PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 4, April 2007, Pages 1001–1005
S 0002-9939(06)08561-3
Article electronically published on October 13, 2006

ON ORDINARY PRIMES FOR MODULAR FORMS AND THE THETA OPERATOR

MASATAKA CHIDA AND MASANOBU KANEKO

(Communicated by Ken Ono)

Abstract. We give a criterion for a prime being ordinary for a modular form, by using the theta operator of Ramanujan.

1. Introduction and statement of the result

A normalized Hecke eigenform is said to be ordinary at a prime p if p does not divide its p-th Fourier coefficient. In the theory of p-adic modular forms and Galois representations attached to modular forms, this notion has fundamental importance, and there is extensive literature on the subject.

In the present paper, we shall give a criterion for ordinariness in terms of certain polynomials attached to derivatives of given modular forms. Throughout the paper, the modular forms considered are those on the full modular group $\mathrm{SL}_2(\mathbb{Z})$.

For any $f = f(z) = \sum_{n=0}^{\infty} a(n)q^n$ $(q = e^{2\pi i z})$, we define

$$\theta f := q\frac{d}{dq}f = \sum_{n=0}^{\infty} n\, a(n)q^n.$$

This is the derivative with respect to $2\pi i z$, and is often referred to as the "theta operator" of Ramanujan. The derivative of a modular form is no longer modular but "quasimodular", which means, in the case of $\mathrm{SL}_2(\mathbb{Z})$, that it is an isobaric element of the ring $\mathbb{C}[E_2, E_4, E_6]$. Here, $E_k = E_k(z)$ for even k is the standard Eisenstein series

$$E_k(z) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\Big(\sum_{d|n} d^{k-1}\Big)q^n,$$

B_k being the k-th Bernoulli number. For $k \geq 4$, the function $E_k(z)$ is modular of weight k, but $E_2(z)$ is not quite modular. The operator θ preserves the ring $\mathbb{C}[E_2, E_4, E_6]$ (as is seen by Ramanujan's formulae $\theta E_2 = (E_2^2 - E_4)/12$, $\theta E_4 = (E_2E_4 - E_6)/3$, $\theta E_6 = (E_2E_6 - E_4)/2$), and hence for any modular form f and non-negative integer n, $\theta^n f$ is an element in $\mathbb{C}[E_2, E_4, E_6]$.

To any $g \in \mathbb{C}[E_2, E_4, E_6]$, we attach a polynomial $F(g; X, Y, Z)$ in three variables so that

$$g(z) = F(g; E_2(z), E_4(z), E_6(z))$$

Received by the editors October 13, 2005 and, in revised form, November 15, 2005.
2000 *Mathematics Subject Classification.* Primary 11F33; Secondary 11F11.
Key words and phrases. Ordinary prime, theta operator.
The first author was supported in part by JSPS Research Fellowships for Young Scientists.

holds. We also define its "modular part" $F^{(0)}(g;Y,Z)$ by

$$F^{(0)}(g;Y,Z) := F(g;0,Y,Z).$$

If in particular g is modular (i.e., $g \in \mathbb{C}[E_4, E_6]$), then $F(g;X,Y,Z)$ is free from X and $F(g;X,Y,Z) = F^{(0)}(g;Y,Z)$. If g has p-integral Fourier coefficients, the polynomial F (and hence $F^{(0)}$) also has p-integral coefficients.

For a prime $p > 3$, set $H_p(Y,Z) = F^{(0)}(E_{p-1};Y,Z)(= F(E_{p-1};X,Y,Z))$. The polynomial $H_p(Y,Z)$ has p-integral coefficients, and $H_p(Y,Z) \bmod p$ is known as the "Hasse invariant" ([3], [4]).

Now we can state our main theorem.

Theorem 1.1. *Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ be a normalized eigencusp form of weight k and p a prime number greater than k. Then the following conditions are equivalent:*

1. $a(p) \not\equiv 0 \mod p$.
2. $H_p(Y,Z) \nmid F^{(0)}(\theta^{p-k+1}f;Y,Z) \mod p$.

2. Proof of the theorem and a corollary

In order to prove the theorem, we use the theory of filtration of modular forms modulo p developed by Swinnerton-Dyer [4], the theory of theta cycles by Tate [1], and a formula for the derivative $\theta^n f$. We first recall the definition of the filtration and then review theorems of Tate and Swinnerton-Dyer.

Let $M_k(\mathbb{Z}_{(p)})$ be the set of modular forms of weight k (on $\mathrm{SL}_2(\mathbb{Z})$) whose Fourier coefficients belong to $\mathbb{Z}_{(p)}$, the local ring of $\mathbb{Q}$ at p. Following [4], let $\widetilde{M_k}$ be the $\mathbb{F}_p$-vector space (in $\mathbb{F}_p[[q]]$) obtained from $M_k(\mathbb{Z}_{(p)})$ by reducing Fourier coefficients modulo p. We note that, since we have $E_{p-1} \equiv 1 \bmod p$ and $E_2 \equiv E_{p+1} \bmod p$ by the Kummer congruences of Bernoulli numbers, any quasimodular form having p-integral Fourier coefficients is congruent modulo p to a modular form of suitable weight.

Definition 2.1. For $f \in \widetilde{M_k}$, we define the filtration $w(f)$ of f to be the least ℓ such that f belongs to $\widetilde{M_\ell}$. For a modular or quasimodular form f whose Fourier coefficients are p-integral, we shall write $w(f)$ instead of $w(f \bmod p)$.

We call an element in $\widetilde{M_k}$ an eigenform if it is congruent modulo p to a Hecke-eigencusp form. Tate's theory of theta cycles connects the ordinariness of an eigenform f to the filtration of the derivative of f.

Proposition 2.2 (Tate [1])**.** *Let $f = \sum_{n=1}^{\infty} a(n)q^n \in \widetilde{M_k}$ be an eigenform. We assume $k < p$ and $w(f) = k$. Then we have*

$$w(\theta^{p-k+1}f) = \begin{cases} 2p-k+2 & \text{if } a(p) \not\equiv 0 \bmod p, \\ p-k+3 & \text{if } a(p) \equiv 0 \bmod p. \end{cases}$$

(In [1] the assumption is weaker (that f is in the kernel of the "U-operator"), but for our purpose it is enough to restrict to the case of eigenform.)

On the other hand, the filtration of a modular form g is related to the divisibility of $F^{(0)}(g;Y,Z) \bmod p$ by the Hasse invariant.

Proposition 2.3 (Swinnerton-Dyer [4, Lemma 5])**.** *For $g \in M_{k'}(\mathbb{Z}_{(p)})$, the following hold:*

(1) *If $w(g) = k'$, then $H_p(Y,Z) \nmid F^{(0)}(g;Y,Z) \mod p$.*
(2) *If $w(g) = k' - p + 1$, then $H_p(Y,Z) \mid F^{(0)}(g;Y,Z) \mod p$.*

Now assume that f is a normalized eigenform of weight k. The derivative $\theta^{p-k+1}f$ is quasimodular of weight $2p-k+2$. If $\theta^{p-k+1}f$ is congruent modulo p to a (true) modular form g of weight $2p-k+2$, then, combining Proposition 2.2 and Proposition 2.3 (with $k' = 2p-k+2$), the condition $a(p) \not\equiv 0 \bmod p$ is equivalent to the polynomial $F^{(0)}(g;Y,Z) \bmod p$ not being divisible by $H_p(Y,Z) \bmod p$. Our theorem is therefore a consequence of the following observation that we can indeed take g to be the modular part of $\theta^{p-k+1}f$. Here, for a quasimodular form $g = \sum_{i=0}^{m} g_i E_2^i,\ g_i \in \mathbb{C}[E_4, E_6]$, we call g_0 its modular part.

Lemma 2.4. *Let $p > 3$ be a prime and f a modular form of weight $k < p$ with p-integral Fourier coefficients. Then we have*

$$\theta^{p-k+1}f \equiv (\theta^{p-k+1}f)_0 \mod p.$$

This is a consequence of a general formula for $\theta^n f$ given in [5]. Recall that, if f is modular of weight k, then

$$\partial f := \theta f - \frac{k}{12} E_2 f$$

is modular of weight $k+2$. For a modular form f of weight k, define a sequence of modular forms f_r of weight $k+2r$ recursively by

$$f_{r+1} = \partial f_r - \frac{r(r+k-1)}{144} E_4 f_{r-1} \quad (r \geq 0)$$

with initial condition $f_0 = f$. Then the formula (37) in [5] is equivalent to the following closed formula.

Proposition 2.5. *Let f be a modular form of weight k. Then for any $n \geq 0$ we have*

$$\frac{\theta^n f}{n!} = \sum_{i=0}^{n} \left[k+n-1 i\right] \frac{f_{n-i}}{(n-i)!} \left(\frac{E_2}{12}\right)^i.$$

When $n = p-k+1$, the binomial coefficients $\binom{k+n-1}{i}$ are divisible by p for all $i > 0$, and hence Lemma 2.4 follows ($f_n = (\theta^n f)_0$). This completes the proof of the theorem. □

Here we give a corollary to the theorem. As in the theorem, assume that $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ is a normalized eigenform of weight k and p is a prime number greater than k. We denote by $b(l,m,n)$ the coefficient of $X^l Y^m Z^n$ in $F(\theta^{p-k+1}f; X,Y,Z)$:

$$F(\theta^{p-k+1}f; X,Y,Z) = \sum_{2l+4m+6n=2p-k+2} b(l,m,n) X^l Y^m Z^n.$$

Corollary 2.6. (1) *Assume that $k \equiv 0 \bmod 6$ and $p \equiv 2 \bmod 3$.*

$$\text{If } b\left(0,0,\frac{2p-k+2}{6}\right) \not\equiv 0 \bmod p, \text{ then } a(p) \not\equiv 0 \bmod p.$$

(2) *Assume that $k \equiv 0 \bmod 4$ and $p \equiv 3 \bmod 4$.*

$$\text{If } b\left(0,\frac{2p-k+2}{4},0\right) \not\equiv 0 \bmod p, \text{ then } a(p) \not\equiv 0 \bmod p.$$

Proof. We only prove (1), the proof of (2) being similar. Write

$$H_p(Y,Z) = \sum_{4m+6n=p-1} c(m,n) Y^m Z^n.$$

By the assumption, $p-1$ is not divisible by 6, and hence the term with $m=0$ does not occur on the right. Therefore, if $b(0,0,\frac{2p-k+2}{6}) \not\equiv 0 \bmod p$, the polynomial $F(\theta^{p-k+1}f;X,Y,Z) \bmod p$ is not a multiple of $H_p(Y,Z) \bmod p$, and thus $a(p) \not\equiv 0 \bmod p$ by Theorem 1.1. □

3. Relation to supersingular j-invariants of elliptic curves

We may rephrase the theorem in terms of the supersingular j-polynomial.

Let f be a modular form of weight k. Write $k = 12m + 4\delta + 6\varepsilon$ with $m \geq 0$, $\delta \in \{0,1,2\}$, $\varepsilon \in \{0,1\}$. Then there exists a unique polynomial $G(f;x)$ such that

$$f(z) = \Delta(z)^m E_4(z)^\delta E_6(z)^\varepsilon G(f;j(z)),$$

where $\Delta(z) = (E_4(z)^3 - E_6(z)^2)/1728$ is the discriminant function and $j(z) = E_4(z)^3/\Delta(z)$ is the modular invariant. Moreover we put

$$\widetilde{G}(f;x) := x^\delta (x-1728)^\varepsilon G(f;x).$$

For a prime number p, we define the supersingular j-polynomial $S_p(x)$ by

$$S_p(x) := \prod_{E/\overline{\mathbb{F}}_p:\,\text{supersingular}} (x - j(E)) \in \mathbb{F}_p[x],$$

where the product runs over the isomorphism classes of supersingular elliptic curves in characteristic p and $j(E)$ is the j-invariant of E. Assume $p > 3$. A theorem of Deligne (cf. [3], [2]) then asserts that

$$\widetilde{G}(E_{p-1};x) \equiv S_p(x) \bmod p.$$

By this and Theorem 1.1, we have the following.

Theorem 3.1. *The assumption being the same as in Theorem* 1.1*, the following conditions are equivalent:*

(1) $a(p) \not\equiv 0 \bmod p$.
(2) $S_p(x) \nmid \widetilde{G}((\theta^{p-k+1}f)_0;x) \bmod p$.

Acknowledgement

The first author would like to thank Ken Ono for his helpful comments on the last section.

References

[1] N. Jochnowitz, *A study of the local components of the Hecke algebra mod l*, Trans. Amer. Math. Soc. **270** (1982), no. 1, 253–267. MR0642340 (83e:10033a)

[2] M. Kaneko, D. Zagier, *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**. MR1486833 (99b:11064)

[3] J.-P. Serre, *Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer)*, Séminaire Bourbaki 1971/72, **416** (Œuvres, vol. 3, 74–88). MR0466020 (57:5904a)

[4] H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Lect. Notes. in Math. **350** (1973), 1–55. MR0406931 (53:10717a)

[5] D. Zagier, *Modular forms and differential operators*, Proc. Indian Acad. Sci. (Math. Sci.) **104** (1994), 57–75. MR1280058 (95d:11048)

Institute of Mathematics, Tohoku University, Aoba, Sendai, 980-8578, Japan
E-mail address: sa2m22@math.tohoku.ac.jp

Faculty of Mathematics, Kyushu University 33, Fukuoka, 812-8581, Japan
E-mail address: mkaneko@math.kyushu-u.ac.jp