

Examples of congruences among modular forms

Jae-young Park

September 25, 2007

We'll prove the following identity

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

This identity can be interpreted as a congruence between the Fourier coefficients of the unique normalized cusp form of weight 12 and the Eisenstein series of the same weight. So this is an easy example of the previous week Prop. 3.4 which we did find a semi cusp form which is congruent to Eisenstein series $G_k = -\frac{B_k}{2k} + \sum_{n \geq 1} \sum_{d|n} d^{k-1} q^n = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$ where $q = e^{2\pi i}$.

Using Eisenstein series,

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

,in particular, $E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n$ and $E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n$, we can construct a form h of weight k with constant term 1 having integral coefficients. Let $f = G_k + \frac{B_k}{2k} h$. Then f is a cusp form of weight k . Let N_k be a numerator of $\frac{B_k}{2k}$ in its reduced form. Then we have

$$f \equiv G_k \pmod{N_k}$$

For $k = 12$, we have $B_{12} = -\frac{691}{2730}$. Since $\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$ is the unique cusp form with first Fourier coefficient 1, we have

$$\Delta(z) \equiv G_{12}(z) \pmod{691}.$$

So we get the Ramanujan's identity.

Ramanujan's identity can be viewed in terms of galois representation. In 1969, Serre made the following conjecture which was proved by Deligne.

Conjecture 1. *For each prime l , there exists a continuous linear representation*

$$\rho_l : Gal(K_l/\mathbb{Q}) \rightarrow Aut(V_l),$$

where V_l is a \mathbb{Q}_l - vector space of dimension 2 which satisfies the following condition: For each prime $p \neq l$, we have

$$Tr(\rho_l(F_p)) = \tau(p) \quad det(\rho_l(F_p)) = p^{11}$$

It is immediate that such representation gives the Ramanujan's identity.

The image of ρ_l need to be "small" to have a congruence. Since it is "as large as possible" for prime other than 2,3,5,7, 23, 691 we don't have a congruence for prime except these.

1 The image of $\rho_{l,1} : Gal(K_l/\mathbb{Q}) \rightarrow GL(2, \mathbb{Z}/l\mathbb{Z})$ for $l = 691$

We calculate the image of $\rho_1 = \rho_{691,1}$. Let $G_1 = Im\rho_1$ and $\rho_2 = \rho_{691,2} : Gal(K_l/\mathbb{Q}) \rightarrow GL(2, \mathbb{Z}/l^2\mathbb{Z})$.

Fact 1. *After conjugation by an element of $GL(2, \mathbb{Z}/l\mathbb{Z})$, we may assume $G_1 \subseteq F = \left\{ \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/l\mathbb{Z})^*, x \in \mathbb{Z}/l\mathbb{Z} \right\}$ and $\rho_1(Frob_p) = \begin{pmatrix} p^{k-1} & x \\ 0 & 1 \end{pmatrix}$*

$l = 691$ satisfies the following property with $p = 6911, k = 12$

Fact 2. *there exists a prime $p \equiv 1 \pmod{l}$ such that $a_p - p^{k-1} - 1 \not\equiv 0 \pmod{l^2}$*

We claim that $G_1 = F$. Note that G_1 contains every element of order dividing $l - 1$.¹ If $G_1 \neq F$, G_1 can be mapped under conjugation by an element of F into the subgroup

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, a \in (\mathbb{Z}/l\mathbb{Z})^* \right\}$$

Consider the canonical epimorphism $\pi : GL(2, \mathbb{Z}/l^2\mathbb{Z}) \rightarrow GL(2, \mathbb{Z}/l\mathbb{Z})$ which is compatible ρ_1, ρ_2 . If $G_1 \neq F$, the preimage of G_1 under π would consist of

$$\begin{pmatrix} a + lA & lB \\ lC & 1 + lD \end{pmatrix}$$

If $p \equiv 1 \pmod{l}$, then $\rho_2(Frob_p)$ would have a representative of the form²

$$\begin{pmatrix} 1 + lA & lB \\ lC & 1 + lD \end{pmatrix}$$

Recall that $tr(\rho_2(Frob_p)) \equiv a_p \pmod{l^2}$ and $\det(\rho_2(Frob_p)) \equiv p^{k-1} \pmod{l^2}$. Then we have

$$a_p - p^{k-1} - 1 \equiv tr - \det - 1 \equiv 2 + l(A+D) - (1+lA)(1+lD) + l^2BC - 1 \equiv 0 \pmod{l^2}$$

But for $p = 6911, k = 12, l = 691$ we have $a + p - p^{k-1} - 1 \not\equiv 0 \pmod{l^2}$, which is a contradiction.

References

1. Serre, J-P, Une interpretation des congruences relatives a la fonction de Ramanujan, Semin. Delange-Pisot-Poitou 9 (1967/68), Theorie Nombres, No.14, 17p. (1969).
2. A. A. Panchishkin, There exist no ramanujan congruences mod 691^2 ,

¹Element of order $l - 1$ is of the form $\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix}$ with $a \neq 1 \in (\mathbb{Z}/l\mathbb{Z})^*$. Since $(k - 1, l - 1) = 1$, we can take a generator $\alpha \in (\mathbb{Z}/l\mathbb{Z})^*$ such that $a \equiv \alpha^{k-1} \pmod{l}$. Taking a prime $p \equiv \alpha \pmod{l}$, we can conclude that $\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p^{k-1} & x \\ 0 & 1 \end{pmatrix} = \rho_1(Frob_p)$

² $\det \rho_2(Frob_p) \equiv p^{k-1} \equiv 1 \pmod{l}$