z)=z^5-5z^4+9z^3-9z^2+9z-1.$$

Since 227 is squarefree, the degree of $\mathcal{P}_{227}$ is equal to the class number of $\mathbb{Q}(\sqrt{-227})$; thus, $h_{227}=5$. The class group structure of $\mathbb{Q}(\sqrt{-227})$, computed using Sage, is $\mathbb{Z}/5\mathbb{Z}$ (see Table 2). By Corollary 1.9, $\Delta(\mathcal{P}_{227})>0$, since $h_{227}=5\equiv 1 \pmod 4$. From Table 2, $\Delta(\mathcal{P}_{227})=2^4\cdot 227^2$. Moreover, using the Sage database for ring class polynomials and their discriminants [13], it can be found that

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press

$$\begin{aligned} H_{227}(z) = {} & z^5 + 360082897644683264000z^4 \\ & - 256232700283296153600000000z^3 \\ & + 182273408079389937945804800000000000z^2 \\ & - 211111820346082162271846400000000000000z \\ & + 508547219321654402770534400000000000000000, \end{aligned}$$

and

$$\Delta(H_{227}) = 2^{316} \cdot 5^{60} \cdot 13^{20} \cdot 17^{20} \cdot 31^4 \cdot 37^6 \cdot 41^4 \cdot 61^4 \cdot 83^2 \cdot 151^2 \cdot 179^2 \cdot 191^2 \cdot 199^2 \cdot 227^2.$$

Therefore,

$$\frac{\Delta(H_{227})}{\Delta(\mathcal{P}_{227})} = (2^{156} \cdot 5^{30} \cdot 13^{10} \cdot 17^{10} \cdot 31^2 \cdot 37^3 \cdot 41^2 \cdot 61^2 \cdot 83 \cdot 151 \cdot 179 \cdot 191 \cdot 199)^2,$$

which is in accord with Theorem 1.3, since the quotient is a perfect square.

By Theorem 1.5, $\mathcal{D}(\mathbb{Q}(\mathrm{j}_{227})) > 0$ since $\Delta(\mathcal{P}_{227}) > 0$, as already seen above and in Table 2. From Remark 1.6, $\mathfrak{D}_0 = 1$, $\mathfrak{D}_1 = 227$, $\mathrm{t} = 1$, and thus

$$\mathcal{D}(\mathbb{Q}(\mathrm{j}_{227})) = 227^2 \mid 2^4 \cdot 227^2 = \Delta(\mathcal{P}_{227}).$$

Notice that 3 does not appear in the prime factorisation of $\Delta(\mathcal{P}_{227})$ and $\Delta(H_{227})$.

5. Concluding remarks and further research

We can now replace the ring class polynomials H_n and their discriminants $\Delta(H_n)$ with the Ramanujan polynomials $\mathcal{P}_n$ and their discriminants $\Delta(\mathcal{P}_n)$ to simplify computations wherever needed. Ramanujan polynomials $\mathcal{P}_n$ can be used in the generation of special curves, such as MNT curves [9, 12], and in the generation of elliptic curves that do not necessarily have prime order [1].

Problems such as primality testing and proving [1], the generation of elliptic curve parameters [8] and the representability of primes by quadratic forms [4] could be considerably advanced once we know more about Ramanujan polynomials $\mathcal{P}_n$ and their discriminants and traces.

Acknowledgements

The majority of this research was done during the Research Science Institute (RSI) at MIT in the summer of 2022. First, I would like to thank my research mentor Alan Peng for his invaluable mentorship, constant encouragement, guidance and support. Next, I would like to thank Andrew Sutherland for suggesting this problem and the MIT Math Department for making this research project possible. I am grateful and indebted to the RSI, CEE and MIT for their hospitality and support during the preparation of this work. Finally, I would like to thank the referee for helpful comments, and for pointing out several mistakes in the earlier version of the paper.

References

[1] A. O. L. Atkin and F. Morain, 'Elliptic curves and primality proving', *Math. Comp.* **61** (1993), 29–68.
[2] B. C. Berndt and H. H. Chan, 'Ramanujan and the modular j-invariant', *Canad. Math. Bull.* **42**(4) (1999), 427–440.
[3] R. Bröker and P. Stevenhagen, 'Efficient CM-constructions of elliptic curves over finite fields', *Math. Comp.* **76** (2007), 2161–2179.
[4] D. A. Cox, *Primes of the Form* $x^2 + ny^2$, 2nd edn (John Wiley and Sons, Hoboken, NJ, 2013).
[5] D. R. Dorman, 'Singular moduli, modular polynomials, and the index of the closure of $\mathbb{Z}[j(\tau)]$ in $\mathbb{Q}(j(\tau))$', *Math. Ann.* **283** (1989), 177–191.
[6] B. H. Gross and D. B. Zagier, 'On singular moduli', *J. reine angew. Math.* **355** (1985), 191–220.
[7] E. Konstantinou and A. Kontogeorgis, 'Computing polynomials of the Ramanujan t_n class invariants', *Canad. Math. Bull.* **52**(4) (2009), 583–597.
[8] E. Konstantinou and A. Kontogeorgis, 'Ramanujan's class invariants and their use in elliptic curve cryptography', *Comput. Math. Appl.* **59**(8) (2010), 2901–2917.
[9] A. Miyaji, M. Nakabayashi and S. Takano, 'New explicit conditions of elliptic curve traces for FR-reduction', *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.* **E84-A**(5) (2001), 1234–1243.
[10] J. Neukirch, *Algebraic Number Theory* (Springer, Berlin–Heidelberg, 1999).
[11] S. Ramanujan, *Notebooks*, Vols. 1, 2 (TIFR, Bombay, 1957).
[12] M. Scott and P. S. L. M. Barreto, 'Generating more MNT elliptic curves', *Des. Codes Cryptogr.* **38** (2006), 209–217.
[13] W. Stein, Sage Mathematics Software, Sage Development Team (2021). Available online at http://www.sagemath.org.
[14] D. Ye, 'Revisiting the Gross–Zagier discriminant formula', *Math. Nachr.* **293** (2020), 1801–1826.

SARTH CHAVAN, Department of Mathematics,
Massachusetts Institute of Technology, Cambridge, MA, USA
e-mail: schavan@mit.edu, sarth5002@outlook.com

https://doi.org/10.1017/S0004972723000278 Published online by Cambridge University Press