Computing congruences of modular forms modulo prime powers

Gabor Wiese

(joint work with Xavier Taixés i Ventosa)

Institut für Experimentelle Mathematik

Universität Duisburg-Essen

16 November 2009

Plan

(I) Congruences mod ℓ^n.

(II) Computing them.

(III) Modular forms mod ℓ^n.

(IV) Examples and applications.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruences mod ℓ^n (black board).

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Next: Computing congruences mod ℓ^n.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Computing congruences mod ℓ^n

Problem: Let $P, Q \in \mathbb{Z}[X]$ be monic coprime polynomials.

For which prime powers ℓ^n are there $\alpha, \beta \in \overline{\mathbb{Z}}$ such that

(i) $P(\alpha) = Q(\beta) = 0$ and

(ii) $\alpha \equiv \beta \mod \ell^n$?

Partial solution (very fast):

Reduced resultant = congruence number (global).

Complete solution:

Newton polygon method (local).

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$P(X) = \sum_{k=0}^{u} a_k X^{u-k}, \quad Q(X) = \sum_{k=0}^{v} b_k X^{v-k} \in \mathbb{Z}[X]$.

Sylvester map:

$$\begin{array}{ccccc} \mathbb{Z}[X]_{<v} & \times & \mathbb{Z}[X]_{<u} & \xrightarrow{(r,s)\mapsto rP+sQ} & \mathbb{Z}[X]_{<u+v} \\ \{X^{v-1},\ldots,X,1\} & & \{X^{u-1},\ldots,X,1\} & & \{X^{u+v-1},\ldots,X,1\}. \end{array}$$

Congruence number

$P(X) = \sum_{k=0}^{u} a_k X^{u-k}$, $\quad Q(X) = \sum_{k=0}^{v} b_k X^{v-k} \in \mathbb{Z}[X]$.

Sylvester map:

$$\begin{array}{ccccc} \mathbb{Z}[X]_{<v} & \times & \mathbb{Z}[X]_{<u} & \xrightarrow{(r,s)\mapsto rP+sQ} & \mathbb{Z}[X]_{<u+v} \\ \{X^{v-1},\dots,X,1\} & & \{X^{u-1},\dots,X,1\} & & \{X^{u+v-1},\dots,X,1\}. \end{array}$$

Sylvester matrix (for column vectors) with $u = 3$ and $v = 2$:

$$\begin{pmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{pmatrix}$$

Congruence number

$P(X) = \sum_{k=0}^{u} a_k X^{u-k}, \quad Q(X) = \sum_{k=0}^{v} b_k X^{v-k} \in \mathbb{Z}[X].$

$$\begin{pmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{pmatrix}$$

Congruence number

$P(X) = \sum_{k=0}^{u} a_k X^{u-k}, \quad Q(X) = \sum_{k=0}^{v} b_k X^{v-k} \in \mathbb{Z}[X]$.

$$\begin{pmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{pmatrix}$$

Want to know its image for the basis $\{X^{u+v-1}, \ldots, X, 1\}$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$P(X) = \sum_{k=0}^{u} a_k X^{u-k}, \quad Q(X) = \sum_{k=0}^{v} b_k X^{v-k} \in \mathbb{Z}[X]$.

$$\begin{pmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{pmatrix}$$

Want to know its image for the basis $\{X^{u+v-1}, \ldots, X, 1\}$.

May multiply by invertible integer matrices *from the right*.

I.e. may perform integral column operations.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$P(X) = \sum_{k=0}^{u} a_k X^{u-k}, \quad Q(X) = \sum_{k=0}^{v} b_k X^{v-k} \in \mathbb{Z}[X]$.

$$\begin{pmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{pmatrix} \circ \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \end{pmatrix} =$$

Want to know its image for the basis $\{X^{u+v-1}, \ldots, X, 1\}$.

May multiply by invertible integer matrices *from the right*.

I.e. may perform integral column operations.

Congruence number

$P(X) = \sum_{k=0}^{u} a_k X^{u-k}, \quad Q(X) = \sum_{k=0}^{v} b_k X^{v-k} \in \mathbb{Z}[X]$.

$$= \begin{pmatrix} * & 0 & 0 & 0 & 0 \\ * & * & 0 & 0 & 0 \\ * & * & * & 0 & 0 \\ * & * & * & * & 0 \\ * & * & * & * & c \end{pmatrix}$$

Want to know its image for the basis $\{X^{u+v-1}, \ldots, X, 1\}$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$P(X) = \sum_{k=0}^{u} a_k X^{u-k}, \quad Q(X) = \sum_{k=0}^{v} b_k X^{v-k} \in \mathbb{Z}[X]$.

$$= \begin{pmatrix} * & 0 & 0 & 0 & 0 \\ * & * & 0 & 0 & 0 \\ * & * & * & 0 & 0 \\ * & * & * & * & 0 \\ * & * & * & * & c \end{pmatrix}$$

Want to know its image for the basis $\{X^{u+v-1}, \ldots, X, 1\}$.

Congruence number $c(P, Q)$ is the bottom right entry!

It divides the resultant of P, Q (determinant of $S(P, Q)$).

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$$P(X) = X - a, \quad Q(X) = X - b.$$

$$S(P,Q) = \begin{pmatrix} 1 & 1 \\ -a & -b \end{pmatrix}$$

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$P(X) = X - a$, $\quad Q(X) = X - b$.

$$S(P,Q) = \begin{pmatrix} 1 & 1 \\ -a & -b \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -a & -b \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

Congruence number

$P(X) = X - a, \quad Q(X) = X - b.$

$$S(P,Q) = \begin{pmatrix} 1 & 1 \\ -a & -b \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -a & -b \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -a & a-b \end{pmatrix}.$$

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$P(X) = X - a$, $\quad Q(X) = X - b$.

$$S(P,Q) = \begin{pmatrix} 1 & 1 \\ -a & -b \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -a & -b \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -a & a-b \end{pmatrix}.$$

$\Rightarrow$ Congruence number $c(P,Q) = a - b$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$$P(X) = X^2 + X + 1, \quad Q(X) = X - 1.$$

$$S(P,Q) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$$

Congruence number

$$P(X) = X^2 + X + 1, \quad Q(X) = X - 1.$$

$$S(P,Q) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 3 \end{pmatrix}.$$

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$$P(X) = X^2 + X + 1, \quad Q(X) = X - 1.$$

$$S(P,Q) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 3 \end{pmatrix}.$$

$\Rightarrow$ Congruence number $c(P,Q) = 3$.

Congruence number

$$P(X) = X^2 + X + 1, \quad Q(X) = (X-1)(X+2) = X^2 + X - 2.$$

$$S(P,Q) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -2 & 1 \\ 0 & 1 & 0 & -2 \end{pmatrix}$$

Congruence number

$$P(X) = X^2 + X + 1, \quad Q(X) = (X-1)(X+2) = X^2 + X - 2.$$

$$S(P,Q) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -2 & 1 \\ 0 & 1 & 0 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

Congruence number

$P(X) = X^2 + X + 1, \quad Q(X) = (X-1)(X+2) = X^2 + X - 2.$

$$S(P,Q) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -2 & 1 \\ 0 & 1 & 0 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

$\Rightarrow$ Congruence number $c(P,Q) = 3$.

(The resultant is 9.)

Next: Partial solution to our problem.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

Theorem. Let $P, Q \in \mathbb{Z}[X]$.

Congruence number

Theorem. Let $P, Q \in \mathbb{Z}[X]$.

Let $r, s \in \mathbb{Z}[X]$ such that for the congruence number

$$\ell^n \mid\mid c(P,Q) = rP + sQ.$$

Congruence number

Theorem. Let $P, Q \in \mathbb{Z}[X]$.

Let $r, s \in \mathbb{Z}[X]$ such that for the congruence number

$$\ell^n \mid\mid c(P,Q) = rP + sQ.$$

Suppose one of the following holds:

- Neither P nor Q has a multiple factor mod ℓ.
- P has no multiple factor mod ℓ and P and r are coprime mod ℓ.
- Q has no multiple factor mod ℓ and Q and s are coprime mod ℓ.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

Theorem. Let $P, Q \in \mathbb{Z}[X]$.

Let $r, s \in \mathbb{Z}[X]$ such that for the congruence number

$$\ell^n \mid\mid c(P,Q) = rP + sQ.$$

Suppose one of the following holds:

- Neither P nor Q has a multiple factor mod ℓ.
- P has no multiple factor mod ℓ and P and r are coprime mod ℓ.
- Q has no multiple factor mod ℓ and Q and s are coprime mod ℓ.

Then there are $\alpha, \beta \in \overline{\mathbb{Z}}$ such that

(i) $P(\alpha) = Q(\beta) = 0$ and

(ii) $\alpha \equiv \beta \mod \ell^n$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Next: Complete solution to our problem.

Newton polygon method

Consider factorisations (over a big enough extension):

$P(X) = \prod_{i=1}^{u}(X - \alpha_i)$ and $Q(X) = \prod_{j=1}^{v}(X - \beta_j)$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Newton polygon method

Consider factorisations (over a big enough extension): $P(X) = \prod_{i=1}^{u}(X - \alpha_i)$ and $Q(X) = \prod_{j=1}^{v}(X - \beta_j)$.

Now take $Q(X+Y) = \prod_{j=1}^{v}(X - (\beta_j - Y))$, considered as a polynomial in X with coefficients in $\mathbb{Z}[Y]$.

Newton polygon method

Consider factorisations (over a big enough extension):
$P(X) = \prod_{i=1}^{u}(X - \alpha_i)$ and $Q(X) = \prod_{j=1}^{v}(X - \beta_j)$.

Now take $Q(X+Y) = \prod_{j=1}^{v}(X - (\beta_j - Y))$, considered as a polynomial in X with coefficients in $\mathbb{Z}[Y]$.

Let $F(Y)$ be the resultant of $P(X)$ and $Q(X+Y)$ wrt. X.
$\Rightarrow F(Y) = \pm \prod_{i=1}^{u} \prod_{j=1}^{v}(Y - (\beta_j - \alpha_i))$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Newton polygon method

Consider factorisations (over a big enough extension):
$P(X) = \prod_{i=1}^{u}(X - \alpha_i)$ and $Q(X) = \prod_{j=1}^{v}(X - \beta_j)$.

Now take $Q(X+Y) = \prod_{j=1}^{v}(X - (\beta_j - Y))$, considered as a polynomial in X with coefficients in $\mathbb{Z}[Y]$.

Let $F(Y)$ be the resultant of $P(X)$ and $Q(X+Y)$ wrt. X.
$\Rightarrow F(Y) = \pm \prod_{i=1}^{u} \prod_{j=1}^{v}(Y - (\beta_j - \alpha_i))$.

$\Rightarrow$ The roots of $F(Y)$ are the numbers we are looking for.

Newton polygon method

$F(Y) = \pm \prod_{i=1}^{u} \prod_{j=1}^{v} (Y - (\beta_j - \alpha_i))$

$\Rightarrow$ The slopes of the Newton Polygon of $F(Y) \in \mathbb{Z}_\ell[Y]$ are the $v_\ell(\beta_j - \alpha_i)$ (normalisation: $v_\ell(\ell) = 1$).

Newton polygon method

$F(Y) = \pm \prod_{i=1}^{u} \prod_{j=1}^{v} (Y - (\beta_j - \alpha_i))$

$\Rightarrow$ The slopes of the Newton Polygon of $F(Y) \in \mathbb{Z}_\ell[Y]$ are the $v_\ell(\beta_j - \alpha_i)$ (normalisation: $v_\ell(\ell) = 1$).

Lemma. $m := \lceil v_\ell(\beta_j - \alpha_i) \rceil$.

Then $\beta_j \equiv \alpha_i \mod \ell^n$ if and only if $m \geq n$.

Newton polygon method

$F(Y) = \pm \prod_{i=1}^{u} \prod_{j=1}^{v} (Y - (\beta_j - \alpha_i))$

$\Rightarrow$ The slopes of the Newton Polygon of $F(Y) \in \mathbb{Z}_\ell[Y]$ are the $v_\ell(\beta_j - \alpha_i)$ (normalisation: $v_\ell(\ell) = 1$).

Lemma. $m := \lceil v_\ell(\beta_j - \alpha_i) \rceil$.

Then $\beta_j \equiv \alpha_i \mod \ell^n$ if and only if $m \geq n$.

Proof.

$$\begin{aligned} & \beta_j \equiv \alpha_i \mod \ell^n \Leftrightarrow \beta_j - \alpha_i \in (\pi_K)^{\gamma_{K/\mathbb{Q}_\ell}(n)} \\ \Leftrightarrow \quad & ev(\beta_j - \alpha_i) \geq \gamma_{K/\mathbb{Q}_\ell}(n) = e(n-1) + 1 \\ \Leftrightarrow \quad & v(\beta_j - \alpha_i) \geq (n-1) + \frac{1}{e} \Leftrightarrow \lceil v(\beta_j - \alpha_i) \rceil \geq n. \qquad \square \end{aligned}$$

Newton polygon method

$F(Y) = \pm \prod_{i=1}^{u} \prod_{j=1}^{v} (Y - (\beta_j - \alpha_i))$

$\Rightarrow$ The slopes of the Newton Polygon of $F(Y) \in \mathbb{Z}_\ell[Y]$ are the $v_\ell(\beta_j - \alpha_i)$ (normalisation: $v_\ell(\ell) = 1$).

Lemma. $m := \lceil v_\ell(\beta_j - \alpha_i) \rceil$.

Then $\beta_j \equiv \alpha_i \mod \ell^n$ if and only if $m \geq n$.

Proof.

$$\begin{aligned} & \beta_j \equiv \alpha_i \mod \ell^n \Leftrightarrow \beta_j - \alpha_i \in (\pi_K)^{\gamma_{K/\mathbb{Q}_\ell}(n)} \\ \Leftrightarrow \; & e v(\beta_j - \alpha_i) \geq \gamma_{K/\mathbb{Q}_\ell}(n) = e(n-1)+1 \\ \Leftrightarrow \; & v(\beta_j - \alpha_i) \geq (n-1) + \frac{1}{e} \Leftrightarrow \lceil v(\beta_j - \alpha_i) \rceil \geq n. \qquad \square \end{aligned}$$

The biggest slope is the number solving the problem.

Conclusion

Let $P, Q \in \mathbb{Z}[X]$ be monic coprime polynomials.

The maximum n such that there are $\alpha, \beta \in \overline{\mathbb{Z}}$ satisfying

(i) $P(\alpha) = Q(\beta) = 0$ and

(ii) $\alpha \equiv \beta \mod \ell^n$

can be computed

- in most cases by the congruence number
- always with the Newton polygon method.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Next: Modular Forms.

Computing modular forms

Let f be a newform (level N, weight k) with Fourier expansion:

$$f = f(z) = \sum_{m=1}^{\infty} a_m(f) q^m \text{ with } q = q(z) = e^{2\pi i z}.$$

Fact: All the $a_m(f)$ are integers of some number field.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Computing modular forms

Let f be a newform (level N, weight k) with Fourier expansion:

$$f = f(z) = \sum_{m=1}^{\infty} a_m(f) q^m \text{ with } q = q(z) = e^{2\pi i z}.$$

Fact: All the $a_m(f)$ are integers of some number field.

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ naturally acts on the Fourier expansion.

$\rightsquigarrow [f] :=$ $\mathbb{Z}$-span of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).f$.

Computing modular forms

Let f be a newform (level N, weight k) with Fourier expansion:

$$f = f(z) = \sum_{m=1}^{\infty} a_m(f) q^m \text{ with } q = q(z) = e^{2\pi i z}.$$

Fact: All the $a_m(f)$ are integers of some number field.

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ naturally acts on the Fourier expansion.

$\rightsquigarrow [f]$:= $\mathbb{Z}$-span of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).f$.

Fact that makes computations possible:

$a_p(f)$ is a zero of the characteristic polynomial $P_{f,p} \in \mathbb{Z}[X]$ of the Hecke operator T_p acting on $[f]$.

$P_{f,p}$ is easy to compute!

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruences of modular forms mod ℓ^n

$f = \sum_{m=1}^{\infty} a_m(f) q^m$ a newform (level N_f, weight k).

$g = \sum_{m=1}^{\infty} a_m(g) q^m$ a newform (level N_g, weight k).

Definition. f and g are congruent modulo ℓ^n if

$$a_p(f) \equiv a_p(g) \mod \ell^n \quad \text{for (almost) all primes } p.$$

Congruences of modular forms mod ℓ^n

$f = \sum_{m=1}^{\infty} a_m(f) q^m$ a newform (level N_f, weight k).
$g = \sum_{m=1}^{\infty} a_m(g) q^m$ a newform (level N_g, weight k).

Definition. f and g are congruent modulo ℓ^n if

$$a_p(f) \equiv a_p(g) \mod \ell^n \quad \text{for (almost) all primes } p.$$

If f and g are congruent mod ℓ^n, then
$P_{f,p}$ and $P_{g,p}$ have zeros which are congruent mod ℓ^n.

(Recall: $P_{f,p}$, $P_{g,p}$ characteristic polynomials of T_p on $[f]$ and $[g]$.)

Congruences of modular forms mod ℓ^n

$f = \sum_{m=1}^{\infty} a_m(f) q^m$ a newform (level N_f, weight k).

$g = \sum_{m=1}^{\infty} a_m(g) q^m$ a newform (level N_g, weight k).

Definition. f and g are congruent modulo ℓ^n if

$$a_p(f) \equiv a_p(g) \mod \ell^n \quad \text{for (almost) all primes } p.$$

If f and g are congruent mod ℓ^n, then

$P_{f,p}$ and $P_{g,p}$ have zeros which are congruent mod ℓ^n.

(Recall: $P_{f,p}$, $P_{g,p}$ characteristic polynomials of T_p on $[f]$ and $[g]$.)

Some propositions (+ a very believable hypothesis)

$\Rightarrow$ converse is true if compute 'enough' p (Sturm bound).

$\rightsquigarrow$ Use congruence numbers/Newton polygon method!

Congruences of modular forms mod ℓ^n

Algorithm:

Congruences of modular forms mod ℓ^n

Algorithm:

$c_2 := c(P_{f,2}, P_{g,2})$

Congruences of modular forms mod ℓ^n

Algorithm:

$$c_2 := c(P_{f,2}, P_{g,2})$$
$$c_3 := c(P_{f,3}, P_{g,3})$$

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruences of modular forms mod ℓ^n

Algorithm:

$c_2 := c(P_{f,2}, P_{g,2})$

$c_3 := c(P_{f,3}, P_{g,3})$

$c_5 := c(P_{f,5}, P_{g,5})$

$\ldots$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruences of modular forms mod ℓ^n

Algorithm:

$c_2 := c(P_{f,2}, P_{g,2})$

$c_3 := c(P_{f,3}, P_{g,3})$

$c_5 := c(P_{f,5}, P_{g,5})$

$\ldots$.

$\Rightarrow$ Upper bound $u := \gcd(c_2 \cdot 2^\infty, c_3 \cdot 3^\infty, c_5 \cdot 5^\infty, \ldots)$.

Prop. f and g are incongruent mod ℓ^m whenever $\ell^m \nmid u$.

Congruences of modular forms mod ℓ^n

Algorithm:

$c_2 := c(P_{f,2}, P_{g,2})$

$c_3 := c(P_{f,3}, P_{g,3})$

$c_5 := c(P_{f,5}, P_{g,5})$

$\dots$.

$\Rightarrow$ Upper bound $u := \gcd(c_2 \cdot 2^\infty, c_3 \cdot 3^\infty, c_5 \cdot 5^\infty, \dots)$.

Prop. f and g are incongruent mod ℓ^m whenever $\ell^m \nmid u$.

Conversely, from congruence number/Newton method and Sturm bound get like this the maximum m such that (under hypothesis):

$$f \equiv g \mod \ell^n.$$

Special case: Level N and Np

Weight 2, level $\Gamma_0(N)$, prime $p \nmid N$. Degeneracy maps:

$$S_2(N) \quad \overset{f(q)\mapsto f(q)}{\underset{f(q)\mapsto f(q^p)}{\rightrightarrows}} \quad S_2(Np).$$

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Special case: Level N and Np

Weight 2, level $\Gamma_0(N)$, prime $p \nmid N$. Degeneracy maps:

$$S_2(N) \quad \underset{f(q)\mapsto f(q^p)}{\overset{f(q)\mapsto f(q)}{\rightrightarrows}} \quad S_2(Np).$$

Span: p-oldspace. Hecke operator $\tilde{T}_p$ on oldspace

$$\begin{pmatrix} T_p & 1_d \\ -p \cdot 1_d & 0_d \end{pmatrix}$$ with T_p Hecke operator on $[f]$.

Let $\tilde{P}_{f,p}$ be the charpoly of $\tilde{T}_p$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Special case: Level N and Np

Weight 2, level $\Gamma_0(N)$, prime $p \nmid N$. Degeneracy maps:

$$S_2(N) \underset{f(q)\mapsto f(q^p)}{\overset{f(q)\mapsto f(q)}{\rightrightarrows}} S_2(Np).$$

Span: p-oldspace. Hecke operator $\tilde{T}_p$ on oldspace

$$\begin{pmatrix} T_p & 1_d \\ -p \cdot 1_d & 0_d \end{pmatrix}$$ with T_p Hecke operator on $[f]$.

Let $\tilde{P}_{f,p}$ be the charpoly of $\tilde{T}_p$.

Modify the algorithm at p:

Compute $c(\tilde{P}_{f,p}, P_{g,p})$ (instead of $c(P_{f,p}, P_{g,p})$).

Examples

Extract from Xavier's table:

N_1	i_1	N_2	i_2	lower bound	upper bound
71	2	71	1	$2 \cdot 3^2$	$2 \cdot 3^2$
109	3	109	1	2^2	2^2
155	4	155	2	2^4	2^4
233	3	233	1	3^3	3^3
613	2	613	1	$7 \cdot 47^2$	$7 \cdot 47^2$
785	2	785	1	7^3	7^3
1073	6	1073	3	$2 \cdot 17^2$	$2 \cdot 17^2$
1481	3	1481	1	$5^2 \cdot 2833$	$5^2 \cdot 2833$
1939	4	1939	3	$37^2 \cdot 4423$	$37^2 \cdot 4423$

Weak $\neq$ Strong

Weight 2, level $\Gamma_0(71)$. Two classes of newforms both with coefficient field K: $[K:\mathbb{Q}] = 3$ and discriminant $d_K = 257$:

$$[f] : K \overset{\longrightarrow}{\underset{\longrightarrow}{\longrightarrow}} \overline{\mathbb{Q}} \overset{\text{fixed}}{\hookrightarrow} \overline{\mathbb{Q}}_3 \quad \text{and} \quad [g] : K \overset{\longrightarrow}{\underset{\longrightarrow}{\longrightarrow}} \overline{\mathbb{Q}} \overset{\text{fixed}}{\hookrightarrow} \overline{\mathbb{Q}}_3.$$

Weak $\neq$ Strong

Weight 2, level $\Gamma_0(71)$. Two classes of newforms both with coefficient field K: $[K:\mathbb{Q}] = 3$ and discriminant $d_K = 257$:

$$[f] : K \begin{array}{c}\longrightarrow\\\longrightarrow\\\longrightarrow\end{array} \overline{\mathbb{Q}} \overset{\text{fixed}}{\hookrightarrow} \overline{\mathbb{Q}}_3 \quad \text{and} \quad [g] : K \begin{array}{c}\longrightarrow\\\longrightarrow\\\longrightarrow\end{array} \overline{\mathbb{Q}} \overset{\text{fixed}}{\hookrightarrow} \overline{\mathbb{Q}}_3.$$

Modulo 3, both f_1 and g_1 land in $\mathbb{F}_3$, others in $\mathbb{F}_9$.

$f_1 \equiv g_1 \mod 9$ and $f_1 \not\equiv g_1 \mod 27$

$\Rightarrow$ Only one strong Hecke eigenform modulo 9.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Weak $\neq$ Strong

Weight 2, level $\Gamma_0(71)$. Two classes of newforms both with coefficient field K: $[K:\mathbb{Q}] = 3$ and discriminant $d_K = 257$:

$$[f] : K \rightrightarrows \overline{\mathbb{Q}} \overset{\text{fixed}}{\hookrightarrow} \overline{\mathbb{Q}}_3 \quad \text{and} \quad [g] : K \rightrightarrows \overline{\mathbb{Q}} \overset{\text{fixed}}{\hookrightarrow} \overline{\mathbb{Q}}_3.$$

Modulo 3, both f_1 and g_1 land in $\mathbb{F}_3$, others in $\mathbb{F}_9$.

$f_1 \equiv g_1 \mod 9$ and $f_1 \not\equiv g_1 \mod 27$

$\Rightarrow$ Only one strong Hecke eigenform modulo 9.

$\hat{\mathbb{T}} :=$ Hecke algebra completed at 3.

The local factor $\hat{\mathbb{T}}_{\mathfrak{m}}$ belonging to f_1 and g_1 satisfies:

$$\hat{\mathbb{T}}_{\mathfrak{m}} \twoheadrightarrow \hat{\mathbb{T}}_{\mathfrak{m}} \otimes_{\mathbb{Z}_3} \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/9\mathbb{Z}[X]/(X^2) \xrightarrow{X \mapsto 0 \text{ or } X \mapsto 3} \mathbb{Z}/9\mathbb{Z}.$$

Hence: two weak Hecke eigenforms!

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Level raising mod ℓ^n

Question. Given: f in level N, weight k, a prime $p \nmid N$ s.t.

$$\ell^n \mid c(P_{f,p}, X - (p+1)) \text{ or } \ell^n \mid c(P_{f,p}, X + (p+1)).$$

Is there g in level Np, weight k such that $f \equiv g \mod \ell^n$?

Level raising mod ℓ^n

Question. Given: f in level N, weight k, a prime $p \nmid N$ s.t.

$$\ell^n \mid c(P_{f,p}, X - (p+1)) \text{ or } \ell^n \mid c(P_{f,p}, X + (p+1)).$$

Is there g in level Np, weight k such that $f \equiv g \mod \ell^n$?

(Famous theorem by Ribet (Diamond, Taylor) for $n = 1$.)

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Level raising mod ℓ^n

Question. Given: f in level N, weight k, a prime $p \nmid N$ s.t.

$$\ell^n \mid c(P_{f,p}, X - (p+1)) \text{ or } \ell^n \mid c(P_{f,p}, X + (p+1)).$$

Is there g in level Np, weight k such that $f \equiv g \mod \ell^n$?

(Famous theorem by Ribet (Diamond, Taylor) for $n = 1$.)

Example. f in level 17, weight 2. Coefficients in $\mathbb{Z}$.

Level raising mod ℓ^n

Question. Given: f in level N, weight k, a prime $p \nmid N$ s.t.

$$\ell^n \mid c(P_{f,p}, X - (p+1)) \text{ or } \ell^n \mid c(P_{f,p}, X + (p+1)).$$

Is there g in level Np, weight k such that $f \equiv g \mod \ell^n$?

(Famous theorem by Ribet (Diamond, Taylor) for $n = 1$.)

Example. f in level 17, weight 2. Coefficients in $\mathbb{Z}$.

$a_{59}(f) = 12$: congruence numbers

$$9 \mid\mid c(X - 12, X + (59 + 1)) = -72,$$

$$3 \mid\mid c(X - 12, X - (59 + 1)) = 48.$$

Level raising mod ℓ^n

Question. Given: f in level N, weight k, a prime $p \nmid N$ s.t.

$$\ell^n \mid c(P_{f,p}, X-(p+1)) \text{ or } \ell^n \mid c(P_{f,p}, X+(p+1)).$$

Is there g in level Np, weight k such that $f \equiv g \mod \ell^n$?

(Famous theorem by Ribet (Diamond, Taylor) for $n = 1$.)

Example. f in level 17, weight 2. Coefficients in $\mathbb{Z}$.

$a_{59}(f) = 12$: congruence numbers

$$9 \,||\, c(X-12, X+(59+1)) = -72,$$

$$3 \,||\, c(X-12, X-(59+1)) = 48.$$

In level $17 \cdot 59$, weight 2, $\exists$ 3 newforms g_1, g_2, g_3 s.t.

$$g_i \equiv f \mod 3 \text{ for all } i = 1, 2, 3,$$

Level raising mod ℓ^n

Question. Given: f in level N, weight k, a prime $p \nmid N$ s.t.

$$\ell^n \mid c(P_{f,p}, X-(p+1)) \text{ or } \ell^n \mid c(P_{f,p}, X+(p+1)).$$

Is there g in level Np, weight k such that $f \equiv g \mod \ell^n$?

(Famous theorem by Ribet (Diamond, Taylor) for $n = 1$.)

Example. f in level 17, weight 2. Coefficients in $\mathbb{Z}$.

$a_{59}(f) = 12$: congruence numbers

$$9 \,||\, c(X-12, X+(59+1)) = -72,$$

$$3 \,||\, c(X-12, X-(59+1)) = 48.$$

In level $17 \cdot 59$, weight 2, $\exists\, 3$ newforms g_1, g_2, g_3 s.t.

$$g_i \equiv f \mod 3 \text{ for all } i = 1, 2, 3,$$

but there is no i s.t. $g_i \equiv f \mod 9$!

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Level raising mod ℓ^n

Does a weaker statement hold?

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Level raising mod ℓ^n

Does a weaker statement hold?

Let $g_1, \ldots, g_r$ be all newforms in $S_2(\Gamma_0(Np))$.

Let ℓ^{n_i} be the highest power of ℓ such that

$$g_i \equiv f \bmod \ell^{n_i} \text{ for } i = 1, \ldots r.$$

Put $n := n_1 + \ldots + n_r$.

Put $c := c(P_{f,p}, X^2 - (p+1)^2)$.

Level raising mod ℓ^n

Does a weaker statement hold?

Let $g_1, \dots, g_r$ be all newforms in $S_2(\Gamma_0(Np))$.

Let ℓ^{n_i} be the highest power of ℓ such that

$$g_i \equiv f \bmod \ell^{n_i} \text{ for } i = 1, \dots r.$$

Put $n := n_1 + \ldots + n_r$.
Put $c := c(P_{f,p}, X^2 - (p+1)^2)$.

Question. Is n at least as big as (or even equal to) the ℓ-valuation of c?

THE END

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK