

A remark on congruences for coefficients of Faber polynomials.

P. Guerzhoy

1. Introduction.

Let $j(z) = q^{-1} + 744 + 19688q + \dots$ denote the usual elliptic modular function on $SL(2, \mathbb{Z})$ ($q = e^{2\pi i\tau}$ throughout). Following [1], [12], [4] we denote by j_m , for a positive integer m , the unique modular function which is holomorphic on \mathfrak{H} , the upper half of the complex plane and has the Fourier expansion of the form $j_m = q^{-m} + \mathcal{O}(q)$. Thus we have

$$j_0 = 1, \quad j_1 = j - 744, \quad j_2 = j^2 - 1488j + 159768, \dots$$

Each j_m is a monic polynomial of degree m in j with rational integer coefficients:

$$\phi_m(j) = j^m + a(m, 1)j^{m-1} + \dots + a(m, m). \quad (1)$$

One also obtains these polynomials from the action of weight 0 Hecke operators on j , namely $(j - 744)|T_m = m\phi_m(j)$ for $m \geq 1$. We put $\phi_0(j) = 1$.

The polynomials $\phi_m(j)$ were introduced a century ago by Faber [5] and since then were widely studied mainly in the analytic context. Their arithmetic significance was recognized recently in the connection with Borcherds products [12], [4], [3]. Their appearance in the connection with infinite products may be explained with the following simple observation.

Proposition 1. *Define the functions $c_n(z)$ of complex variable z and positive integer indeces n by the infinite product expansion:*

$$j(\tau) - z = q^{-1} \prod_{n \geq 1} (1 - q^n)^{c_n(z)}. \quad (2)$$

Then $c_n(z)$ turn out to be polynomials of degree n :

$$c_n(z) = \frac{1}{n} \sum_{d|n} \mu(n/d) \phi_d(z),$$

where μ denotes the Möbius function.

Proof. Take logarithm of both sides of the product expansion (2), expand $\log(1 - q^n)$ as a power series in q , and rearrange terms to obtain

$$\log(j(\tau) - z) = \log(q^{-1}) - \sum_{m \geq 1} \left(\sum_{d|m} dc_d(z) \right) \frac{q^m}{m}. \quad (3)$$

On the other side, one has the identity

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

which appears, in particular, in [12]. Take 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.

Proposition 1 provides a kind of polynomial interpolation for the infinite product expansions of the difference $j(\tau) - z$; if z specializes to one of the 13 exceptional integer values given in [2, Example 4, p.205], then, of course, (2) specializes to a Borcherds product.

An interesting and deep result about the zeros of polynomials ϕ_m was obtained in [1].

In this paper we record some congruences for the coefficients $a(m, n)$ of these polynomials. Roughly, these numbers appear to be highly divisible by powers of primes $p \equiv 2 \pmod{3}$. These congruences follow from the fact that certain formal q -series are p -adic modular forms (here and in the following we consider only p -adic modular forms in the sense of Serre [9]). This result and the methods to derive congruences out of it are closely related to those of [4], [3]. We formulate and prove this fact in Section 2, and apply it to obtain the congruences in Section 3, which also contains specific numerical examples.

The author is very grateful to W. Kohnen; his very nice talk at the Temple University Number Theory seminar attracted the author's attention to this nice area of research.

2. Formal q -series which are p -adic modular forms.

Theorem 1 *Let E be an elliptic curve defined over \mathbb{Q} , and let $j(E) \in \mathbb{Q}$ denote its j -invariant. For a rational prime p assume that E has good supersingular reduction at p . Then for any integer $l > 0$ the formal power series in $\mathbb{Q}[[q]]$ constructed as generating functions for the values at $j(E)$ of $(l-1)$ st and l th derivatives of the polynomials ϕ_n*

$$F_l = \sum_{n \geq 0} \phi_n^{(l-1)}(j(E))q^n$$

and

$$G_l = \sum_{n \geq 1} \frac{\phi_n^{(l)}(j(E))}{n} q^n$$

are p -adic modular forms of weights 2 and 0 respectively.

Note that this result is closely related to [3, Theorem 1]; in particular, our series F_1 coincides with one of the p -adic modular form constructed in this theorem.

Proof. Here and in the following E_k is the standard notation for Eisenstein series of weight k :

$$E_k = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n)q^n.$$

Logarithmic differentiation of (4) with respect to τ and z gives

$$\frac{E_{14}(\tau)}{\Delta(\tau)} \frac{1}{j(\tau) - z} = \sum_{n \geq 0} \phi_n(z)q^n,$$

where $\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$ is the unique normalized cusp form of weight 12, and

$$\frac{1}{j(\tau) - z} = \sum_{n \geq 1} \frac{\phi'_n(z)}{n} q^n.$$

Note that the above formulas for the generating functions were also obtained in [1]. Differentiating the above formulas repeatedly with respect to z , we obtain the q -expansion of meromorphic modular forms, namely, for and integer $l > 0$

$$(l-1)! \frac{E_{14}(\tau)}{\Delta(\tau)} \frac{1}{(j(\tau) - z)^l} = \sum_{n \geq 0} \phi_n^{(l-1)}(z)q^n$$

$$(l-1)! \frac{1}{(j(\tau) - z)^l} = \sum_{n \geq 1} \frac{\phi_n^{(l)}(z)}{n} q^n.$$

The congruence of two polynomials in X

$$\prod_{\tau_i, E_{p-1}(\tau_i)=0} (X - j(\tau_i)) \equiv \prod_{E_{ss}} (X - j(E_{ss})) \pmod{p}$$

follows from [7, Theorem 1]. The product in the left is over all the values τ_i in the fundamental domain of $SL_2(\mathbb{Z})$, for which $E_{p-1}(\tau_i) = 0$; it belongs to $\mathbb{Q}[[X]]$. The product in the right is the supersingular polynomial at p ; it is taken over all supersingular elliptic curves, E_{ss} , over $\overline{\mathbb{F}}_p$, and it is known to be a polynomial over \mathbb{F}_p . Since the elliptic curve E has good supersingular reduction at p , its j -invariant $j(E)$ should be a modulo p root of the supersingular polynomial: there is a E_{ss} such that $j(E) \equiv j(E_{ss}) \pmod{p}$ (the values $j(E_{ss})$ belong in fact to \mathbb{F}_{p^2}). Lift this particular $j(E_{ss})$ to $j^*(E_{ss}) = j(E) \in \mathbb{Q}$, and lift all the others to $j^*(E_{ss}) \in \mathbb{Q}$ conserving their residues modulo p , namely $j^*(E_{ss}) \equiv j(E_{ss}) \pmod{p}$. We thus have

$$\prod_{\tau_i, E_{p-1}(\tau_i)=0} (X - j(\tau_i)) \equiv \prod_{E_{ss}} (X - j^*(E_{ss})) \pmod{p}$$

as polynomials over \mathbb{Q} and therefore

$$\prod_{\tau_i, E_{p-1}(\tau_i)=0} (j - j(\tau_i)) \equiv \prod_{E_{ss}} (j - j^*(E_{ss})) \pmod{p}$$

as q -series. This implies that the modular form

$$\mathcal{E} = E_{p-1}(\tau) \frac{\prod_{E_{ss}} (j - j^*(E_{ss}))}{\prod_{\tau_i} (j - j(\tau_i))}$$

is holomorphic on the upper half-plane, vanishes at τ corresponding to the elliptic curve E (if $j(\tau) = j(E)$), and its q -expansion is congruent to that of E_{p-1} modulo p . Notice also the well known q -expansion congruence which is an easy consequence from the Kummer congruences for Bernoulli numbers $E_{p-1} \equiv 1 \pmod{p}$. To sum up, we have proved that

$$\mathcal{E}(\tau) = 0 \quad \text{for} \quad j(\tau) = j(E), \quad \text{and} \quad \mathcal{E} \equiv 1 \pmod{p}. \quad (5)$$

Remarks. 1 In the terminology of [3, Definition 3.1] we have shown that the modular forms F_l and G_l are good at p . The argument above is an adoption, to the case of a rational curve E , of the ideas of the proof of [3, Theorem 2], where a similar statement was proved for a modular form with a Heegner divisor.

2 Notice that the above argument may be adopted to a single CM point: the condition that the elliptic curve has good supersingular reduction at p corresponds to the condition that the prime p stays inert in the imaginary quadratic field.

3 We indicate also another way to construct a modular form \mathcal{E} which enjoys the required properties (5). The formal group of supersingular elliptic curve E has height 2, and one can follow the lines of [8] in order to show that the algebraic parts of the values of Eisenstein series $E_{p^M(p-1)}$ and $E_{p^N(p-1)}$ at τ corresponding to E for different (sufficiently big) positive integers M and N have different p -adic valuations. Since by Kummer congruences $E_{p^M(p-1)} \equiv E_{p^N(p-1)} \equiv 1 \pmod{p}$, one easily constructs \mathcal{E} as their linear combination. Notice also that this viewpoint reveals the importance of the supersingular reduction condition: the q -expansion principle forbids the existence of \mathcal{E} in the case of good ordinary reduction.

To finish the proof of Theorem 1 we multiply the meromorphic modular forms by sufficiently big powers of \mathcal{E} : their poles cancel with zeros of \mathcal{E} , and their q -expansion coefficients remain unchanged modulo big powers of p . In this way we obtain holomorphic modular forms whose reductions modulo any given power of p coincide with the reductions of F_l and G_l . This is what is claimed in Theorem 1.

3. Applications to congruences for the coefficients of the polynomials ϕ_n .

All the limits below should be considered in p -adic topology.

The fact that certain generating functions for the polynomials ϕ_n and their derivatives turn out to be p -adic modular forms implies congruences for the values of these polynomials. We remark that the methods below would work for any elliptic curve E defined over \mathbb{Q} , and for any prime p , where E has good supersingular reduction. It is most tempting, meanwhile, to plug in zero for the variable in a polynomial and its derivatives. For this reason we concentrate on the elliptic curve

$$E : y^2 = x^3 - 1$$

with $j(E) = 0$ corresponding to the point $\tau = (1 + \sqrt{-3})/2$. Since any prime $p \equiv 2 \pmod{3}$ is inert in $\mathbb{Q}(\sqrt{-3})$, the elliptic curve has good supersingular reduction at any such prime. The meromorphic modular forms under consideration become

$$F_l = \frac{E_{14}}{\Delta} \frac{1}{j^l} \quad G_l = \frac{1}{j^l}.$$

Remark that although j is not a p -adic modular form (some closely connected q -series are, see [10, §5]), our Theorem 1 implies that $1/j$ and its powers are p -adic modular forms as soon as $p \equiv 2 \pmod{3}$.

Recall that the rational integers $a(m, n)$ are defined by (1).

Theorem 2 *If $p \equiv 2 \pmod{3}$ is a prime then for any fixed $l > 0$ the powers of p which appear in the denominators of the rational numbers*

$$\frac{a(n, n-l)}{n}$$

are bounded.

Proof. Theorem 1 (with $j(E) = 0$) implies that for any $N > 0$ there is a holomorphic modular form Φ such that

$$\Phi - G_l \equiv 0 \pmod{p^N}. \quad (6)$$

The assertion of Theorem 2 follows now from the standard bounded denominator argument [11, Theorem 3.52].

Theorem 3 *Let $p \equiv 2 \pmod{3}$ be a prime, $l > 0$ and M be a positive integer. There exist positive real numbers $\alpha(M)$ and $\beta(M, l)$ such that*

$$\#\{n \leq x : \frac{a(n, n-l)}{n} \not\equiv 0 \pmod{p^M}\} = \mathcal{O}\left(\frac{x}{\log^{\beta(M, l)} x}\right)$$

There exists a positive integer $\gamma(M)$ such that

$$\#\{n \leq x : a(n, n) \not\equiv 0 \pmod{p^M}\} = \mathcal{O}\left(\frac{x}{\log^{\gamma(M)} x}\right)$$

Proof. The first result follows from Serre's theorem [10, Theorem 4.7] applied to (6). The second statement may be derived in the same way using the series F_l instead of G_l ; this coincides with [4, Theorem 6].

Another way to derive congruences from Theorem 1 is based on the following idea. Recall that the U_p -operator is defined for any q -series by

$$U_p : \sum c(n)q^n \mapsto \sum c(pn)q^n.$$

Applying this operator repeatedly, one kills the non- p -ordinary component and obtains the Hida's ordinary projector [6]:

$$\mathcal{H} = \lim_{n \rightarrow \infty} U^{(p-1)p^n}$$

If the p -ordinary component is small and can be identified independently, one obtains specific congruences. We apply these ideas to our modular forms F_l and G_l and record the results below.

Since for any $l > 0$

$$F_{l+1} = q \frac{d}{dq} G_l,$$

the p -adic cusp forms F_l for $l > 1$ have no p -ordinary component, and

$$\lim_{n \rightarrow \infty} U^n F_l = 0.$$

Thus we have

Theorem 4 *For any positive m and l and any prime $p \equiv 2 \pmod{3}$*

$$\lim_{n \rightarrow \infty} a(mp^n, mp^n - l) = 0.$$

At the same time, p -adic modular form F_1 of weight 2 has a p -ordinary component. Consider first the case when there are no p -ordinary p -adic cusp forms of weight 2. This happens [9, Remark, p. 217] when $p = 2, 3, 5, 7, 13$. In these cases we obtain for any p -adic modular form f of weight 2

$$\lim_{n \rightarrow \infty} U^n f = E_{2,p},$$

where

$$E_{2,p} = 1 - \frac{24}{p-1} \sum_{n \geq 1} \left(\sum_{\substack{d|n, \\ (d,p)=1}} d \right) q^n$$

is the p -adic Eisenstein series of weight 2 (it is complex-analytic with respect to $\Gamma_0(p)$). Equating the coefficients of q^n in the above identity, we obtain the following.

Theorem 5 *If $p = 5$ then for any positive integer m*

$$\frac{p-1}{24} \lim_{n \rightarrow \infty} a(mp^n, mp^n) = \sigma_1^*(m),$$

where $\sigma_1^*(m) = \sum_{\substack{d|m, \\ (d,p)=1}} d$.

The special case of this statement with $m = 1$ coincides with a special case of [4, Theorem 9] (see the remark after the quoted result). Note that other cases of the quoted theorem may also be generalized in the same way. For this, one may adopt our Theorem 1 to the case of a CM-point in $\mathbb{Q}(\sqrt{-D})$ (see Remark 2 in the proof of Theorem 1), obtain limit identities as in our Theorem 5, notice that the left-hand side belongs to the Hilbert class field, K , and take the trace from K to \mathbb{Q} . Since the number in the right side is rational, taking the trace will multiply it by the degree of K , which equals the Hurwitz class number $H(-D)$. Alternatively (and equivalently), one can make use of [3, Theorem 1]. The mild (from $m = 1$ to arbitrary positive m) generalization of [4, Theorem 9], which one obtains in this way is the following.

Theorem 6 *Suppose that $-D < -4$ is a fundamental discriminant of an imaginary quadratic field, and let τ be a Heegner point of discriminant $-D$. If $K = \mathbb{Q}(j(\tau))$, then the following is true. Let the prime $p \in \{2, 3, 5, 7, 13\}$ stay inert in $\mathbb{Q}(\sqrt{-D})$. For any positive integer m*

$$\frac{p-1}{24} \lim_{n \rightarrow \infty} \text{Tr}_{K/\mathbb{Q}} \phi_{mp^n}(j(\tau)) = H(-D) \sigma_1^*(m).$$

We remark that the prime $p = 13$ was omitted from the list in [4, Theorem 9] and [3, Corrolary 3] without any reason.

Consider now the case when there is exactly one p -ordinary p -adic cusp form of weight 2; this happens when $p = 11, 17, 19$. Since we want to stick to the coefficients of the polynomials ϕ_n , we have to choose $p = 11$ or 17, because we want $p \equiv 2 \pmod{3}$. Denote by $f_{2,p}$ the unique p -ordinary p -adic cusp form of weight 2, which coincides with the unique cusp form of weight 2 on $\Gamma_0(p)$ (see [6] for details):

$$f_{2,11} = q \prod_{m \geq 1} (1 - q^m)^2 (1 - q^{11m})^2 = \sum_{m \geq 1} b_{11}(m) q^m \quad \text{and} \quad f_{2,19} = \sum_{m \geq 1} b_{19}(m) q^m.$$

Theorem 7 *Let $p = 11$ or 17 . There exists a non-zero constant $A_p \in \mathbb{Q}_p$ such that for $m \geq 1$*

$$\frac{p-1}{24} \lim_{n \rightarrow \infty} a(mp^n, mp^n) = \sigma_1^*(m) + A_p b_p(m)$$

We have taken just $\lim_{n \rightarrow \infty} U_p^n$ as Hida's ordinary projector here since both $f_{2,p}$ and $E_{2,p}$ have 1 as eigenvalue of U_p . The nonvanishing of the constants A_p is not clear *a priori*; it comes from the fact that the claimed congruences hold even with $n = 0$:

$$\frac{p-1}{24} a(m, m) \equiv \sigma_1^*(m) + \alpha_p b_p(m) \pmod{p}$$

with $\alpha_{11} = 8$ and $\alpha_{17} = 13$. These congruences, can be also written as the modular forms congruences

$$\frac{p-1}{24} \left(\frac{E_6}{E_4} - E_2 \right) \equiv \alpha_p f_{2,p} \pmod{p},$$

where $E_2 = 1 - 24 \sum \sigma_1(n) q^n$ stands for the non-modular weight 2 Eisenstein series. These prove the non-vanishing statements and simultaneously illustrate Theorem 7.

Let us now consider the cusp p -adic modular forms G_l of weight zero from this viewpoint. The Hida's Control Theorem [6] implies that the dimension of the space of p -ordinary cusp forms of weight zero equals the dimension of the space of p -ordinary cusp forms of weight $p - 1$. It follows from [6, Proposition 7.2.2] that this last is definitely zero if there are no cusp forms of weight $p - 1$, namely, when $p = 2, 3, 5, 7$ and 11 . Thus we obtain the refinement of Theorem 4 for these primes.

Theorem 8 *Let $p = 2, 5$ or 11 . Then for any positive m and l*

$$\lim_{n \rightarrow \infty} \frac{1}{p^n} a(mp^n, mp^n - l) = 0.$$

Such a strong statement is not true for an arbitrary prime. Consider, for example, the case when the dimension of the space of p -ordinary cusp forms of weight $p - 1$ is one and $p \equiv 2 \pmod{3}$. This happens, in particular, for

$p = 17$ and 23 . An application of Hida's theory (Hida's Control Theorem and [6, Proposition 7.2.2]) implies the following result.

Theorem 9 For $p = 17$ or 23 denote by $d_p(m)$ the Fourier coefficients of the unique cusp form g_{p-1} of weight $p - 1$:

$$g_{p-1} = \sum_{m \geq 1} d_p(m) q^m.$$

Then for any positive l the limit

$$\lim_{n \rightarrow \infty} \frac{a(mp^{(p-1)p^n}, mp^{(p-1)p^n} - l)}{mp^{(p-1)p^n}}$$

exists, and for n big enough there exists a residue $B_p(l)$ modulo p (independent of m) such that

$$\frac{a(mp^n, mp^n - l)}{mp^n} \equiv B_p(l) d_p(m) \pmod{p}.$$

Examples. Let $p = 17$; then $g_{16} = E_4 \Delta$. If $l = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ then $n = 1$ is big enough, and the claimed congruence

$$U_{17}(1/j^l) \equiv B_{17}(l) E_4 \Delta \pmod{17}.$$

with the corresponding values $B_{17}(l) = 1, 13, 12, 2, 12, 12, 6, 13, 9, 14$ respectively. If $l = 10, 11, 12, 13$, then one may take $n = 2$ to obtain the claimed congruence

$$U_{17}^2(1/j^l) \equiv B_{17}(l) E_4 \Delta \pmod{17}.$$

with $B_{17}(l) = 13, 15, 13, 2$ respectively.

Now consider $p = 23$ with $g_{22} = E_4 E_6 \Delta$. If $l = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ then $n = 1$ is big enough, and

$$U_{23}(1/j^l) \equiv B_{23}(l) E_4 E_6 \Delta \pmod{23}$$

with $B_{23}(l) = 17, 3, 19, 9, 13, 3, 2, 6, 17, 17, 12, 3, 15, 11$.

R E F E R E N C E S

- [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] Borcherds, Richard E., Automorphic forms on $O_{s+2,2}(R)$ and infinite products, *Invent. Math.* 120 (1995), no. 1, 161–213.
- [3] Bruinier, Jan H. and Ono, Ken, The arithmetic of Borcherds’ exponents, preprint.
- [4] Bruinier, Jan H.; Kohlen, Winfried; Ono, Ken The arithmetic of the values of modular functions and the divisors of modular forms, *Compos. Math.* 140 (2004), no. 3, 552–566.
- [5] Faber, G., Über polynomische Entwicklungen, *Math. Ann.* 57(1903), 389–408.
- [6] Hida, Haruzo, Elementary theory of L -functions and Eisenstein series, London Mathematical Society Student Texts, 26. Cambridge University Press, Cambridge, 1993.
- [7] Kaneko, Masanobu and Zagier, Don Supersingular j -invariants, hypergeometric series, and Atkin’s orthogonal polynomials, *Computational perspectives on number theory* (Chicago, IL, 1995), 97–126, AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI, 1998.
- [8] Katz, Nicholas M., Divisibilities, congruences, and Cartier duality, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28 (1981), no. 3, 667–678 (1982).
- [9] Serre, Jean-Pierre, Formes modulaires et fonctions zêta p -adiques, Modular functions of one variable, III, Proc. Internat. Summer School, Univ. Antwerp, 1972, pp. 191–268, *Lecture Notes in Math.*, Vol. 350, Springer, Berlin, 1973.
- [10] Serre, Jean-Pierre, Divisibilité de certaines fonctions arithmétiques, *Enseignement Math.* (2) 22 (1976), no. 3-4, 227–260.

- [11] Shimura, Goro, Introduction to the arithmetic theory of automorphic functions, Kanô Memorial Lectures, Princeton University Press, Princeton, N.J., 1971.
- [12] 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..