

ON $U(p)$ -CONGRUENCES

P. GUERZHOY[†]

ABSTRACT. The phenomenon of $U(p)$ -congruences was recently studied by Ahlgren and Ono [1] and by Elkies, Ono and Yang [2]. We provide a necessary and sufficient condition which improves their general results.

Let

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \in \frac{1}{q}\mathbb{Z}[[q]]$$

be the usual elliptic modular function on $SL_2(\mathbb{Z})$ ($q := e^{2\pi i\tau}$ throughout). Recall that a modular form (on $SL_2(\mathbb{Z})$) is called weakly holomorphic if its only pole is at infinity. Every weakly holomorphic modular form of weight zero f on $SL_2(\mathbb{Z})$ is a polynomial F in j and has a q -expansion of the form

$$f = F(j) = \sum_{n \gg -\infty} a(n)q^n.$$

For a rational prime p the action of the $U = U(p)$ -operator on formal power series in the variable q is defined by $F \mapsto F|U$, where $F = \sum a(n)q^n$ and $F|U = \sum a(pn)q^n$. Denote by $\bar{j} \in \mathbb{F}_p[[q]]$ the modulo p coefficient-wise reduction of j . Recently Elkies, Ono and Yang in [2] considered the following question. For a monic polynomial $F(x) \in \mathbb{F}_p[x]$, under which conditions does there exist a polynomial $G(x) \in \mathbb{F}_p[x]$ such that

$$(1) \quad F(\bar{j})|U = G(\bar{j})$$

as power series in $\mathbb{F}_p[[q]]$? Note that $\deg(G) \leq \deg(F)/p$ since $j = q^{-1} + O(1)$. A special case of this question with $\deg(F) < p$ is considered in a recent paper by Ahlgren and Ono [1]. In this case $\deg(G) = 0$ or $-\infty$, and the question specializes as follows. For a polynomial $F(x) \in \mathbb{F}_p[x]$ of degree $< p$, under which conditions does the congruence

$$(2) \quad F(j)|U \equiv a(0) \pmod{p}.$$

1991 *Mathematics Subject Classification.* 11F33.

[†]Supported by NSF grant DMS-0501225.

hold? Ono in [4] calls (2) a $U(p)$ -congruence. We adopt this terminology and generalize it to (1). In this note we prove a simple necessary and sufficient condition for the $U(p)$ -congruence to hold.

Note that general $U(p)$ -congruences are not the primary focus of [1] and [2]. These projects are devoted to the interplay between singular moduli and class polynomials. In particular, general criteria for an arbitrary (monic) polynomial F to satisfy a $U(p)$ -congruence were obtained in loc. cit. and were applied to the case when F is a Hilbert class polynomial.

The author wants to thank Ken Ono for a valuable suggestion to prove a result in the generality corresponding to [2], whereas the initial version of this paper was bounded by the framework of [1].

Following [1] and [2], consider an arbitrary rational prime p and introduce the polynomial $S_p(x) \in \mathbb{F}_p[x]$ of degree $\lfloor \frac{p}{12} \rfloor$, which is a slight modification of the supersingular polynomial at p . More specifically, let $S_p(x) = 1$ if $p \leq 11$, and for $p > 11$ let

$$S_p(x) = \prod_{\substack{E/\overline{\mathbb{F}}_p \text{ supersingular} \\ j(E) \notin \{0, 1728\}}} (x - j(E)) \in \mathbb{F}_p[x],$$

where the product is taken over $\overline{\mathbb{F}}_p$ -isomorphism classes of supersingular elliptic curves E .

The general results pertaining to $U(p)$ -congruences, proved in [1] and [2], may be summarized as follows.

Theorem 0.

- (i) ([1, Theorem 2], [2, Theorem 2.3]) *If $S_p(x)^2 | F(x)$ then F satisfies a $U(p)$ -congruence.*
- (ii) ([1, Corollary 5], [2]) *If F satisfies a $U(p)$ -congruence, then $p \leq 12 \deg(F) + 1$.*

It is mentioned in [1, Theorem 2, Remark 1] that the sufficient double divisibility condition (i) is not necessary; the necessary condition (ii) is not sufficient. We present a necessary and sufficient condition in this paper.

Theorem 1. *Assume that $p > 3$. A monic polynomial $F(x) \in \mathbb{F}_p[x]$ satisfies a $U(p)$ -congruence if and only if its derivative $F'(x)$ is divisible by $S_p(x)$ in $\mathbb{F}_p[x]$.*

Remarks.

- (1) Our Theorem 1 immediately implies Theorem 0. Indeed, if $S_p(x)^2 | F(x)$, then $S_p | F'(x)$ (but not conversely), and, by Theorem 1, F satisfies a $U(p)$ -congruence, which proves (i). Conversely, if F satisfies a $U(p)$ -congruence, then, by Theorem 1, $S_p | F'(x)$, and therefore $p \leq 12 \deg(F) + 1$ since $\deg S_p = \lfloor \frac{p}{12} \rfloor$, which proves (ii).

(2) One can slightly generalize the notion of $U(p)$ -congruences (2) allowing repeated application of the U -operator. This generalization, however, does not bring anything new as soon as the degree of F is smaller than p . Using a result of Serre [5, Théorème 6 ii] (and our proof of Theorem 1) one proves that if the congruence

$$F(j)|U^m \equiv a(0) \pmod{p}$$

holds with some $m \geq 1$, then it holds for any $m \geq 1$.

(3) If $p \leq 11$ further divisibilities appear. For an arbitrary polynomial $F(x) \in \mathbb{Z}[x]$ and any positive integer α the results of Serre [5, Lemme 3] for $p < 11$, [5, Théorème 8, Exemple 1] and [6, Théorème 5.4] allow one to prove that the congruence

$$F(j)|U^m \equiv a(0) \pmod{p^\alpha}$$

holds if m is big enough.

Our proof of Theorem 1 is based on an idea of Serre [6, 6.16b], where a special case of a similar argument ($F(x) = x$ in loc. cit.) was left as an exercise to the reader.

Proof. We use the standard (Ramanujan) notations for the Eisenstein series of weights 4 and 6 and for the normalized cusp form of weight 12:

$$Q = 1 + 240 \sum_{n \geq 1} \sigma_3(n)q^n, \quad R = 1 - 504 \sum_{n \geq 1} \sigma_5(n)q^n, \quad \Delta = \frac{1}{1728}(Q^3 - R^2).$$

We denote by \bar{Q}, \bar{R} and $\bar{\Delta} \in \mathbb{F}_p[[q]]$ the coefficientwise modulo p reductions of the above series. The operator D (sometimes denoted by θ) acts on formal q -series and takes $\sum a(n)q^n$ to $\sum na(n)q^n$.

We begin with the identity $(F|U)^p = F - D^{p-1}F$ of power series over \mathbb{F}_p , which implies the identity

$$(3) \quad \bar{\Delta}^{bp}(F|U)^p = \bar{\Delta}^{bp}F - \bar{\Delta}^{bp}D^{p-1}F$$

for any positive integer b . Recall that a modulo p modular form is a power series in $\mathbb{F}_p[[q]]$ which coincides with a modulo p reduction of the q -expansion of a holomorphic modular form on $SL(2, \mathbb{Z})$ with rational p -integral q -expansion coefficients. We denote the space of modulo p modular forms by M . For $f \in M$ we denote by $w(f)$ its filtration. The definition and a detailed exposition of the theory of filtration are contained in [5, 6, 7].

If b is big enough (i.e. $b > (\deg F)/p$) all three terms in (3) belong to M . Indeed, evidently $\bar{\Delta}^{bp}F \in M$. Also $\bar{\Delta}^{bp}(F|U)^p \in M$ by [6, Théorème 5.4]. Then (3) implies $\bar{\Delta}^{bp}D^{p-1}F \in M$. Thus the filtrations of these terms are well-defined. We are particularly interested in

$w(\bar{\Delta}^b(F|U))$, and we are going to estimate the filtrations of the three terms in (3) in order to conclude that

$$(4) \quad w(\bar{\Delta}^b(F|U)) \begin{cases} = 12b + p - 1 & \text{if } S_p(x) \nmid F'(x) \text{ in } \mathbb{F}_p[x] \\ < 12b + p - 1 & \text{if } S_p(x) \mid F'(x) \text{ in } \mathbb{F}_p[x]. \end{cases}$$

We have

$$(5) \quad w(\bar{\Delta}^{bp}F) \leq 12bp.$$

It follows from [5, Lemme 1(b)] that

$$(6) \quad w(\bar{\Delta}^{bp}(F|U)^p) = w((\bar{\Delta}^b(F|U))^p) = pw(\bar{\Delta}^b(F|U)).$$

We now want to calculate the filtration $w(\bar{\Delta}^{bp}D^{p-1}F)$. The identity $D(j) = -Q^2R/\Delta$, chain rule for $a = 0$, product rule for $a > 0$ (D is a differential operator), and an induction argument in a imply that $\bar{\Delta}^{bp}D^{a+1}F \equiv -D^a(F'Q^2R\bar{\Delta}^{bp-1}) \pmod{p}$ for $a \geq 0$. Pick $a = p - 2$ and pass to the modulo p reductions to obtain

$$(7) \quad w(\bar{\Delta}^{bp}D^{p-1}F) = w(D^{p-2}(F'Q^2R\bar{\Delta}^{bp-1})).$$

We use the equality

$$w(\bar{\Delta}^m f) = 12m + w(f) \quad \text{for any positive integer } m \text{ and } f \in M,$$

which follows from [3, §10.7, Lemma (i)] (cf. the proof of [7, Lemma 5]), and [7, Lemma 5(i)] to conclude that

$$w(F'Q^2R\bar{\Delta}^{bp-1}) \begin{cases} = 12bp + 2 & \text{if } S_p(x) \nmid F'(x) \text{ in } \mathbb{F}_p[x] \\ < 12bp + 2 & \text{if } S_p(x) \mid F'(x) \text{ in } \mathbb{F}_p[x] \end{cases}$$

Notice that $12bp + 2 \equiv 2 \pmod{p}$ and apply [7, Lemma 5(ii)] combined with the identity (7) to conclude that

$$(8) \quad w(\bar{\Delta}^{bp}D^{p-1}F) \begin{cases} = p^2 + (12b - 1)p & \text{if } S_p(x) \nmid F'(x) \text{ in } \mathbb{F}_p[x] \\ < p^2 + (12b - 1)p & \text{if } S_p(x) \mid F'(x) \text{ in } \mathbb{F}_p[x]. \end{cases}$$

Filtration satisfies the ultrametric inequality $w(f+g) \leq \sup(w(f), w(g))$ for $f, g \in M$, which implies that $w(f+g) = \max(w(f), w(g))$ provided that $w(f) \neq w(g)$. We apply this observation to (3), taking into account (5), (6), (8), and the evident inequality $p^2 + (12b - 1)p > 12pb$, and obtain

$$pw(\bar{\Delta}^b(F|U)) \begin{cases} = p^2 + (12b - 1)p & \text{if } S_p(x) \nmid F'(x) \text{ in } \mathbb{F}_p[x] \\ < p^2 + (12b - 1)p & \text{if } S_p(x) \mid F'(x) \text{ in } \mathbb{F}_p[x], \end{cases}$$

which implies (4).

We now derive the statement of Theorem 1 from (4). Assume that $S_p(x) \mid F'(x)$ in $\mathbb{F}_p[x]$. It follows from [6, Théorème 5.4], that $\bar{\Delta}^b(F|U)$

is a modulo p reduction of a p -adic modular form of weight $12b$. Therefore by [5, Théorème 1] its filtration is $w(\Delta^b(F|U)) = w(\bar{\Delta}^b(F|U)) \equiv 12b \pmod{p-1}$. This observation together with the inequality in (4) implies that $w(\bar{\Delta}^b(F|U)) \leq 12b$. Thus there exists a modular form f on $SL_2(\mathbb{Z})$ of weight $12b$ such that $f \equiv \Delta^b(F|U) \pmod{p}$. It follows that $(F|U) \equiv f/\Delta^b \pmod{p}$. However, f/Δ^b is a modular form on $SL_2(\mathbb{Z})$ of weight zero with its only pole at infinity, which must be a polynomial in j . This proves that $F(x)$ satisfies a $U(p)$ -congruence if $S_p(x) \mid F'(x)$ in $\mathbb{F}_p[x]$.

Conversely, if the congruence (1) holds, then

$$w(\Delta^b(F|U)) = w(\Delta^b G) \leq 12b,$$

and it follows from (4) that $S_p(x) \mid F'(x)$ in $\mathbb{F}_p[x]$. □

REFERENCES

- [1] Ahlgren, Scott; Ono, Ken, Arithmetic of singular moduli and class polynomials, *Compos. Math.* 141 (2005), no. 2, 293–312.
- [2] Elkies, Noam; Ono, Ken; Yang, Tonghai, Reduction of CM elliptic curves and modular function congruences, *Int. Math. Res. Not.* (2005), no. 44, 2695–2707.
- [3] Lang, Serge, Introduction to modular forms, *Grundlehren der mathematischen Wissenschaften*, No. 222, Springer-Verlag, Berlin-New York, 1976.
- [4] Ono, Ken, The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q -series, *CBMS Reg. Conf. Ser. Math.*, 102, Amer. Math. Soc., Providence, RI, 2004.
- [5] 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.
- [6] Serre, Jean-Pierre, Divisibilité de certaines fonctions arithmétiques, *Enseignement Math.* (2) 22 (1976), no. 3-4, 227–260.
- [7] Swinnerton-Dyer, H. P. F., On l -adic representations and congruences for coefficients of modular forms, *Modular functions of one variable, III* (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 1–55, *Lecture Notes in Math.*, Vol. 350, Springer, Berlin, 1973.

UNIVERSITY OF HAWAII AT MANOA, DEPARTMENT OF MATHEMATICS, 2565
MCCARTHY MALL, HONOLULU, HI 96822-2273

E-mail address: p.guerzhoy@gmail.com