IRREDUCIBILITY OF SOME FABER POLYNOMIALS

P. GUERZHOY*

Abstract. Apply weight 0 Hecke operators to the modular function j and express the result as a polynomial in j. These polynomials were considered long ago in analysis, and recently attracted the attention of number theorists primarily for their connection with Borcherds' infinite products. In particular, Ken Ono conjectured that all of them are irreducible. We prove a partial result towards this conjecture by presenting infinite families of these polynomials which are proved to be irreducible.

Let $E_4 = 1 + 240 \sum_{n>0} \sum_{d|n} d^3 q^n$ and $E_6 = 1 - 504 \sum_{n>0} \sum_{d|n} d^5 q^n$ be the Eisenstein series of weights 4 and 6 correspondingly, and let

$$j(\tau) = 1728 \frac{E_4^3}{E_4^3 - E_6^2} = q^{-1} + 744 + 19688q + ... \tag{1}$$

denote the usual elliptic modular function on $SL(2, \mathbb{Z})$ ($q = e^{2\pi i \tau}$ throughout). It is well-known that the q-expansion coefficients for j are rational integers. This follows from the definitions of E_4 and E_6 combined with the identity

$$E_4^3 - E_6^2 = 1728q \prod_{n \geq 1} (1 - q^n)^{24}.$$

Following [1], [7], [2] we denote by j_m, for a positive integer m, the unique modular function which is holomorphic on the upper half of the complex plane and has the Fourier expansion of the form $j_m(\tau) = q^{-m} + \mathcal{O}(q)$. Each j_m is a monic polynomial of degree m in j with rational integer coefficients:

$$\phi_m(j) := j_m(\tau) = j^m + a(m, 1) j^{m-1} + \ldots + a(m, m). \tag{2}$$

One also obtains these polynomials from the action of weight 0 Hecke operators on j, namely $m(j - 744)|T_m = \phi_m(j)$. In particular,

$$\phi_0 = 1, \quad \phi_1(z) = z - 744, \quad \phi_2(z) = z^2 - 1488z + 159768, \quad \ldots.$$

The polynomials ϕ_m were introduced a century ago by Faber [4] and since then were widely studied mainly in the analytic context.

1991 *Mathematics Subject Classification.* Primary 11F33; Secondary 11F03.
*Supported by NSF grant DMS-0501225.

Their arithmetic significance was recognized recently particulary in the connection with Borcherds products [7], [2], [1].

It was shown in [1] that the polynomials ϕ_m have only real roots. Ken Ono recently [6, Problem 4.30] asked whether these polynomials are irreducible (here and in the following irreducibility is considered over the rationals). In this paper we prove, in particular, that there are infinitely many m such that ϕ_m is irreducible.

Theorem 1. *Let p be a prime. Define the integers r_n by the series decomposition*

$$\frac{72E_4^2E_6}{41E_4^3+31E_6^2}=\sum_{n\geq 0} r_n q^n. \tag{3}$$

If r_p is not divisible by p^2, then for $m=p^k$ with any positive integer k the polynomials ϕ_m are irreducible.

Remark 1. The numbers r_n are integers. We will show below that $r_p \equiv 0 \bmod p$.

Theorem 1 provides a criterion that allows us to check numerically whether the polynomials ϕ_{p^l} are irreducible. Specific machine computation shows that the number r_p is not divisible by p^2 for all primes $p \leq 12097$ with the exception of $p=2$ and $p=761$. This observation combined with Theorem 1 implies the following.

Corollary 1. *If p is an odd prime different from* 761 *and $p \leq 12097$, then for any $k>0$ the polynomials ϕ_{p^k} are irreducible.*

The rest of the paper is devoted to the proof of Theorem 1, reducing the statement to the Eisenstein irreducibility criterion.

We need the identity

$$j(\tau)-z=q^{-1}\exp\left(-\sum_{m\geq 1}\phi_m(z)\frac{q^m}{m}\right), \quad \Im(\tau)\gg 0, \tag{4}$$

which appears in [7]. This identity is equivalent to the famous denominator formula for the monster Lie algebra and is proven in [2].

Proposition 1. *Let p be a prime. For any positive integers k,l such that $1\leq l\leq p^k-1$, the polynomial coefficients $a(p^k,p^k-l)$ are divisible by p.*

Proof. Take logarithmic derivatives of both sides of (4) with respect to z:

$$\frac{1}{j-z}=\sum_{m\geq 1}\frac{1}{m}\phi_m'(z)q^m.$$

Differentiate this identity $l-1$ times with respect to z:

$$(l-1)!\frac{1}{(j-z)^l} = \sum_{m\geq 1} \frac{1}{m}\phi_m^{(l)}(z)q^m.$$

Put $z=0$ in the above identity and divide both sides by $(l-1)!$:

$$\frac{1}{j^l} = \sum_{m\geq 1} \frac{l}{m} a(m, m-l)q^m.$$

Notice that since $qj \in 1+\mathbb{Z}[[q]]$, the left-hand side, and, therefore, also the right-hand side of the latter identity belongs to $\mathbb{Z}[[q]]$. It follows that for $1 \leq l \leq p^k - 1$,

$$\frac{l}{p^k} a(p^k, p^k - l) \in \mathbb{Z},$$

which implies the divisibility claimed in Proposition 1. □

As an immediate consequence of Proposition 1, we record the following statement.

Proposition 2. *Let p be a prime, b an arbitrary integer and k a positive integer. All the coefficients of the polynomial $\phi_{p^k}(z+b)$, except the leading coefficient and possibly the constant term, are divisible by p*

Define the functions $c_n(z)$ of complex variable z and positive integer indices n by the infinite product expansion:

$$j(\tau) - z = q^{-1}\prod_{n\geq 1}(1-q^n)^{c_n(z)}. \tag{5}$$

We need the connection between the numbers $c_n(z)$ and the values $\phi_m(z)$ which is provided in [5, Proposition 1] (the idea goes back to [3]). For the sake of completeness we state and prove here the following statement.

Proposition 3. *The functions $c_n(z)$ are polynomials of degree n. Moreover,*

$$c_n(z) = \frac{1}{n}\sum_{d|n}\mu(n/d)\phi_d(z) \quad \textit{and} \quad \phi_m(z) = \sum_{d|m} dc_d(z), \tag{6}$$

where μ denotes the Möbius function.

Proof. Take the logarithm of both sides of the product expansion (5), expand $\log(1-q^n)$ as a power series in q, and rearrange the terms to

obtain

$$\log(j(\tau)-z)=\log(q^{-1})-\sum_{m\geq 1}\left(\sum_{d|m}dc_d(z)\right)\frac{q^m}{m}. \tag{7}$$

On the other side, take the logarithm of (4) and equate the corresponding coefficients to obtain

$$\phi_m(z)=\sum_{d|m}dc_d(z).$$

An application of the Möbius inversion formula finishes the proof. □

Now we analyze the constant terms of the polynomials.

Proposition 4. *Let p be a prime, b an arbitrary integer and k a positive integer. The modulo p^2 residue of the constant term of the polynomial $\phi_{p^k}(z+b)$ does not depend on k.*

Proof. It is sufficient to prove that for any $z\in\mathbb{Z}$ and $k\geq 1$

$$\phi_{p^k}(z)\equiv\phi_p(z) \bmod p^2. \tag{8}$$

Note that it follows from the definition (5) of the functions $c_n(z)$ that $c_n(z)\in\mathbb{Z}$ if $z\in\mathbb{Z}$. Indeed, (5) provides an inductive procedure for calculation of $c_n(z)$ which does not involve any denominators. Since $z\in\mathbb{Z}$ implies $(j-z)q\in 1+q\mathbb{Z}[[q]]$, an induction argument in n guarantees $c_n(z)\in\mathbb{Z}$.

It follows from (6) that

$$\phi_p(z)=c_1(z)+pc_p(z) \tag{9}$$

and

$$\phi_{p^k}(z)=c_1(z)+pc_p(z)+p^2c_{p^2}(z)+\ldots\equiv\phi_p(z) \bmod p^2,$$

as it was claimed. □

We are now in a position to finish the proof of Theorem 1. Note that $c_1(z)=\phi_1(z)=z-744$. It follows from Propositions 2 and 4 that all the coefficients except the leading one of the monic polynomial $\phi_{p^k}(z+744)$ are divisible by p. The residue of its constant term modulo p^2 is equal to $\phi_p(744)$ modulo p^2 due to Proposition 4. It follows from (9) that $\phi_p(744)\equiv 0 \bmod p$. Differentiate the identity (4) logarithmically with respect to τ and take into the account the identity

$$\frac{-1}{2\pi i}j'(\tau)=1728\frac{E_4^2E_6}{E_4^3-E_6^2}$$

to obtain

$$1728\frac{E_4^2E_6}{E_4^3-E_6^2}\frac{1}{j-z}=\sum_{n\geq 0}\phi_n(z)q^n.$$

Put $z = 744$ and make use of (1) to find out that the left-hand side of the last identity coincides with the left-hand side of (3). It follows that $\phi_p(744) = r_p$. The statement of Theorem 1 now follows from the Eisenstein irreducibility criterion.

References

[1] Asai, Tetsuya, Kaneko, Masanobu and Ninomiya, Hirohito, Zeros of certain modular functions and an application, Comment. Math. Univ. St. Paul. 46 (1997), no. 1, 93–101.

[2] Bruinier, Jan H., Kohnen, Winfried and Ono, Ken, The arithmetic of the values of modular functions and the divisors of modular forms, to appear in Compos. Math.

[3] Eholzer, Wolfgang, Skoruppa, Nils-Peter, Product expansions of conformal characters, Phys. Lett. B 388 (1996), no. 1, 82–89.

[4] Faber, G., Über polynomische Entwickelungen, Math. Ann. 57(1903), 389-408.

[5] Guerzhoy, P., A remark on congruences for coefficients of Faber polynomials, to appear.

[6] Ono, Ken, The Web of Modularity: Arithmetics of the Coefficients of Modular Forms and q-series, CBMS Reg. Conf. Ser. Math., 102, Amer. Math. Soc. Providence RI, 2004.

[7] Zagier, Don, Traces of singular moduli, Motives, Polylogarithms and Hodge Theory, Part I (Irvine, CA, 1998), 211–244, Int. Press Lect. Ser., 3, I, Int. Press, Somerville, MA, 2002

Deapartment of Mathematics, Temple University, 1805 N. Broad Str., Philadelphia, PA 19122

E-mail address: pasha@math.temple.edu