Computing congruences of modular forms modulo prime powers (extended version)

Gabor Wiese

(joint work with Xavier Taixés i Ventosa)

Institut für Experimentelle Mathematik

Universität Duisburg-Essen

3 April 2009

Plan

(I) Congruences mod ℓ^n.

(II) Computing them.

(III) Applications to modular forms,
Galois representations
and abelian varieties.

Congruences mod ℓ^n

Fix $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Consider $K/\mathbb{Q}_\ell$ with π_K uniformizer.

We want:

- Congruence mod ℓ

  should be

  congruence mod π_K.
- If $K/\mathbb{Q}_\ell$ is unramified, then

  congruence mod ℓ^n

  should be

  congruence mod $(\pi^n) = (\ell^n)$.

Congruences mod ℓ^n

Define congruences mod ℓ^n for $a, b \in \overline{\mathbb{Z}}_\ell$.

For $L/K/\mathbb{Q}_\ell$ finite extensions (inside $\overline{\mathbb{Q}}_\ell$) define

$$\gamma_{L/K}(n) := (n-1)e_{L/K} + 1$$

with $e_{L/K}$ the ramification index.

Properties:

- $\gamma_{L/K}(1) = 1$,
- $\gamma_{M/K}(n) = \gamma_{M/L}(\gamma_{L/K}(n))$ for $M/L/K$,
- $\lceil \frac{\gamma_{L/K}(n)}{e_{L/K}} \rceil = n$.

Congruences mod ℓ^n

Define congruences mod ℓ^n for $a, b \in \overline{\mathbb{Z}}_\ell$.

The definition $\gamma_{L/K}(n) := (n-1)e_{L/K} + 1$ ensures:

$$\mathbb{Z}/\ell^n\mathbb{Z} \hookrightarrow \mathcal{O}_K/(\pi_K^{\gamma_{K/\mathbb{Q}_\ell}(n)}) \hookrightarrow \mathcal{O}_L/(\pi_L^{\gamma_{L/\mathbb{Q}_\ell}(n)}).$$

Define

$$a \equiv b \mod \ell^n \Leftrightarrow a - b \in (\pi_K^{\gamma_{K/\mathbb{Q}_\ell}(n)})$$

for any $K/\mathbb{Q}_\ell$ containing a, b.

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:

Reduced resultant (Kristin Lauter's talk)

= Congruence ideal/number (our name for it).

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:

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

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

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

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

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.

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 $S(P, Q)$).

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 $c(P,Q) = a - b$.

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

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

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

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

(The resultant is 9.)

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Congruence number

$P(X) = X^2 + 5X + 3$, $\quad Q(X) = X^2 + 2X + 3$.

$$S(P,Q) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 5 & 1 & 2 & 1 \\ 3 & 5 & 3 & 2 \\ 0 & 3 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & 3 & 0 \\ 3 & 3 & 0 & 9 \end{pmatrix}$$

$\Rightarrow$ Congruence number $c(P,Q) = 9$.

(The resultant is 27.)

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

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 minimal polynomial $P_{f,p} \in \mathbb{Z}[X]$ of the Hecke operator T_p acting on $[f]$.

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

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

Some propositions (+ a very believable hypothesis)
$\Rightarrow$ converse is true if compute 'enough' p.

$\rightsquigarrow$ Perfect for use of congruence numbers!

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 $\ell^m \nmid u$.

From Theorem (before) often get (under hypothesis):

$$f \equiv g \mod \ell^n \text{ with } \ell^n \mid\mid u.$$

A question of Frey

Let f, g two newforms of weight 2.

$\rightsquigarrow$ Shimura's construction: A_f, A_g abelian varieties over $\mathbb{Q}$.

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

$$A_f[\ell^n] \cong A_g[\ell^n] \quad \text{as } \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\text{-modules.}$$

How big can M with

$$A_f[M] \cong A_g[M]$$

be without $A_f \sim A_g$ (i.e. f Galois conjugate to g)?

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Level raising mod ℓ^n

Question. Given: f in level N, weight k, a prime p such that

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

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

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

Level raising mod ℓ^n

Level raising does not generalise so easily!

Does a weaker statement hold?

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK