Computers and Mathematics with Applications 59 (2010) 2901–2917

Contents lists available at ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa

Ramanujan's class invariants and their use in elliptic curve cryptography

Elisavet Konstantinou [a,*], Aristides Kontogeorgis [b]

[a] Department of Information and Communication Systems Engineering, University of the Aegean, 83200, Samos, Greece
[b] Department of Mathematics, University of the Aegean, 83200, Samos, Greece

ARTICLE INFO

Article history:
Received 10 November 2009
Received in revised form 9 February 2010
Accepted 10 February 2010

Keywords:
Generation of elliptic curves
Complex Multiplication
Class polynomials

ABSTRACT

The Complex Multiplication (CM) method is a method frequently used for the generation of elliptic curves (ECs) over a prime field $\mathbb{F}_p$. The most demanding and complex step of this method is the computation of the roots of a special type of class polynomials, called Hilbert polynomials. However, there are several polynomials, called class polynomials, which can be used in the CM method, having much smaller coefficients, and fulfilling the prerequisite that their roots can be easily transformed to the roots of the corresponding Hilbert polynomials.

In this paper, we propose the use of a new class of polynomials which are derived from Ramanujan's class invariants t_n. We explicitly describe the algorithm for the construction of the new polynomials and give the necessary transformation of their roots to the roots of the corresponding Hilbert polynomials. We provide a theoretical asymptotic bound for the bit precision requirements of all class polynomials and, also using extensive experimental assessments, we compare the efficiency of using the new polynomials against the use of the other class polynomials. Our comparison shows that the new class of polynomials clearly surpass all of the previously used polynomials when they are used in the generation of prime order elliptic curves.

1. Introduction

Since its introduction in 1985, elliptic curve cryptography has come to be seen as an attractive alternative to conventional public key cryptosystems, allowing the development of fast and memory efficient cryptographic algorithms. However, before the deployment of an elliptic curve cryptosystem, a *cryptographically* secure elliptic curve must be chosen in order to guarantee the robustness of the cryptosystem against all (currently) known attacks (e.g. [1–4]). All these attacks can be avoided if the order of the EC possesses certain properties. An equally important alternative to cryptographic robustness (see e.g., [5]) requires that the order of the EC generated is a prime number. It is clear that the generation of cryptographically secure elliptic curves over prime fields is one of the most fundamental and complex problems in elliptic curve cryptography. The methods most commonly used for the generation of ECs over prime fields are the Complex Multiplication (CM) method [6,7] and the point counting method [8]. In this paper we will follow the first approach.

The most complex and demanding step of the CM method is the computation of a class polynomial, called a Hilbert polynomial, whose roots are then used directly for the construction of the EC parameters. These polynomials are uniquely determined by a (positive) parameter D called the CM discriminant, which is congruent to 0, 3 (mod 4). In particular, for the construction of prime order ECs, the CM discriminant must be congruent to 3 (mod 8). The disadvantage of Hilbert

* Corresponding author.
E-mail addresses: ekonstantinou@aegean.gr (E. Konstantinou), kontogar@aegean.gr (A. Kontogeorgis).

0898-1221/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2010.02.008

polynomials is that their coefficients grow very large as the value of the discriminant D increases and thus their construction requires high precision arithmetic. To overcome these shortcomings of Hilbert polynomials, we can use other classes of polynomials which have much smaller coefficients and their use can considerably improve the efficiency of the whole CM method. In the literature, three kinds of these polynomials are proposed: Weber polynomials [9], $M_{D,l}(x)$ polynomials [10] and double-eta polynomials (we will denote them by $M_{D,p_1,p_2}(x)$) [11]. The logarithmic heights of the coefficients of the Weber, $M_{D,l}(x)$ and $M_{D,p_1,p_2}(x)$ polynomials are smaller by a constant factor than the corresponding logarithmic heights of the Hilbert polynomials and this is the reason for their much more efficient construction.

Our contribution. Srinivasa Ramanujan (1887–1920) defined in his third notebook, pages 392 and 393 in the pagination of [12, vol. 2], the values of five class polynomials for five different values of the discriminant D. The simplicity and the small coefficients of these polynomials were remarkable. In 1999 Bruce C. Berndt and Heng Huat Chan [13] proved that if D is square-free and $D \equiv 11 \mod 24$ then the roots of these five polynomials are real units and can generate the Hilbert class field. Moreover, they asked for an efficient way of computing these polynomials for every discriminant D (and not only for the five values computed by Ramanujan). In the rest of the paper, we will call them *Ramanujan polynomials*. Interpreting the theorem of Berndt and Chan (that the roots of the Ramanujan polynomials can generate the Hilbert class field for values $D \equiv 11 \mod 24$), we see that Ramanujan polynomials can be used in the CM method, as the aforementioned theorem proves that there is a transformation of their roots to the roots of the corresponding Hilbert polynomials. In addition, as $D \equiv 11 \bmod 24 \equiv 3 \bmod 8$, Ramanujan polynomials can also be used in the generation of prime order ECs.

In this paper, we introduce for the first time the use of Ramanujan polynomials in the CM method by providing an efficient algorithm for their construction for all values of the discriminant. The theory behind this construction is based on the Shimura Reciprocity Law [14,15], and mathematical proofs behind it are presented in [16]. In the context of this paper we present a new, simplified and much more efficient construction method for the polynomials which avoids the use of matrices (as in [16]) and is based solely on quadratic forms. The new construction method resembles the corresponding methods for all other class polynomials using modular functions under the conditions of the quadratic forms. We observe that Ramanujan polynomials have the same degree as their corresponding Hilbert polynomials and we provide the necessary transformation of a Ramanujan polynomial root to a root of the corresponding Hilbert polynomial. The new construction algorithm, together with the transformation formula, gives all the necessary information that a practitioner needs in order to use the new class of polynomials in the CM method.

Beside the introduction of the new class polynomials, we give an asymptotic bound for the logarithmic height of the Weber, $M_{D,l}(x)$, $M_{D,p_1,p_2}(x)$ and Ramanujan polynomials and prove theoretically that this bound does not depend solely on the height of the corresponding class invariants that generate the particular polynomials. For example, it can be shown that when $D \equiv 3 \pmod 8$, the logarithmic heights of the corresponding Weber polynomials are three times larger than the logarithmic heights of the Weber polynomials when $D \equiv 7 \pmod 8$ even though similar class invariants are used for the two cases. The logarithmic height of the polynomials is equal to the bit precision required for their construction. Thus, the asymptotic bounds of the logarithmic heights can be used as an estimation for the precision requirements of all polynomials. Obviously, this information is very crucial for anyone who wants to construct the polynomials.

Finally, we perform a comparative theoretical and experimental study as regards the efficiency of using the aforementioned Weber, $M_{D,l}(x)$ and $M_{D,p_1,p_2}(x)$ polynomials, against the new class of polynomials. We show that Ramanujan polynomials are by far the best choice when the CM method is used for the generation of prime order elliptic curves since their construction is more efficient than the construction of all previously used polynomials. We show that the logarithmic heights of the coefficients of the Ramanujan polynomials are asymptotically 36 times smaller than the logarithmic heights of the Hilbert polynomials and this allows us to show that the precision requirements for the construction of Ramanujan polynomials can be from 22% to 66% smaller than the precision requirements for all other class polynomials.

Ramanujan polynomials can also be used in the generation of special curves, such as MNT curves [17,18], and in the generation of ECs that do not necessarily have prime order [6,7]. In the case where non-prime order elliptic curves are constructed, the best known class invariant is the one used for the construction of Weber polynomials with $D \not\equiv 0 \pmod 3$ and $D \equiv 7 \pmod 8$. However, our experiments indicated that this is not always true and the choice of Ramanujan polynomials can be more advantageous in many cases. Moreover, problems such as primality testing/proving [6] and the representability of primes by quadratic forms [19] can be considerably improved with the use of Ramanujan polynomials. This makes our analysis for these polynomials even more useful.

The rest of the paper is organized as follows. In Section 2 we review some basic definitions and facts about the CM method and class polynomials. In Section 3 we elaborate on the construction of Ramanujan polynomials, describing in an explicit way how they can be used in the CM method. In Section 4 we provide theoretical estimations for the precision requirements of all previously mentioned class polynomials, in Section 5 we present our experimental results and we give our conclusions in Section 6.

2. Complex multiplication and class polynomials

In this section we give a brief introduction to elliptic curve theory, the Complex Multiplication (CM) method and class polynomials. Our aim is to facilitate the reading of the sections that follow.

2.1. Elliptic curve theory and complex multiplication

An *elliptic curve* over a finite field $\mathbb{F}_p$, p a prime larger than 3, is denoted by $E(\mathbb{F}_p)$ and it is comprised of all the points $(x, y) \in \mathbb{F}_p$ (in affine coordinates) such that

$$y^2 = x^3 + ax + b, \tag{1}$$

with $a, b \in \mathbb{F}_p$ satisfying $4a^3 + 27b^2 \neq 0$. These points, together with a special point denoted by $\mathcal{O}$ (the *point at infinity*) and a properly defined addition operation form an Abelian group. This is the *elliptic curve group* and the point $\mathcal{O}$ is its zero element (see [20–22] for more details on this group). The *order*, denoted by m, is the number of points that belong in $E(\mathbb{F}_p)$.

Among the most important quantities defined for an elliptic curve $E(\mathbb{F}_p)$ are the *curve discriminant* Δ and the *j-invariant*. These two quantities are given by the equations $\Delta = -16(4a^3 + 27b^2)$ and $j = -1728(4a)^3/\Delta$. Given a j-invariant $j_0 \in \mathbb{F}_p$ (with $j_0 \neq 0$, 1728) *two* ECs can be constructed. If $k = j_0/(1728 - j_0) \bmod p$, one of these curves is given by Eq. (1) by setting $a = 3k \bmod p$ and $b = 2k \bmod p$. The second curve (the *twist* of the first) is given by the equation $y^2 = x^3 + ac^2x + bc^3$ with c any quadratic non-residue of $\mathbb{F}_p$. If m_1 and m_2 denote the orders of an elliptic curve and its twist respectively, then $m_1 + m_2 = 2p + 2$ which implies that if one of the curves has order $p + 1 - t$, then its twist has order $p + 1 + t$, or vice versa (see [21, Lemma VIII.3]). Finding a suitable j-invariant for a curve that has a given order m can be accomplished through the theory of *Complex Multiplication* (CM) of elliptic curves over the rationals. This method is called the *CM method* and in what follows we will give a brief account of it.

Given a prime p, the smallest, positive square-free D is chosen for which there exists some integer u such that the equation $4p = u^2 + Dv^2$ holds. The negative parameter $-D$ is called a *CM discriminant for the prime p*. For convenience throughout the paper, we will use (the positive integer) D to refer to the CM discriminant. The CM method uses D to determine a j-invariant. This j-invariant, in turn, will lead to the construction of an EC of order $p + 1 - u$ or $p + 1 + u$. If neither of the possible orders $p + 1 - u$ and $p + 1 + u$ is suitable for our purposes, the process is repeated with a new D. If at least one of these orders is suitable, then the method proceeds with the construction of the *Hilbert polynomial* (uniquely defined by D) and the determination of its roots modulo p. Any root of the Hilbert polynomial can be used as a j-invariant. From this root the corresponding EC and its twist can be constructed. In order to find which one of the curves has the desired suitable order ($m = p + 1 - u$ or $m = p + 1 + u$), Lagrange's theorem can be used as follows: we repeatedly choose points P at random in each EC until a point is found in one of the curves for which $mP \neq \mathcal{O}$. This implies that the curve that we seek is the other one. Recently, different methods have been proposed for choosing efficiently the correct elliptic curve in the CM method [23,24]. If the order m should be a prime number, then it is obvious that u should be odd. It is also easy to show that D must be congruent to 3 mod 8 and v should be odd, too.

The most demanding step of the CM method is the construction of the Hilbert polynomial, as it requires high precision floating point and complex arithmetic. As the value of the discriminant D increases, the coefficients of the polynomials grow extremely large and their computation becomes more inefficient. If we could find a way to compute the roots of the Hilbert polynomials directly, it is clear that it wouldn't be necessary to construct the polynomials (since only their roots are needed in the CM method). Indeed, there are polynomials (known as class polynomials) [25,26,9], with much smaller coefficients, which can be constructed much more efficiently than Hilbert polynomials and their roots can be transformed to the roots of the Hilbert polynomials. Thus, we can replace the Hilbert polynomials in the CM method with another class of polynomials given that their roots can be transformed to the roots of the Hilbert polynomials. In the following section we will briefly review the definition of these polynomials, while in Section 3 we will propose the use of a new class of polynomials.

2.2. Class polynomials

Beside Hilbert polynomials, other class polynomials can be used in the CM method. In the literature, three kinds of these polynomials are proposed: Weber polynomials [9], $M_{D,l}(x)$ polynomials [10] and double-eta polynomials (we will denote them by $M_{D,p_1,p_2}(x)$) [11]. In what follows, we will briefly review the definitions of these polynomials.

2.2.1. Hilbert polynomials

Every CM discriminant D defines a unique Hilbert polynomial, denoted by $H_D(x)$. Given a positive D, the Hilbert polynomial $H_D(x) \in \mathbb{Z}[x]$ is defined as

$$H_D(x) = \prod_{\tau} (x - j(\tau)) \tag{2}$$

for values of τ satisfying $\tau = (-\beta + \sqrt{-D})/2\alpha$, for all integers α, β, and γ such that (i) $\beta^2 - 4\alpha\gamma = -D$, (ii) $|\beta| \leq \alpha \leq \sqrt{D/3}$, (iii) $\alpha \leq \gamma$, (iv) $\gcd(\alpha, \beta, \gamma) = 1$, and (v) if $|\beta| = \alpha$ or $\alpha = \gamma$, then $\beta \geq 0$. The 3-tuple of integers $[\alpha, \beta, \gamma]$ that satisfies these conditions is called a *primitive, reduced quadratic form* of $-D$, with τ being a root of the quadratic equation $\alpha z^2 + \beta z + \gamma = 0$. Clearly, the set of primitive reduced quadratic forms of a given discriminant is finite. The quantity $j(\tau)$ in Eq. (2) is called *class invariant* and is defined as follows. Let $z = e^{2\pi\sqrt{-1}\tau}$ and $h(\tau) = \left(\frac{\eta(2\tau)}{\eta(\tau)}\right)^{24}$, where $\eta(\tau) = z^{1/24}\prod_{n=1}^{\infty}(1 - z^n)$ is the Dedekind eta function. Then, $j(\tau) = \frac{(256h(\tau)+1)^3}{h(\tau)}$.

2.2.2. Weber polynomials

Weber polynomials are defined using the Weber functions $f(\tau) = \zeta_{48}^{-1}\frac{\eta((\tau+1)/2)}{\eta(\tau)}$, $f_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)}$ and $f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}$ where $\zeta_{48} = e^{2\pi i/48}$. Then, the Weber polynomial $W_D(x)$ is defined as

$$W_D(x) = \prod_{\ell=1}^{h'}(x - g(\tau_\ell))$$

where $g(\tau_\ell)$ (a class invariant of $W_D(x)$) is an expression – depending on the value of D – for the Weber functions, τ_ℓ satisfies the equation $a_\ell z^2 + 2b_\ell z + c_\ell = 0$ and h' is the degree of the polynomial. This quadratic equation corresponds to a primitive reduced quadratic form $[a_\ell, 2b_\ell, c_\ell]$ for which $4b_\ell^2 - 4a_\ell c_\ell = -4d$, where $d = D/4$ if $D \equiv 4, 8 \pmod{16}$, and $d = D$ if $D \equiv 3 \pmod 4$ and (i) $\gcd(a_\ell, b_\ell, c_\ell) = 1$, (ii) $|2b_\ell| \le a_\ell \le c_\ell$, and (iii) if either $a_\ell = |2b_\ell|$ or $a_\ell = c_\ell$, then $b_\ell \ge 0$. In particular, $g(\tau_\ell)$ is constructed using the following equation given in [27]:

$$g(\tau_\ell) = \left[N \exp\left(\frac{-\pi\sqrt{-1}KLb_\ell}{24}\right) 2^{-I/6}\left(f_J(\tau_\ell)\right)^K\right]^G$$

where $J \in \{0, 1, 2\}$, $f_0(\tau_\ell) = f(\tau_\ell)$, $G = \gcd(D, 3)$, $I, K \in [0, 6]$, and L, N are positive integers. The precise values of these parameters depend on certain, rather tedious, conditions among a_ℓ, c_ℓ and D that encompass the various cases of the mathematical definition of the Weber polynomials; the interested reader can find all the details in [27].

There are ten cases of the discriminant D that define ten different class invariants and consequently ten class polynomials. Recall that D is either 3 (mod 4) or 4, 8 (mod 16) and that $d = D/4$ if $D \equiv 0 \pmod 4$, and $d = D$ if $D \equiv 3 \pmod 4$. This in turn implies that $d \equiv 3, 7 \pmod 8$ if $D \equiv 3 \pmod 4$, while $d \equiv 1, 2, 5, 6 \pmod 8$ when $D \equiv 4, 8 \pmod{16}$. The ten class invariants split into two groups of five each, depending on whether $D \not\equiv 0 \pmod 3$ or $D \equiv 0 \pmod 3$. Finally, we note that the degree h' of $W_D(x)$ is equal to the degree of the corresponding Hilbert polynomial for all cases of $D \not\equiv 3 \pmod 8$. When $D \equiv 3 \pmod 8$ the degree of Weber polynomials is *three* times larger than the degree of the corresponding Hilbert polynomials. This is why these values of D are usually avoided in the generation of ordinary ECs. However, when we want to construct *prime order* ECs [5], it is necessary that $D \equiv 3 \pmod 8$.

2.2.3. $M_{D,l}(x)$ polynomials

Another class of polynomials was proposed in [10], referred to as the $M_{D,l}(x)$ polynomials. These polynomials have degree equal to the degree of their corresponding Hilbert polynomials and are constructed from a family of η-products: $m_l(z) = \frac{\eta(z/l)}{\eta(z)}$ for an integer $l \in \{3, 5, 7, 13\}$. The polynomials are obtained from this family by evaluating their values for a suitably chosen system of quadratic forms. Once a polynomial is computed, we can use a modular equation in order to compute a root modulo p of the Hilbert polynomial from a root modulo p of the $M_{D,l}(x)$ polynomial.

The polynomials $M_{D,l}(x) \in \mathbb{Z}[x]$ for $D \equiv 0 \pmod l$ are defined as

$$M_{D,l}(x) = \prod_{\tau_Q}(x - m_l^e(\tau_Q))$$

where $\tau_Q = \frac{-B_i+\sqrt{-D}}{2A_i}$ for all representatives $S = \{(A_i, B_i, C_i)\}_{1\le i\le h}$ of the reduced primitive quadratic forms of a discriminant $-D$ derived from the l-system. Details on the construction of the invariants $m_l^e(\tau_Q)$ can be found in [25,10]. The invariants $m_l^e(\tau_Q)$ are related to $j(\tau)$ through the corresponding modular equations $\Phi_l(m_l^e(\tau_Q), j(\tau)) = 0$ [10]. Since $M_{D,l}(x)$ polynomials have roots R_M modulo p, we use an algorithm for their computation (for example Berlekamp's algorithm [28]) and then we can compute the roots R_H modulo p of the corresponding Hilbert polynomial $H_D(x)$ from the modular equation $\Phi_l(R_M, R_H) = 0$.

2.2.4. $M_{D,p_1,p_2}(x)$ polynomials

The authors of [11] proposed the use of another class of polynomials. Like $M_{D,l}(x)$ polynomials, these polynomials are constructed using a family of η-products: $m_{p_1,p_2}(z) = \frac{\eta(z/p_1)\eta(z/p_2)}{\eta(z/(p_1p_2))\eta(z)}$, where p_1, p_2 are primes. We will refer to the minimal polynomials of these products (powers of which generate the Hilbert class field and are called class invariants like $j(\tau)$) as $M_{D,p_1,p_2}(x)$ where D is the discriminant used for their construction. The only restriction imposed on the discriminant is that $\left(\frac{D}{p_1}\right) \ne -1$ and $\left(\frac{D}{p_2}\right) \ne -1$ where $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol.

The polynomials are obtained from this family by evaluating their value at a suitably chosen system of quadratic forms. In particular, the polynomial $M_{D,p_1,p_2}(x) \in \mathbb{Z}[x]$ is defined as

$$M_{D,p_1,p_2}(x) = \prod_{\tau_Q}(x - m_{p_1,p_2}^s(\tau_Q))$$

where $s = 24/\gcd(24, (p_1 - 1)(p_2 - 1))$ and $\tau_Q = \frac{-B_i+\sqrt{-D}}{2A_i}$ for all representatives $S = \{(A_i, B_i, C_i)\}_{1\le i\le h}$ of the reduced primitive quadratic forms of a discriminant $-D$ derived from a (p_1p_2)-system (the definition of a l-system can be found in [9]).

Once a polynomial is computed, we can use the modular equations $\Phi_{p_1,p_2}(x, j) = 0$, in order to compute a root j modulo p of the Hilbert polynomial from a root x modulo p of the $M_{D,p_1,p_2}(x)$ polynomial. However, a disadvantage of the $M_{D,p_1,p_2}(x)$ polynomial is that the degree in j in the modular equations is at least 2 and the coefficients of the modular equations are quite large (which makes their use less efficient).[1] The only modular polynomials that have degree 2 in j are $\Phi_{3,13}(x, j)$ and $\Phi_{5,7}(x, j)$. In addition, $M_{D,3,13}(x)$ and $M_{D,5,7}(x)$ polynomials are constructed more efficiently than other polynomials of the double-eta family [25]. Thus, we only used these polynomials in our experiments.

3. Ramanujan polynomials

In this section, we define a new class of polynomials which can be used in the CM method for the generation of secure ECs. We elaborate on their construction and provide the necessary transformations of their roots to the roots of the corresponding Hilbert polynomials.

3.1. Construction of polynomials

Srinivasa Ramanujan (1887–1920) defined in his third notebook, pages 392 and 393 in the pagination of [12, vol. 2], the values

$$t_D = \sqrt{3}q_D^{1/18}\frac{f(q_D^{1/3})f(q_D^3)}{f^2(q_D)} \in \mathbb{R} \tag{3}$$

where $f(-q) = \prod_{d=1}^{\infty}(1-q^d) = q^{-1/24}\eta(\tau), q = \exp(2\pi i\tau), q_D = \exp(-\pi\sqrt{D}), \tau \in \mathbb{H}$ ($\mathbb{H}$ is the upper half-plane) and $\eta(\tau)$ denotes the Dedekind eta function. Without any further explanation on how he found them, Ramanujan gave the following table of polynomials $T_D(x)$ based on t_D for five values of D:

D	$T_D(x)$
11	$x - 1$
35	$x^2 + x - 1$
59	$x^3 + 2x - 1$
83	$x^3 + 2x^2 + 2x - 1$
107	$x^3 - 2x^2 + 4x - 1$

In [13] Berndt and Chan proved that these polynomials do indeed have the Ramanujan values t_D as roots. The method that they used could not be applied for higher values of D and they asked for an efficient way of computing the polynomials T_D for every D. They also proved that if $D \in \mathbb{N}$ is square-free and such that $D \equiv 11 \bmod 24$, then t_D is a real unit generating the Hilbert class field. This actually means that the polynomials T_D can be used in the CM method because their roots can be transformed to the roots of the corresponding Hilbert polynomials. In addition, the remarkably small coefficients of these polynomials are a clear indication that their use in the CM method can be especially favoured.

In [16] the authors applied the Shimura Reciprocity Law for the Ramanujan class invariant t_D and an algorithm for computing the polynomials $T_D(x)$ was provided using the work of Gee and Stevenhagen [14,15]. The construction of these polynomials (which we will call *Ramanujan polynomials*) involves six modular functions $R_i()$ with $i \in \{0, 1, 2, 3, 4, 5\}$ of level 72 which are defined by

$$R_0(\tau) = \frac{\eta(3\tau)\eta(\tau/3)}{\eta^2(\tau)}$$
$$R_1(\tau) = \frac{\eta(3\tau)\eta(\tau/3 + 1/3)}{\eta^2(\tau)}$$
$$R_2(\tau) = \frac{\eta(3\tau)\eta(\tau/3 + 2/3)}{\eta^2(\tau)}$$
$$R_3(\tau) = \frac{\eta(\tau/3)\eta(\tau/3 + 2/3)}{\eta^2(\tau)}$$
$$R_4(\tau) = \frac{\eta(\tau/3)\eta(\tau/3 + 1/3)}{\eta^2(\tau)}$$

[1] For example, notice in [29] the size of the smallest modular polynomial $\Phi_{5,7}(x, j)$.

and

$$R_5(\tau) = \frac{\eta(\tau/3+2/3)\eta(\tau/3+1/3)}{\eta^2(\tau)}.$$

It was proved in [16] that $t_D = \sqrt{3}R_2(\theta)$ where $\theta = 1/2 - 1/2\sqrt{-D}$. The Shimura Reciprocity Law gives us the action of every primitive, reduced quadratic form $[a, b, c]$ of $-D$ on $\sqrt{3}R_2(\theta)$:

$$\left(\sqrt{3}R_2(\theta)\right)^{[a,-b,c]} = (\zeta_{72}^{6d_{[a,b,c]}} - \zeta_{72}^{30d_{[a,b,c]}})R_2\left(\frac{\alpha_{[a,b,c]}\tau_{[a,b,c]} + \beta_{[a,b,c]}}{\gamma_{[a,b,c]}\tau_{[a,b,c]} + \delta_{[a,b,c]}}\right)^{\sigma_{d_{[a,b,c]}}},$$

where $\zeta_{72} = e^{2\pi i/72}$, $\tau_{[a,b,c]}$ is the (complex) root of az^2+bz+c with positive imaginary part, $\begin{pmatrix}\alpha_{[a,b,c]} & \beta_{[a,b,c]}\\ \gamma_{[a,b,c]} & \delta_{[a,b,c]}\end{pmatrix} = A_{[a,b,c]}$ is an element in $GL_2(\mathbb{Z}/N\mathbb{Z})$, $d_{[a,b,c]} = \det A_{[a,b,c]}$ and $\sigma_{d_{[a,b,c]}} \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ sends $\zeta_{72} \mapsto \zeta_{72}^{d_{[a,b,c]}}$. In particular, the matrix $A_{[a,b,c]}$ is the unique element in $GL_2(\mathbb{Z}/N\mathbb{Z})$ that is mapped to $A_{[a,b,c],p^r}$ modulo p^r, where p^r is the maximum power of a prime p that divides 72. Namely, the matrices $A_{[a,b,c],p^r}$ for $p = 2, 3$ and $p^r = 8, 9$ are defined by

$$A_{[a,b,c],p^r} = \begin{cases} \begin{pmatrix} a & \dfrac{b-1}{2} \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} \dfrac{-b-1}{2} & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c \\ \begin{pmatrix} \dfrac{-b-1}{2} - a & \dfrac{1-b}{2} - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c. \end{cases} \tag{4}$$

The determinants of the matrices $A_{[a,b,c],p^r}$ are easily found:

$$d_{[a,b,c],p^r} = \begin{cases} a & \text{if } p \nmid a \\ c & \text{if } p \mid a \text{ and } p \nmid c \\ a+b+c & \text{if } p \mid a \text{ and } p \mid c. \end{cases} \tag{5}$$

On the basis of the Chinese remainder theorem, we can compute the determinant

$$d_{[a,b,c]} = 9d_{[a,b,c],8} - 8d_{[a,b,c],9}. \tag{6}$$

Now, we can write the matrix $A_{[a,b,c]}$ uniquely as a product

$$A_{[a,b,c]} = B_{[a,b,c]}\begin{pmatrix} 1 & 0 \\ 0 & d_{[a,b,c]} \end{pmatrix},$$

where $d_{[a,b,c]} = \det A_{[a,b,c]}$ and $B_{[a,b,c]}$ is a matrix with determinant 1. The construction of the polynomials would be completed if we could compute the expansion of $B_{[a,b,c]}$ as a word of the matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ which generate the group $SL_2(\mathbb{Z})$.

In this paper, we will try to simplify the approach provided in [16]. Since the construction of the polynomials $T_D(x)$ is based on the six modular functions R_i, we must provide the action of $\sigma_{d_{[a,b,c]}}$ and $B_{[a,b,c]}$ on them. In particular, the action of σ_d on the modular functions is expressed in terms of the matrix

$$\Sigma = \begin{cases} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_{72}^{d-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{72}^{2d-2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_{72}^{2d-2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_{72}^{d-1} & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_{72}^{3d-3} \end{pmatrix} & \text{if } d \equiv 1 \bmod 3 \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{72}^{d-2} & 0 & 0 & 0 \\ 0 & \zeta_{72}^{2d-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_{72}^{2d-1} & 0 \\ 0 & 0 & 0 & \zeta_{72}^{d-2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_{72}^{3d-3} \end{pmatrix} & \text{if } d \equiv 2 \bmod 3. \end{cases} \tag{7}$$

The action of the matrix $B_{[a,b,c]}$ on the modular functions R_i can be found if we compute the expansion of $B_{[a,b,c]}$ as a word of the matrices S and T. The actions of the elements S and T on the modular functions R_i are

$$T_d = \begin{pmatrix} 0 & \zeta_{72}^{3d} & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{72}^{3d} & 0 & 0 & 0 \\ \zeta_{72}^{6d} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dfrac{1}{\zeta_{72}^{3d}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \dfrac{1}{\zeta_{72}^{6d}} \\ 0 & 0 & 0 & \dfrac{1}{\zeta_{72}^{3d}} & 0 & 0 \end{pmatrix},$$

$$S_d = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \dfrac{1}{\zeta_{72}^{3d}(-\zeta_{72}^{30d}+\zeta_{72}^{6d})} & 0 & 0 \\ 0 & 0 & 0 & 0 & \dfrac{\zeta_{72}^{3d}}{-\zeta_{72}^{30d}+\zeta_{72}^{6d}} & 0 \\ 0 & \zeta_{72}^{3d}(-\zeta_{72}^{30d}+\zeta_{72}^{6d}) & 0 & 0 & 0 & 0 \\ 0 & 0 & \dfrac{-\zeta_{72}^{30d}+\zeta_{72}^{6d}}{\zeta_{72}^{3d}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

where $d = d_{[a,b,c]}$ (see Eq. (6)). For every representative $[a, b, c]$ of an equivalence class in the class group we form the 2×2 matrix $A_{[a,b,c],p^r}$ for $p^r = 8, 9$ as defined in Eq. (4). The matrix $A_{[a,b,c],p^r}$ is then expressed as the product $B_{[a,b,c],p^r}$ of a 2×2 matrix of determinant 1 and a matrix of the form $\begin{pmatrix} 1 & 0 \\ 0 & d_{[a,b,c],p^r} \end{pmatrix}$. In particular,

$$A_{[a,b,c],p^r} = B_{[a,b,c],p^r} \begin{pmatrix} 1 & 0 \\ 0 & d_{[a,b,c],p^r} \end{pmatrix} \overset{\text{using Eq. (5)}}{\rightarrow}$$

$$B_{[a,b,c],p^r} = \begin{cases} \begin{pmatrix} a & \dfrac{b-1}{2a} \\ 0 & \dfrac{1}{a} \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} \dfrac{-b-1}{2} & -1 \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c \\ \begin{pmatrix} \dfrac{-b-1}{2} - a & \dfrac{1-b-2c}{2(a+b+c)} \\ 1 & -\dfrac{1}{a+b+c} \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c. \end{cases} \tag{8}$$

According to Lemma 3.3 in [16], the matrix $B_{[a,b,c],p^r}$ for $p^r = 8, 9$ can be written as a word of the matrices F_8, G_8, F_9, G_9, where $F_8 = T_d^{-1 \pmod{72}} S_d T_d^{-10 \pmod{72}} S_d T_d^{-1 \pmod{72}} S_d T_d^{-162 \pmod{72}} = T_d^{71} S_d T_d^{62} S_d T_d^{71} S_d T_d^{54}$, $G_8 = T_d^9$, $F_9 = T_d^{-1} S_d T_d^{-65} S_d T_d^{-1} S_d T_d^{1096} = T_d^{71} S_d T_d^7 S_d T_d^{71} S_d T_d^{16}$ and $G_9 = T_d^{-8} = T_d^{64}$, where $d = d_{[a,b,c]}$. In particular, we have computed that

$$F_8 = G_8 = \begin{pmatrix} (-1)^d & 0 & 0 & 0 & 0 & 0 \\ 0 & (-1)^d & 0 & 0 & 0 & 0 \\ 0 & 0 & (-1)^d & 0 & 0 & 0 \\ 0 & 0 & 0 & (-1)^d & 0 & 0 \\ 0 & 0 & 0 & 0 & (-1)^d & 0 \\ 0 & 0 & 0 & 0 & 0 & (-1)^d \end{pmatrix}$$

$$F_9 = \begin{pmatrix} (-1)^d & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \dfrac{1}{\zeta_{72}^{33d}(-\zeta_{72}^{30d}+\zeta_{72}^{6d})} & 0 & 0 \\ 0 & 0 & 0 & 0 & \dfrac{1}{\zeta_{72}^{33d}(-\zeta_{72}^{30d}+\zeta_{72}^{6d})} & 0 \\ 0 & (-1)^d(-\zeta_{72}^{33d}+\zeta_{72}^{9d}) & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{72}^{33d}(-\zeta_{72}^{30d}+\zeta_{72}^{6d}) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & (-1)^d \end{pmatrix}$$

and

$$G_9 = \begin{pmatrix} 0 & \frac{1}{\zeta_{72}^{33d}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{\zeta_{72}^{33d}} & 0 & 0 & 0 \\ \frac{1}{\zeta_{72}^{30d}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_{72}^{33d} & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_{72}^{30d} \\ 0 & 0 & 0 & \zeta_{72}^{33d} & 0 & 0 \end{pmatrix}.$$

Following again Lemma 3.3 in [16], we can prove the next lemma:

Lemma 1. *The matrices $B_{[a,b,c],p^r}$ can be written as a word of the matrices F_{p^r} and G_{p^r} using the following equation:*

$$B_{[a,b,c],p^r} = \begin{cases} F_{p^r} G_{p^r}^{-\frac{1}{a} \bmod p^r} F_{p^r} G_{p^r}^{-a \bmod p^r} F_{p^r} G_{p^r}^{(\frac{1}{a^2}(\frac{b-1}{2})-\frac{1}{a}) \bmod p^r} & \text{if } p \nmid a \\ G_{p^r}^{(1-\frac{b+1}{2}) \bmod p^r} F_{p^r} G_{p^r} F_{p^r} G_{p^r} & \text{if } p \mid a \text{ and } p \nmid c \\ G_{p^r}^{(1-\frac{b+1}{2}-a) \bmod p^r} F_{p^r} G_{p^r} F_{p^r} G_{p^r}^{1-\frac{1}{a+b+c} \bmod p^r} & \text{if } p \mid a \text{ and } p \mid c. \end{cases} \tag{9}$$

Proof. The proof is derived directly from Lemma 3.3 in [16]. For example, in the case that $p \nmid a$ the matrix $B_{[a,b,c],p^r} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is equal to $F_{p^r} G_{p^r}^{-z} F_{p^r} G_{p^r}^{-A} F_{p^r} G_{p^r}^{Bz-D}$ where $z = \frac{1+C}{A} \bmod p^r$. Substituting $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with $\begin{pmatrix} a & \frac{b-1}{2a} \\ 0 & \frac{1}{a} \end{pmatrix}$ from Eq. (8) we can easily find that

$$B_{[a,b,c],p^r} = F_{p^r} G_{p^r}^{-\frac{1}{a} \bmod p^r} F_{p^r} G_{p^r}^{-a \bmod p^r} F_{p^r} G_{p^r}^{(\frac{1}{a^2}(\frac{b-1}{2})-\frac{1}{a}) \bmod p^r}. \quad \blacksquare$$

Concluding the above discussion, the Ramanujan polynomial $T_D(x) \in \mathbb{Z}[x]$ for $D \equiv 11 \bmod 24$ is defined as

$$T_D(x) = \prod_{\tau} (x - t(\tau))$$

for values of τ satisfying $\tau = \frac{-b+\sqrt{-D}}{2a}$ for all primitive, reduced quadratic forms $[a, b, c]$ of $-D$. Every value $t(\tau)$ that corresponds to a specific form $[a, b, c]$ is defined by

$$t(\tau) = (\zeta_{72}^{6d} - \zeta_{72}^{30d}) \sum_{i=0}^{5} a_{2i} R_i(\tau) \tag{10}$$

where the value d is equal to $d_{[a,b,c]}$ (see Eq. (6)) and the values a_{2i} with $i \in \{0, 1, 2, 3, 4, 5\}$ are the elements of the third row of the 6×6 matrix $A = B_{[a,b,c],8} B_{[a,b,c],9} \Sigma$.

It is easy to see that every row in the matrix A has only one non-zero element. Thus, only one value a_{2i} is not equal to zero and the computation of every value $t(\tau)$ requires the evaluation of only one value $R_i(\tau)$. However, the construction described above is not very efficient since it involves many multiplications of matrices (see Eq. (9)). A question that immediately arises is that of whether we can avoid the use of matrices and construct the Ramanujan polynomials in a way similar to the construction of Hilbert or Weber polynomials (e.g. using only quadratic forms and modular functions). Clearly, the answer is positive and will be analysed in the next section.

3.2. Constructing the polynomials without matrices

Let us define the following function of $d = d_{[a,b,c]}$:

$$N(d) = \begin{cases} \left(\frac{1-b}{2}\right) d & \text{if } 2 \nmid a \text{ or } 2 \nmid c \\ \left(\frac{1-3b}{2}\right) d & \text{if } 2 \mid a, 2 \mid c. \end{cases} \tag{11}$$

We introduce the following notation:

- If $3 \nmid a$ then let a^* be an inverse of a mod 9. Write $a = 3\pi_a + \upsilon_a$, $a^* = 3\pi_{a^*} + \upsilon_{a^*}$, $\left(\frac{b-1}{2}a^* - 1\right)a^* = 3\pi_1 + \upsilon_1$, where $0 \le \upsilon_a, \upsilon_{a^*}, \upsilon_1 < 3$.
- If $3 \mid a$ and $3 \nmid c$ then write $1 - (\frac{b+1}{2}) = 3\pi_2 + \upsilon_2$, where $0 \le \upsilon_2 < 3$.
- If $3 \mid a$ and $3 \mid c$ then write $y = 1 - (\frac{b+1}{2}) - a = 3\pi_y + \upsilon_y$, $0 \le \upsilon_y < 3$. Let $(a+b+c)^*$ be the multiplicative inverse of $(a+b+c)$ mod 9 and write $-(a+b+c)^* + 1 = 3\pi_3 + \upsilon_3$, $0 \le \upsilon_3 < 3$.

Moreover, consider the following function of $\tau = \tau_{[a,b,c]}$:

$$f(\tau) = \begin{cases} \zeta_{72}^{24d(\pi_a - \pi_{a^*} - \pi_1) + 42d} R_0(\tau) & \text{if } a \equiv 1 \bmod 3,\ \upsilon_1 = 0 \\ \zeta_{72}^{24d(\pi_a - \pi_{a^*} - \pi_1) + 10d - 1} R_1(\tau) & \text{if } a \equiv 1 \bmod 3,\ \upsilon_1 = 1 \\ \zeta_{72}^{24d(\pi_a - \pi_{a^*} - \pi_1) + 50d - 2} R_2(\tau) & \text{if } a \equiv 1 \bmod 3,\ \upsilon_1 = 2 \\ \zeta_{72}^{48d(\pi_a + \pi_{a^*} + \pi_1) - 14d - 2} R_2(\tau) & \text{if } a \equiv 2 \bmod 3,\ \upsilon_1 = 0 \\ \zeta_{72}^{48d(\pi_a + \pi_{a^*} + \pi_1) - 46d - 1} R_1(\tau) & \text{if } a \equiv 2 \bmod 3,\ \upsilon_1 = 1 \\ \zeta_{72}^{48d(\pi_a + \pi_{a^*} + \pi_1) - 6d} R_0(\tau) & \text{if } a \equiv 2 \bmod 3,\ \upsilon_1 = 2 \\ \dfrac{\zeta_{72}^{48d\pi_2 - 4d - 2}}{-\zeta_{72}^{30d} + \zeta_{72}^{6d}} R_3(\tau) & \text{if } a \equiv 0 \bmod 3,\ \upsilon_2 = 0,\ c \equiv 1 \bmod 3 \\ \dfrac{\zeta_{72}^{48d\pi_2 - 4d - 1}}{-\zeta_{72}^{30d} + \zeta_{72}^{6d}} R_4(\tau) & \text{if } a \equiv 0 \bmod 3,\ \upsilon_2 = 0,\ c \equiv 2 \bmod 3 \\ \dfrac{\zeta_{72}^{48d\pi_2 + 40d - 1}}{-\zeta_{72}^{30d} + \zeta_{72}^{6d}} R_4(\tau) & \text{if } a \equiv 0 \bmod 3,\ \upsilon_2 = 1,\ c \equiv 1 \bmod 3 \\ \dfrac{\zeta_{72}^{48d\pi_2 + 40d - 2}}{-\zeta_{72}^{30d} + \zeta_{72}^{6d}} R_3(\tau) & \text{if } a \equiv 0 \bmod 3,\ \upsilon_2 = 1,\ c \equiv 2 \bmod 3 \\ \zeta_{72}^{48d\pi_2 + 6d} R_0(\tau) & \text{if } a \equiv 0 \bmod 3,\ \upsilon_2 = 2 \\ \dfrac{\zeta_{72}^{24d(\pi_3 - \pi_y) + 36d - 3}}{-\zeta_{72}^{30d} + \zeta_{72}^{6d}} R_5(\tau) & \text{if } a \equiv 0 \bmod 3, c \equiv 0 \bmod 3,\ \upsilon_y = 0 \\ \dfrac{\zeta_{72}^{24d(\pi_3 - \pi_y) - 3}}{-\zeta_{72}^{30d} + \zeta_{72}^{6d}} R_5(\tau) & \text{if } a \equiv 0 \bmod 3, c \equiv 0 \bmod 3,\ \upsilon_y = 1. \end{cases}$$

Then, the following theorem can be proved.

Theorem 1. *The roots of the Ramanujan polynomials are given by the equation*

$$t(\tau_{[a,b,c]}) = \left(\zeta_{72}^{6d_{[a,b,c]}} - \zeta_{72}^{30d_{[a,b,c]}}\right) \cdot (-1)^{N(d_{[a,b,c]})} \cdot f\left(\tau_{[a,b,c]}\right) \tag{12}$$

where $[a, b, c]$ runs over the set of equivalences of quadratic forms of discriminant $-D$ and $\tau_{[a,b,c]}$ is the unique root of ax^2+bx+c with positive imaginary part.

Proof. According to Eq. (10), the roots of the Ramanujan polynomials are equal to $t(\tau) = (\zeta_{72}^{6d} - \zeta_{72}^{30d}) \sum_{i=0}^{5} a_{2i} R_i(\tau)$. The values a_{2i} with $i \in \{0, 1, 2, 3, 4, 5\}$ are the elements of the third row of the 6×6 matrix $A = B_{[a,b,c],8} B_{[a,b,c],9} \Sigma$. On the basis of the congruences of the elements $[a, b, c]$, we will try to evaluate the matrices $B_{[a,b,c],8}$, $B_{[a,b,c],9}$ and Σ in order to find the value of the only non-zero element a_{2i}.

First, we will investigate the action of the $B_{[a,b,c],8}$ matrix on the final matrix A and consequently on the values a_{2i}. The matrix $B_{[a,b,c],8}$ is actually responsible for the term $(-1)^{N(d_{[a,b,c]})}$ in Eq. (12). Notice that the matrix $B_{[a,b,c],8}$ is constructed from powers of the matrices F_8 and G_8 (see Eq. (9)). Having in mind that the multiplicative group of invertible elements modulo 8 is isomorphic to the direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we conclude that the inverse of every element modulo 8 coincides with the element itself, i.e. $a^2 \equiv 1 \bmod 8$ if $(a, 8) = 1$. This means that Eq. (9) for the case $p = 2$ takes the form

$$B_{[a,b,c],8} = \begin{cases} F_8 G_8^{-a \bmod 8} F_8 G_8^{-a \bmod 8} F_8 G_8^{(\frac{b-1}{2} - a) \bmod 8} & \text{if } 2 \nmid a \\ G_8^{(1 - \frac{b+1}{2}) \bmod 8} F_8 G_8 F_8 G_8 & \text{if } 2 \mid a \text{ and } 2 \nmid c \\ G_8^{(1 - \frac{b+1}{2} - a) \bmod 8} F_8 G_8 F_8 G_8^{1-(a+b+c) \bmod 8} & \text{if } 2 \mid a \text{ and } 2 \mid c. \end{cases}$$

Moreover, the form of the matrices F_8 and G_8 implies that F_8G_8, G_8^2 and F_8^2 are all equal to the unit matrix I. This means that the matrix $B_{[a,b,c],8}$ can be further simplified, leading to the equation

$$B_{[a,b,c],8} = \begin{cases} G_8^{(\frac{b-1}{2}) \bmod 8} & \text{if } 2 \nmid a \\ G_8^{(\frac{1-b}{2}) \bmod 8} & \text{if } 2 \mid a \text{ and } 2 \nmid c \\ G_8^{(\frac{1-3b}{2}) \bmod 8} & \text{if } 2 \mid a \text{ and } 2 \mid c. \end{cases}$$

Clearly, the matrix $B_{[a,b,c],8}$ will add a multiplier ± 1 to the final value of the invariants. The sign in front of 1 will be determined by the above equation and is given by Eq. (11).

Dealing with the effect of the $B_{[a,b,c],9}$ matrix is much more complicated. In this case, we have to compute powers of the matrix G_9. This task becomes less difficult with the observation that G_9^3 is a diagonal matrix equal to

$$G_9^3 = \begin{pmatrix} \zeta_{72}^{-24d} & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_{72}^{-24d} & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{72}^{-24d} & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_{72}^{24d} & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_{72}^{24d} & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_{72}^{24d} \end{pmatrix}.$$

Therefore, integer powers G_9^k can be computed by considering different cases according to the values of $k \mod 3$. Let us consider the case where $3 \mid a$ and $3 \mid c$. Then, the matrix $B_{[a,b,c],9}$ is equal to $B_{[a,b,c],9} = G_9^{(1-\frac{b+1}{2}-a) \bmod 9} F_9 G_9 F_9 G_9^{1-1/(a+b+c) \bmod 9}$. Since we want to use the fact that the matrix G_9^3 is diagonal, we must express the values $y = 1-(\frac{b+1}{2})-a$ and $x = 1-(a+b+c)^*$, where $(a+b+c)^*$ is the multiplicative inverse of $(a+b+c) \bmod 9$, as multiplies of 3 plus the residue modulo 3. Thus, we write $y = 1-(\frac{b+1}{2})-a = 3\pi_y+\upsilon_y, 0 \le \upsilon_y < 3$ and $x = 1-(a+b+c)^* = 3\pi_3+\upsilon_3, 0 \le \upsilon_3 < 3$. Notice that $y \equiv 1-(\frac{b+1}{2}) \bmod 3 \equiv \frac{1-b}{2} \bmod 3 \equiv 2(1-b) \bmod 3$ and $x \equiv 1-(a+b+c)^* \bmod 3 \equiv 1-(a+b+c) \bmod 3 \equiv 1-b \bmod 3$. The residue υ_y cannot be equal to 2, because then $b \equiv 0 \bmod 3$ (this is not possible since $a \equiv 0 \bmod 3$ and $c \equiv 0 \bmod 3$). So, the only possible values for υ_y are 0 and 1. If $\upsilon_y = 0$ then $x \equiv 0 \bmod 3$ and if $\upsilon_y = 1$ then $x \equiv 2 \bmod 3$. Considering these two cases, we can symbolically compute integer powers of the matrix G_9 and finally find the values of the matrix $B_{[a,b,c],9}$. Following the same reasoning, we can evaluate $B_{[a,b,c],9}$ for the cases $3 \mid a$, $3 \nmid c$ and $3 \nmid a$.

The final step before the calculation of the function $f(\tau)$ is the multiplication of the Σ matrix with $B_{[a,b,c],9}$. In order to decide which of the two matrices to use (see Eq. (7)) we must know the value of $d \bmod 3$. Notice that $d = d_{[a,b,c]} = 9d_{[a,b,c],8} - 8d_{[a,b,c],9}$. This means that the congruence of $d \bmod 3$ depends only on the value of $d_{[a,b,c],9}$. From Eq. (5), we can compute $d_{[a,b,c],9}$ and use the corresponding Σ matrix. For example, when $3 \mid a$ and $3 \mid c$, $d \bmod 3 \equiv d_{[a,b,c],9} \bmod 3 \equiv b \bmod 3$. If $b \bmod 3 = 1$, then $\upsilon_y = 0$ and if $b \bmod 3 = 2$, then $\upsilon_y = 1$. So, in every case we know with which Σ matrix we will multiply $B_{[a,b,c],9}$. This finally leads us to the value of the $f(\tau)$ function. ■

Taking a more careful look at the $f(\tau)$ function, we notice that it can be simplified into the following form:

$$f(\tau) = \begin{cases} \zeta_{72}^{24d(\pi_a-\pi_{a^*}-\pi_1)+42d-(32d+1)\upsilon_1} R_{\upsilon_1}(\tau) & \text{if } a \equiv 1 \bmod 3 \\ \zeta_{72}^{48d(\pi_a+\pi_{a^*}+\pi_1)-6d+(32d-1)(2-\upsilon_1)} R_{2-\upsilon_1}(\tau) & \text{if } a \equiv 2 \bmod 3 \\ \zeta_{72}^{48d\pi_2+6d} R_0(\tau) & \text{if } a \equiv 0 \bmod 3,\ \upsilon_2 = 2,\ c \equiv 1, 2 \bmod 3 \\ \dfrac{\zeta_{72}^{48d\pi_2-4d-2+(44d+1)\upsilon_2}}{-\zeta_{72}^{30d}+\zeta_{72}^{6d}} R_{3+\upsilon_2}(\tau) & \text{if } a \equiv 0 \bmod 3,\ \upsilon_2 \neq 2,\ c \equiv 1 \bmod 3 \\ \dfrac{\zeta_{72}^{48d\pi_2-4d-1+(44d-1)\upsilon_2}}{-\zeta_{72}^{30d}+\zeta_{72}^{6d}} R_{4-\upsilon_2}(\tau) & \text{if } a \equiv 0 \bmod 3,\ \upsilon_2 \neq 2,\ c \equiv 2 \bmod 3 \\ (-1)^{d(1-\upsilon_y)} \dfrac{\zeta_{72}^{24d(\pi_3-\pi_y)-3}}{-\zeta_{72}^{30d}+\zeta_{72}^{6d}} R_5(\tau) & \text{if } a \equiv 0 \bmod 3,\ c \equiv 0 \bmod 3. \end{cases}$$

A numerical example: Suppose that we want to compute the Ramanujan polynomial for $D = 491$. The quadratic forms that correspond to this value are $[1, 1, 123]$, $[3, \pm 1, 41]$, $[9, \pm 7, 15]$, $[5, \pm 3, 25]$ and $[11, \pm 9, 13]$.

- For the quadratic form $[1, 1, 123]$ we have that $d = 1, N(d) = 1, a = 1 \equiv 1 \bmod 3$ and $\upsilon_1 = 2$. The corresponding root $t(\tau_{[1,1,123]})$ of the Ramanujan polynomial is equal to 0.036222.
- For $[3, 1, 41]$, we compute $d = -301, N(d) = 1, a \equiv 0 \bmod 3, c \equiv 2 \bmod 3$ and $\upsilon_2 = 0$. The corresponding root is equal to $-0.422245 - 3.603760$i while for the quadratic form $[3, -1, 41]$ is $-0.422245 + 3.603760$i.
- For $[9, 7, 15]$, we compute $d = -167, N(d) = -1, a \equiv 0 \bmod 3, c \equiv 0 \bmod 3$ and $\upsilon_y = 0$. The corresponding root is equal to $-0.706141 - 1.456263$i while for the quadratic form $[9, -7, 15]$ is $-0.706141 + 1.456263$i.

- For [5, 3, 25], we compute $d = 5, N(d) = -1, a \equiv 2 \bmod 3, c \equiv 1 \bmod 3$ and $\upsilon_1 = 2$. The corresponding root is equal to $0.644187 - 0.462340\mathrm{i}$ while for the quadratic form $[5, -3, 25]$ is $0.644187 + 0.462340\mathrm{i}$.
- For [11, 9, 13], we compute $d = 11, N(d) = 1, a \equiv 2 \bmod 3, c \equiv 1 \bmod 3$ and $\upsilon_1 = 2$. The corresponding root is equal to $-0.033911 - 1.127898\mathrm{i}$ while for the quadratic form $[11, -9, 13]$ is $-0.033911 + 1.127898\mathrm{i}$.

Finally, the Ramanujan polynomial is calculated using the relation $T_{491}(x) = \prod_\tau (x - t(\tau))$ and is equal to

$$x^9 + x^8 + 16x^7 + 2x^6 + 37x^5 - 31x^4 + 44x^3 - 40x^2 + 29x - 1.$$

3.3. Transformation of the roots

In order to use Ramanujan polynomials in the CM method, we must prove that they have roots modulo p and then find a transformation of their roots modulo p to the roots modulo p of the corresponding Hilbert polynomials. The following proposition proves that a Ramanujan polynomial with degree h has exactly h roots modulo p under certain conditions (which are satisfied in the CM method):

Proposition 1. *A Ramanujan polynomial $T_D(x)$ with degree h has exactly h roots modulo p if and only if the equation $4p = u^2 + Dv^2$ has integer solutions and p does not divide the discriminant $\Delta(T_D)$ of the polynomial.*

Proof. Let H_K be the Hilbert class field of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, and let $\mathcal{O}_{H_K}$ and $\mathcal{O}_K$ be the rings of algebraic integers of H_K and K respectively. Let p be a prime such that $4p = u^2 + Dv^2$ has integer solutions. Then, according to [19, Th. 5.26], p splits completely in H_K. Proposition 5.29 in [19] implies that (since t_D generates H_K) $T_D(x)$ has a root modulo p if and only if p splits in H_K and does not divide its discriminant $\Delta(T_D)$. But since $\frac{\mathcal{O}_{H_K}}{p\mathcal{O}_{H_K}}/\mathbb{F}_p$ is Galois, $T_D(x)$ has not only one root modulo p, but h distinct roots modulo p. ■

We will present now a method for retrieving a root modulo p of the Hilbert polynomial $H_D(x)$ from a root modulo p of the corresponding Ramanujan polynomial $T_D(x)$. Our aim is to find a transformation that maps a real root of the Ramanujan polynomial to a real root of the corresponding Hilbert polynomial. Then, we can reduce this transformation modulo a prime ideal of the ring of integers of the Hilbert class field. In this way we see that the same transformation will transfer a root of the Ramanujan polynomial modulo p to a root of the Hilbert polynomial modulo p. We know that if $\ell_0 = (1, 1, \frac{1+D}{4})$ is a quadratic form (known as the principal form) that corresponds to the root $\tau_{\ell_0} = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{D}}{2}$ then $j(\tau_{\ell_0})$ is a real root of the Hilbert polynomial $H_D(x)$. The following lemma shows that the value t_D defined in Eq. (3) is a real root of the Ramanujan polynomial $T_D(x)$.

Lemma 2. *The value t_D is a real root of the Ramanujan polynomial $T_D(x)$ and is equal to*

$$t_D = \sqrt{3}R_2(\tau_{\ell_0}).$$

Proof. Set

$$q_D = \exp(-\pi\sqrt{D}) = -\exp(2\pi\mathrm{i}\tau_{\ell_0}),$$

where $\tau_{\ell_0} = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{D}}{2}$. Then

$$\begin{aligned} f(q_D) &= f(-\exp(2\pi\mathrm{i}\tau_{\ell_0})) = \exp(2\pi\mathrm{i}\tau_{\ell_0})^{-1/24}\eta(\tau_{\ell_0}),\\ f(q_D^3) &= \exp(2\pi\mathrm{i}\tau_{\ell_0})^{-3/24}\eta(3\tau_{\ell_0}),\\ f(q_D^{1/3}) &= \exp(2\pi\mathrm{i}\tau_{\ell_0})^{-\frac{1}{3\cdot 24}}\eta\left(\frac{\tau_{\ell_0}}{3}\right). \end{aligned}$$

Taking Eq. (3) and all the above equations into consideration we can easily derive that $t_D = \sqrt{3}R_2(\tau_{\ell_0})$.

If we could prove that $t(\tau_{\ell_0}) = \sqrt{3}R_2(\tau_{\ell_0})$ then it would immediately follow that $t_D = t(\tau_{\ell_0})$ and thus it is a root of the Ramanujan polynomial. In order to compute the value $t(\tau_{\ell_0})$ we will use Eq. (12) from Theorem 1. Notice that the quadratic form that corresponds to τ_{ℓ_0} is equal to $[a, b, c] = [1, 1, \frac{1+D}{4}]$. Then, $d_{[a,b,c]} = 1, N(d_{[a,b,c]}) = 0, a^* = 1, \pi_a = 1, \pi_{a^*} = 1$, $\pi_1 = -1$ and $\upsilon_1 = 2$. Therefore, the value $f(\tau_{[a,b,c]}) = f(\tau_{\ell_0}) = \zeta_{72}^{24d(\pi_a - \pi_{a^*} - \pi_1) + 50d - 2} R_2(\tau_{\ell_0}) = R_2(\tau_{\ell_0})$. Finally, observe that $\sqrt{3} = \zeta_{72}^6 - \zeta_{72}^{30}$. Indeed, the value $\mathrm{i}\sqrt{3}$ can be expressed as a difference of two primitive 3-roots of unity, ζ_3, ζ_3^2, since $\mathrm{i} = \zeta_{72}^{18}$ and $\zeta_3 = \zeta_{72}^{24}$. Thus, using Theorem 1 we have that $t(\tau_{\ell_0}) = \left(\zeta_{72}^{6d_{[a,b,c]}} - \zeta_{72}^{30d_{[a,b,c]}}\right) \cdot (-1)^{N(d_{[a,b,c]})} \cdot f\left(\tau_{[a,b,c]}\right) = \sqrt{3}R_2(\tau_{\ell_0}) = t_D$. ■

Lemma 3. *Suppose R_T is a real root of a Ramanujan polynomial $T_D(x)$. Then, the real number R_H obtained from the equation*

$$R_H = (R_T^6 - 27R_T^{-6} - 6)^3 \tag{13}$$

is a real root of the corresponding Hilbert polynomial $H_D(x)$.

Proof. Set $R_T = t_D$ and $R_H = j(\tau_{\ell_0})$. Using Equations (4.4) and (4.5) from [13] it can be easily derived that $h(e^{2\pi i\tau_{\ell_0}/3}) - 27h(e^{2\pi i\tau_{\ell_0}/3})^{-1} = \gamma_2(\tau_{\ell_0}) + 6$ where $\gamma_2^3(\tau_{\ell_0}) = j(\tau_{\ell_0})$ and

$$h(q) = \frac{f^{12}(-q^3)}{qf^6(-q)f^6(-q^9)}. \tag{14}$$

Thus, $j(\tau_{\ell_0}) = (h(e^{2\pi i\tau_{\ell_0}/3}) - 27h(e^{2\pi i\tau_{\ell_0}/3})^{-1} - 6)^3$ which means that we now have to find the relation between t_D and $h(e^{2\pi i\tau_{\ell_0}/3})$. Substituting q with $e^{2\pi i\tau_{\ell_0}/3}$ in Eq. (14) we have that $h(e^{2\pi i\tau_{\ell_0}/3}) = \frac{f^{12}(-e^{2\pi i\tau_{\ell_0}})}{e^{2\pi i\tau_{\ell_0}/3}f^6(-e^{2\pi i\tau_{\ell_0}/3})f^6(-e^{3(2\pi i\tau_{\ell_0})})}$. Noticing that $q_D = \exp(-\pi\sqrt{D}) = -\exp(2\pi i\tau_{\ell_0})$, and from Eq. (3), we derive that $h(e^{2\pi i\tau_{\ell_0}/3}) = -27t_D^{-6}$ which completes the proof of the lemma. ■

The final step is to reduce Eq. (13) modulo p. The elements R_H, R_T are not in $\mathbb{Z}$ but are elements of the ring of algebraic integers $\mathcal{O}_{H_K}$ of the Hilbert class field and can be reduced modulo an ideal P extending the ideal $p\mathbb{Z}$ of $\mathbb{Z}$. But the ideal $p\mathbb{Z}$ splits completely; therefore the Galois extension $\frac{\mathcal{O}_{H_K}/P}{\mathbb{Z}/p\mathbb{Z}}$ is the trivial one, and $\mathcal{O}_{H_K}/P$ is the field $\mathbb{F}_p$. The argument above proves that Eq. (13) holds not only for the real roots of the polynomials but also for their roots modulo p. The interested reader is referred to [19,30,31] for definitions from algebraic number theory not given here. Using Eq. (13), we can easily derive the modular polynomial $\Phi_T(x, j)$ for Ramanujan polynomials. The polynomial is equal to

$$\Phi_T(x, j) = (x^{12} - 6x^6 - 27)^3 - jx^{18}. \tag{15}$$

4. Precision requirements for the construction of the polynomials

In this section we focus on the precision required for the construction of all previously mentioned polynomials. In order to compare them, we introduce the notion of *logarithmic height* for estimating the size of a polynomial. For a polynomial $g(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ its logarithmic height is defined as

$$H(g) = \max_{i=0,\ldots,n} \log_2 |a_i|.$$

The value $H(g)$ is actually the bit precision needed for performing all floating point computations in order to obtain the coefficients of the polynomial $g(x)$.

In the literature the "efficiency" of a class invariant (a root of a class polynomial) is measured by the asymptotic ratio of the logarithmic height of a root of the Hilbert polynomial to a root of the class polynomial in question. The best known class invariant is the one used for the construction of Weber polynomials with $D \not\equiv 0 \pmod 3$ and $D \equiv 3, 7 \pmod 8$. The roots of these Weber polynomials have logarithmic height that is asymptotically 72 times smaller than the logarithmic height of the roots of the corresponding Hilbert polynomials. However, in practice we are not interested in the logarithmic height of the roots but in the logarithmic height of the polynomials, since the latter measures the precision required for the construction of the polynomials. In this section, we will show that these two heights coincide only if the class polynomial has degree equal to the degree of the corresponding Hilbert polynomial. For the construction of prime order elliptic curves, Weber class polynomials have degree three times larger than the degree of the Hilbert polynomials. We will show that in this case the logarithmic height of the Weber polynomials is asymptotically $24 = 72/3$ times less than the logarithmic height of Hilbert polynomials and not 72. In what follows, it will be proved that even though the height of the Weber polynomials' roots for $D \equiv 3 \bmod 8$ is smaller than the height of the roots of Ramanujan's class polynomials, the precision requirements for the construction of the latter are smaller.

Starting from Hilbert polynomials, a remarkably accurate estimation of their precision requirements in bits (and of their logarithmic height also) was given in [32]:

$$\text{H-Prec1}(D) \approx 33 + \frac{\pi\sqrt{D}}{\ln 2} \sum_{\tau} \frac{1}{\alpha}$$

with the sum running over the same values of τ as the product in Eq. (2). It will be shown in the rest of the section that on the basis of this estimation, we can derive estimations of the precision requirements of every class polynomial.

Let f be a modular function such that $f(\tau)$ for some $\tau \in \mathbb{Q}(\sqrt{-D})$ generates the Hilbert class field of $\mathbb{Q}(\sqrt{-D})$. The element $f(\tau)$ is an algebraic integer, and let us denote by P_f its minimal polynomial. For every modular function there is a polynomial Φ (called a modular polynomial) such that $\Phi(f, j) = 0$ where j is the modular function used in the construction of Hilbert polynomials. This polynomial equation is used in order to transform the roots of the minimal polynomial of a class

invariant to the roots of the Hilbert polynomial. We have seen that in the cases of Weber, $M_{D,l}(x)$ and Ramanujan polynomials the degree in j of the modular polynomial is equal to 1 while for $M_{D,p_1,p_2}(x)$ polynomials it is at least 2. Asymptotically, one can estimate the ratio of the logarithmic height $h(j(\tau))$ of the algebraic integer $j(\tau)$ to the logarithmic height $h(f(\tau))$ of the algebraic integer $f(\tau)$.[2] Namely,

$$\lim_{h(j(\tau))\to\infty} \frac{h(j(\tau))}{h(f(\tau))} = \frac{\deg_f \Phi(f,j)}{\deg_j \Phi(f,j)} = r(f), \tag{16}$$

where the limit is taken over all CM points $\mathrm{SL}_2(\mathbb{Z})\tau \in \mathbb{H}$ [33].

A question that immediately arises is how Eq. (16) can be used for the estimation of the logarithmic height of the minimal polynomial P_f. The following lemma gives an answer to this question by generalizing the result in [25] for every algebraic number which generates either the Hilbert class field or an extension of it.

Lemma 4. *Suppose that $H(P_f)$ is the logarithmic height of the minimal polynomial of the algebraic number $f(\tau)$ and $H(P_j)$ is the logarithmic height of the corresponding Hilbert polynomial. If $f(\tau)$ generates the Hilbert class field then*

$$\lim_{h(j(\tau))\to\infty} \frac{H(P_j)}{H(P_f)} = \frac{\deg_f \Phi(f,j)}{\deg_j \Phi(f,j)} = r(f). \tag{17}$$

If $f(\tau)$ generates not the Hilbert class field but an algebraic extension of it with extension degree m, then

$$\lim_{h(j(\tau))\to\infty} \frac{H(P_j)}{H(P_f)} = \frac{\deg_f \Phi(f,j)}{\deg_j \Phi(f,j)} = \frac{r(f)}{m}.$$

Proof. The proof is based on the following bounds [22, Th. 5.9]:

$$-k + kh(a) \le H(P_a) \le k - 1 + kh(a)$$

where $h(a)$ is the logarithmic height of the algebraic integer a and k is the degree of its minimal polynomial P_a. If $f(\tau)$ generates the Hilbert class field then the degree of its minimal polynomial is equal to the degree of the corresponding Hilbert polynomial. Suppose that their degree is equal to k. Then, we have that

$$-k + kh(f(\tau)) \le H(P_f) \le k - 1 + kh(f(\tau)) \tag{18}$$

and

$$-k + kh(j(\tau)) \le H(P_j) \le k - 1 + kh(j(\tau)).$$

Thus,

$$\frac{-k + kh(j(\tau))}{k - 1 + kh(f(\tau))} \le \frac{H(P_j)}{H(P_f)} \le \frac{k - 1 + kh(j(\tau))}{-k + kh(f(\tau))}.$$

Taking the limit $h(j(\tau)) \to \infty$ we obtain that

$$\frac{H(P_j)}{H(P_f)} \to r(f). \tag{19}$$

In the case where $f(\tau)$ generates an algebraic extension of the Hilbert class field, we similarly have that

$$\frac{H(P_j)}{H(P_f)} \to \frac{r(f)}{m} \tag{20}$$

where m is the degree of the extension. This is easily derived from the fact that the degree of the minimal polynomial P_f is m times larger than the degree of the corresponding Hilbert polynomial and Eq. (18) becomes

$$-mk + mkh(f(\tau)) \le H(P_f) \le mk - 1 + mkh(f(\tau)).$$

Thus,

$$\frac{-k + kh(j(\tau))}{mk - 1 + mkh(f(\tau))} \le \frac{H(P_j)}{H(P_f)} \le \frac{k - 1 + kh(j(\tau))}{-mk + mkh(f(\tau))}. \quad \blacksquare$$

[2] Let K be a number field, $\alpha \in K$ be an algebraic number and M_K be the set of absolute values on K. Following the notation of [22, VIII], the absolute logarithmic height of an element $\alpha \in K$ is defined as $h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \log_2 \left(\prod_{v \in M_K} \max\{|\alpha|_v, 1\} \right)$.

Table 1
Precision estimations for $D \not\equiv 0 \pmod 3$.

D	Precision estimation
$D \equiv 7 \pmod 8$	$\frac{1}{72}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$D \equiv 3 \pmod 8$	$\frac{1}{24}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$D/4 \equiv 1, 2, 6 \pmod 8$	$\frac{1}{36}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$D/4 \equiv 5 \pmod 8$	$\frac{1}{18}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$

Table 2
Precision estimations for $D \equiv 0 \pmod 3$.

D	Precision estimation
$D \equiv 7 \pmod 8$	$\frac{1}{24}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$D \equiv 3 \pmod 8$	$\frac{1}{8}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$D/4 \equiv 1, 2, 6 \pmod 8$	$\frac{1}{12}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$D/4 \equiv 5 \pmod 8$	$\frac{1}{6}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$

Table 3
Precision estimations for $M_{D,l}(x)$, $M_{D,p_1,p_2}(x)$ and $T_D(x)$ polynomials.

Class polynomial	Precision estimation
$M_{D,3}(x)$	$\frac{1}{4}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$M_{D,5}(x)$	$\frac{1}{6}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$M_{D,7}(x)$	$\frac{1}{8}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$M_{D,13}(x)$	$\frac{1}{14}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$M_{D,5,7}(x)$	$\frac{1}{24}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$M_{D,3,13}(x)$	$\frac{1}{28}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$
$T_D(x)$	$\frac{1}{36}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$

Eqs. (19) and (20) relate the precision required for the construction of Hilbert polynomials to the precision needed for other classes of polynomials. Estimating the height $H(P_j)$ of Hilbert polynomials with the quantity $\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$, we can derive the precision requirements for the construction of every class polynomial by the equation

$$\frac{m}{r(f)}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha},$$

where m is either 1 or larger.

Obviously, we want to find class invariants $f(\tau)$ such that the ratio $r(f)$ is as big as possible. However, there is a limit on the ratio $r(f)$. It is known [34] that $r(f) \leq 800/7$ and if the Selberg eigenvalue conjecture in [35] holds then $r(f) \leq 96$. As regards Weber polynomials, when $D \equiv 3 \pmod 8$ their degree is three times larger than the degree of the corresponding Hilbert polynomials. Therefore, for this case of D, the estimation of the precision requirements will be approximately $\frac{3}{r(f)}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$. Concluding, estimations of the precision requirements of Weber polynomials are given in Tables 1 and 2 (these estimations can be derived from the definition of the corresponding class invariants, e.g. in [27]).

Again on the basis of Eq. (17), it can be concluded that the precision required for the construction of the $M_{D,l}(x)$ polynomials is approximately $\frac{1}{(l+1)}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$ and for $M_{D,p_1,p_2}(x)$ polynomials it is approximately $\frac{(p_1-1)(p_2-1)}{12(p_1+1)(p_2+1)}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$ where the sum runs over the same values of τ as the product in Eq. (2) [25]. Thus, it is equal to $\frac{1}{28}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$ for $M_{D,3,13}(x)$ polynomials and to $\frac{1}{24}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$ for $M_{D,5,7}(x)$ polynomials. Finally, in order to find an estimation for the precision requirements of Ramanujan polynomials, we use Eqs. (17) and (15). We readily conclude that the precision required for the construction of the Ramanujan polynomials is approximately $\frac{1}{36}\frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$. The above precision estimations are summarized in Table 3.

5. Implementation and experimental results

In this section, we discuss some issues regarding the construction of the Weber, $M_{D,l}(x)$, $M_{D,p_1,p_2}(x)$ and Ramanujan polynomials. All implementations and experiments were made in Pari 2.3.1 [36] compiled with the GMP-4.2.1 kernel [37] and have been carried out on a double 2 GHz Xeon machine running Linux 2.6.9-22 and equipped with 2 Gb of main memory.

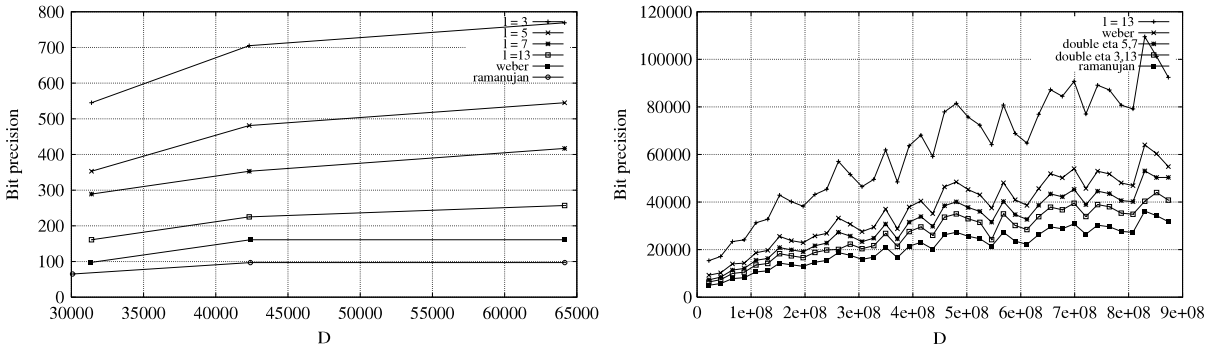

Fig. 1. Bit precision for the construction of all polynomials.

Table 4
Precision requirements (in bits) for the computation of $M_{D,13}(x)$, Weber, $M_{D,5,7}(x)$, $M_{D,3,13}(x)$ and Ramanujan polynomials.

D	h	$M_{D,13}(x)$	Weber	$M_{D,5,7}(x)$	$M_{D,3,13}(x)$	Ramanujan
109200299	5016	31270	18657	15546	13534	10624
240240299	6944	45402	26837	22757	19834	15442
349440299	9772	61933	37004	30768	26804	20998
458640299	12660	77894	46387	38447	33633	26245
698880299	13950	90734	54030	45311	39508	30813
851760299	15904	101214	60333	50322	43984	34243

5.1. Comparing polynomials for $D \equiv 3 \bmod 8$

In Fig. 1 we report on the precision needed for the construction of all polynomials for various values of $D \equiv 3 \bmod 8$. These values are used when the CM method is applied for the generation of prime order ECs. In the left figure, we examine the precision requirements of Ramanujan, Weber ($D \not\equiv 0 \pmod 3$) and $M_{D,l}(x)$ polynomials for all values of l. The values of D range from 30083 to 64163 while the degree h ranges from 32 to 48. We noticed that, as the theory dictates, the precision required for the construction of Ramanujan polynomials is much less than the precision required for the construction of Weber and $M_{D,l}(x)$ polynomials for all values of D that we examined. Weber polynomials require less precision than $M_{D,l}(x)$ polynomials, while among them $M_{D,13}(x)$ polynomials require the least precision. Examining larger values of the discriminant D and adding $M_{D,3,13}(x)$ and $M_{D,5,7}(x)$ polynomials in our comparison, we show (Fig. 1 (right)) that Ramanujan polynomials are constructed more efficiently than all other polynomials. $M_{D,3,13}(x)$ polynomials require less precision than $M_{D,5,7}(x)$ polynomials which are constructed more efficiently than Weber polynomials. In this figure, we examined all values of D from 21840299 to 873600299 using a step of 21840000. The degree h of the polynomials constructed (for these values of D) ranges from 2880 to 17472. Summarizing the results of our experiments, we see that Ramanujan polynomials surpass $M_{D,13}(x)$, Weber, $M_{D,5,7}(x)$ and $M_{D,3,13}(x)$ polynomials as they require on average 66%, 42%, 32% and 22% less precision respectively. Table 4 shows this difference by presenting the exact bit precision needed for the construction of the polynomials for several values of D.

Comparing the number of bits for the storage of all classes of polynomials, it is clear that the memory required for the storage of the Ramanujan polynomials is smaller than the memory needed for the storage of the other three classes of polynomials. The percentages are the same as in the precision requirements of the polynomials with one exception: Weber polynomials. Notice that the degree of Weber polynomials is $3h$ and thus the memory used for the storage of Ramanujan polynomials is not just 42% (like the precision requirements) less than the corresponding memory needed for the Weber polynomials but approximately 81% less! This means that as regards the storage requirements of all polynomials, Weber polynomials are by far the worst choice. In Table 5 we present the memory in MB needed for the storage of all classes of polynomials for a few values of D. The differences in efficiency of construction for all classes of polynomials can be easily understood by noticing the size of polynomials for a small value of D, namely $D = 299$. Even though this is a small value for the discriminant, the difference in size of the coefficients of the polynomials is remarkable. In particular, 25 bits are required for the storage of the coefficients of the $T_{299}(x)$ polynomial, 188 bits for the storage of the $W_{299}(x)$ polynomial, 112 bits for the $M_{299,13}(x)$ polynomial, 31 bits for $M_{299,3,13}(x)$ and 32 bits for $M_{299,5,7}(x)$.

$$\begin{aligned} W_{299}(x) \;=\; & x^{24} - 8x^{23} - 12x^{22} - 28x^{21} - 56x^{20} - 40x^{19} + 144x^{18} + 144x^{17} + 16x^{16} - 112x^{15} - 224x^{14} - 416x^{13} \\ & - 32x^{12} + 256x^{11} + 704x^{10} + 832x^{9} + 640x^{8} - 384x^{7} - 1792x^{6} - 1280x^{5} - 256x^{4} + 1280x^{3} \\ & + 1536x^{2} + 512x + 256 \end{aligned}$$

$$M_{299,13}(x) = x^8 + 78x^7 + 793x^6 + 5070x^5 + 20956x^4 + 65910x^3 + 134017x^2 + 171366x + 28561$$

$$M_{299,5,7}(x) = x^8 - 8x^7 + 31x^6 - 22x^5 + 28x^4 - 2x^3 - 19x^2 + 8x - 1$$

Table 5
Memory requirements (in MB) for the storage of $M_{D,13}(x)$, Weber, $M_{D,5,7}(x)$, $M_{D,3,13}(x)$ and Ramanujan polynomials.

D	h	$M_{D,13}(x)$	Weber	$M_{D,5,7}(x)$	$M_{D,3,13}(x)$	Ramanujan
109200299	5016	134	245	68	59	47
240240299	6944	271	492	138	119	94
349440299	9772	518	950	262	227	179
458640299	12660	842	1539	423	366	289
698880299	13950	1087	1986	551	478	377
851760299	15904	1379	2524	697	604	475

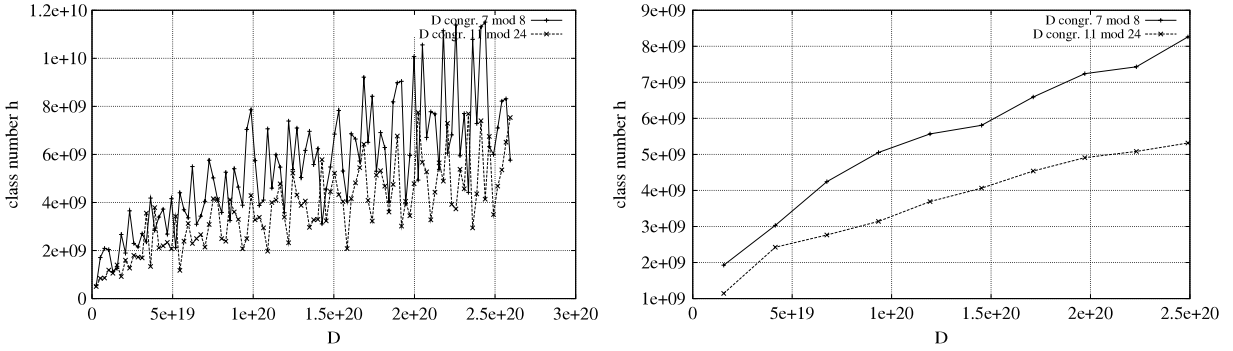

Fig. 2. Class number h for various values of D.

$$M_{299,3,13}(x) = x^8 - 6x^7 + 16x^6 + 12x^5 - 23x^4 + 12x^3 + 16x^2 - 6x + 1$$
$$T_{299}(x) = x^8 + x^7 - x^6 - 12x^5 + 16x^4 - 12x^3 + 15x^2 - 13x + 1.$$

The time efficiency of the construction of the polynomials is clearly proportional to the corresponding precision requirements. However, notice that computing the Weber and $M_{D,l}(x)$ polynomials amounts to $2h$ evaluations of the eta function η, while for Ramanujan and $M_{D,p_1,p_2}(x)$ polynomials we need to evaluate the function $3h$ and $4h$ times respectively. This could be a disadvantage for Ramanujan and $M_{D,p_1,p_2}(x)$ polynomials, but this is not the case. In particular, it was shown in [25] that it is sufficient for any polynomial to precompute the values of η only for the h reduced quadratic forms. Finally, we note that the times required for the transformations of a root of a Weber, a Ramanujan and a $M_{D,l}(x)$ polynomial to a root of the corresponding Hilbert polynomial are approximately the same. The situation gets worse when $M_{D,p_1,p_2}(x)$ polynomials are used, because the time for the transformation and the storage of the modular polynomials are larger.

Finally, as noted in [38,18], the values $D \equiv 3 \bmod 8$ are most suited also for the construction of MNT curves. This means that Ramanujan polynomials are the best choice also for the construction of these special curves.

5.2. Ramanujan versus Weber polynomials for $D \not\equiv 3 \bmod 8$

In the previous section it was proved that Ramanujan polynomials require much less precision than all other class polynomials which can be used for discriminants $D \equiv 3 \bmod 8$. This is a considerable advantage of Ramanujan polynomials if someone wants to construct prime order elliptic curves or MNT curves where it is necessary to use such discriminants. However, in the case of non-prime elliptic curves, every possible square-free discriminant D can be used. This means that all cases of Weber polynomials mentioned in Section 2.2.2 can be employed, together with $M_{D,l}(x)$, $M_{D,p_1,p_2}(x)$ and Ramanujan polynomials. Using Lemma 4 we can estimate the precision requirements of every class polynomial. In particular, an estimation of the precision requirements of Weber polynomials will be equal to the estimations given in Tables 1 and 2. On the basis of these estimations, the choice of Weber polynomials with $D \equiv 7 \bmod 8$ and $D \not\equiv 0 \bmod 3$ seems to be the best among all class polynomials.

From these two tables, we see that only this case of Weber polynomials can be constructed more efficiently than Ramanujan polynomials. Interestingly, this might not be true in practice. It was noted in [39] that for comparable values of D, the minimum value of the class number (e.g. the degree of the corresponding polynomial) $h(-D)$ accessible using the residue $3 \bmod 8$ is approximately three times smaller than that for $7 \bmod 8$. According to [39], this result can be derived from [40, Cor. 5.3.13]. If this is true on average, then the use of Ramanujan polynomials can be more advantageous than the use of Weber polynomials for $D \equiv 7 \bmod 8$ (because their degree will be three times smaller for comparable values of D).

In order to determine whether this is true in practice, we calculated the class number for 100 comparable values of the discriminant D, for each one of the cases $D \equiv 7 \bmod 8$ and $D \equiv 11 \bmod 24$. We started with a value D close to $2594073385461405696 \approx 2.6 \cdot 10^{18}$ and to a value $25940733853636569600 \approx 2.6 \cdot 10^{20}$. In Fig. 2(left) we present for these 100 values of D the corresponding class number h for $D \equiv 11 \bmod 24$ and $D \equiv 7 \bmod 8$. We have noted that for most of the values D, the class number for polynomials with $D \equiv 7 \bmod 8$ is indeed much larger than the class number

for polynomials with $D \equiv 11 \mod 24$. In Fig. 2(right), we have computed the mean value of the class numbers for every group of 10 discriminants D. It is clear that on average, the degree of Ramanujan polynomials is much smaller than the degree of Weber polynomials with $D \equiv 7 \mod 8$ for comparable values of the discriminant. The (surprising) consequence of this result is that in many cases the construction of a Ramanujan polynomial will have less precision and lower storage requirements compared to a Weber polynomial with $D \equiv 7 \mod 8$.

6. Conclusions

We have introduced Ramanujan polynomials in the generation of elliptic curves by providing a new efficient method for their construction based on quadratic forms. We showed that Ramanujan polynomials are clearly superior in every aspect to all previously used class polynomials for all values of the discriminant $D \equiv 3 \mod 8$ and therefore their use is particularly favoured in the CM method for the generation of prime order ECs or MNT curves. Even in the case where someone applies the CM method for the generation of non-prime ECs, Ramanujan polynomials are among the best choices.

References

[1] G. Frey, H.G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, Mathematics of Computation 62 (1994) 865–874.
[2] A.J. Menezes, T. Okamoto, S.A. Vanstone, Reducing elliptic curve logarithms to a finite field, Institute of Electrical and Electronics Engineers. Transactions on Information Theory 39 (1993) 1639–1646.
[3] G.C. Pohlig, M.E. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, Institute of Electrical and Electronics Engineers. Transactions on Information Theory 24 (1978) 106–110.
[4] T. Satoh, K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, Commentarii Mathematici Universitatis Sancti Pauli 47 (1998) 81–91.
[5] E. Savaş, T.A. Schmidt, Ç.K. Koç, Generating elliptic curves of prime order, in: Cryptographic Hardware and Embedded Systems, CHES 2001, in: LNCS, Vol. 2162, Springer-Verlag, 2001, pp. 145–161.
[6] A.O.L. Atkin, F. Morain, Elliptic curves and primality proving, Mathematics of Computation 61 (1993) 29–67.
[7] G.J. Lay, H. Zimmer, Constructing elliptic curves with given group order over large finite fields, in: Algorithmic Number Theory, ANTS-I, in: LNCS, vol. 877, Springer-Verlag, 1994, pp. 250–263.
[8] R. Schoof, Counting points on elliptic curves over finite fields, Journal de Theorie des Nombres de Bordeaux 7 (1995) 219–254.
[9] R. Schertz, Weber's class invariants revisited, Journal de Théorie des Nombres de Bordeaux 4 (2002) 325–343.
[10] F. Morain, Modular curves and class invariants, June 2000, preprint.
[11] A. Enge, R. Schertz, Constructing elliptic curves over finite fields using double eta-quotients, Journal de Théorie des Nombres de Bordeaux 16 (2004) 555–568.
[12] S. Ramanujan, Notebooks. Vols. 1, 2, Tata Institute of Fundamental Research, Bombay, 1957.
[13] B.C. Berndt, H.H. Chan, Ramanujan and the modular j-invariant, Canadian Mathematical Bulletin 42 (4) (1999) 427–440.
[14] A. Gee, Class invariants by Shimura's reciprocity law, Journal de Théorie des Nombres de Bordeaux 11 (1999) 45–72.
[15] A. Gee, P. Stevenhagen, Generating class fields using Shimura reciprocity, in: Algorithmic Number Theory (Portland, OR, 1998), in: LNCS, vol. 1423, Springer-Verlag, 1998, pp. 441–453.
[16] E. Konstantinou, A. Kontogeorgis, Computing polynomials of the Ramanujan t_n class invariants, Canadian Mathematical Bulletin 52 (4) (2009) 583–597.
[17] A. Miyaji, M. Nakabayashi, S. Takano, New explicit conditions of elliptic curve traces for FR-reduction, IEICE Transactions on Fundamentals E84-A (5) (2001) 1234–1243.
[18] M. Scott, P.S.L.M. Barreto, Generating more MNT elliptic curves, Designs, Codes and Cryptography 38 (2006) 209–217.
[19] D.A. Cox, Primes of the Form $x^2 + ny^2$, John Wiley and Sons, New York, 1989.
[20] R.M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall, CRC, 2006.
[21] I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, in: London Mathematical Society Lecture Note Series, vol. 265, Cambridge University Press, 1999.
[22] J.H. Silverman, The Arithmetic of Elliptic Curves, in: GTM, vol. 106, Springer-Verlag, 1986.
[23] Y. Nogami, Y. Morikawa, A method for distinguishing the two candidate elliptic curves in CM method, in: International Conference on Information Security and Cryptology, ICISC 2004, in: LNCS, vol. 3506, Springer-Verlag, 2005, pp. 249–260.
[24] K. Rubin, A. Silverberg, Choosing the correct elliptic curve in the CM method, Mathematics of Computation 79 (2010) 545–561.
[25] A. Enge, F. Morain, Comparing invariants for class fields of imaginary quadratic fields, in: Algebraic Number Theory, ANTS V, in: LNCS, vol. 2369, Springer-Verlag, 2002, pp. 252–266.
[26] A. Enge, R. Schertz, Constructing elliptic curves from modular curves of positive genus, 2003, preprint.
[27] IEEE P1363/D13, Standard Specifications for Public-Key Cryptography, 1999. http://grouper.ieee.org/groups/1363/tradPK/draft.html.
[28] E.R. Berlekamp, Factoring polynomials over large finite fields, Mathematics of Computation 24 (1970) 713–735.
[29] A. Enge, R. Schertz, Modular curves of composite level, Acta Arithmetica 118 (2) (2005) 129–141.
[30] I. Stewart, Galois Theory, third ed., Chapman & Hall, CRC, Boca Raton, FL, 2004.
[31] I. Stewart, D. Tall, Algebraic Number Theory, second ed., Chapman & Hall, London, 1987.
[32] F. Morain, Construction of Hilbert class fields of imaginary quadratic fields and dihedral equation modulo p, Report 1087, INRIA, 1989.
[33] M. Hindry, J. Silverman, Diophantine geometry An introduction, in: Graduate Texts in Mathematics, Springer-Verlag, New York, 2000.
[34] R. Bröker, P. Stevenhagen, Constructing elliptic curves of prime order, Contemporary Mathematics 463 (2008) 17–28.
[35] P. Sarnak, Selberg's eigenvalue conjecture, Notices of the American Mathematical Society 42 (11) (1995) 1272–1277.
[36] PARI/GP, version 2.3.1, Bordeaux, 2005. Available at: http://pari.math.u-bordeaux.fr/.
[37] GNU multiple precision library, edition 4.2.1, 2007. Available at: http://www.swox.com/gmp.
[38] D. Page, N.P. Smart, E. Vercauteren, A comparison of MNT curves and supersingular curves, Applicable Algebra in Engineering, Communication and Computing 17 (2006) 379–392.
[39] D. Broadhurst, Solutions by radicals at singular values k_N from new class invariants for $N \equiv 3 \mod 8$, July 2008. Arxiv:0807.2976v3.
[40] H. Cohen, A Course in Computational Algebraic Number Theory, in: Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1996.