Counting points over finite fields

Adriana Salerno

Bates College

July 10, 2013

The congruent Zeta function

- $X/\mathbb{F}_q$ - algebraic variety over finite field of $q = p^f$ elements.

The congruent Zeta function

- $X/\mathbb{F}_q$ - algebraic variety over finite field of $q = p^f$ elements.
- $N_s(X) = \#X(\mathbb{F}_{q^s})$ - number of $\mathbb{F}_{q^s}$-rational points on X.

The congruent Zeta function

- $X/\mathbb{F}_q$ - algebraic variety over finite field of $q = p^f$ elements.
- $N_s(X) = \#X(\mathbb{F}_{q^s})$ - number of $\mathbb{F}_{q^s}$-rational points on X.
- The *Zeta function* of X is

$$\text{Zeta}(X/\mathbb{F}_q, T) := \exp\left(\sum_{s=1}^{\infty} N_s(X)\frac{T^s}{s}\right) \in \mathbb{Q}[[t]]$$

The congruent Zeta function

- $X/\mathbb{F}_q$ - algebraic variety over finite field of $q = p^f$ elements.
- $N_s(X) = \#X(\mathbb{F}_{q^s})$ - number of $\mathbb{F}_{q^s}$-rational points on X.
- The *Zeta function* of X is

$$\mathrm{Zeta}(X/\mathbb{F}_q, T) := \exp\left(\sum_{s=1}^{\infty} N_s(X)\frac{T^s}{s}\right) \in \mathbb{Q}[[t]]$$

Theorem (Dwork '60)

$\mathrm{Zeta}(X/\mathbb{F}_q, T)$ *is a rational function of* T.

Weil conjectures (for hypersurfaces)

X smooth, projective hypersurface in $\mathbb{P}^n$, we have:

Weil conjectures (for hypersurfaces)

X smooth, projective hypersurface in $\mathbb{P}^n$, we have:

Theorem (Deligne '73)

Weil conjectures (for hypersurfaces)

X smooth, projective hypersurface in $\mathbb{P}^n$, we have:

Theorem (Deligne '73)

- $\mathrm{Zeta}(X/\mathbb{F}_q, T) = \dfrac{P(T)^{\pm 1}}{(1-T)(1-qT)(1-q^2T)\cdots(1-q^{n-1}T)}$
  where $\deg P(T) = b_{n-1} = \dim H^{n-1}_{dR}(X) =$ *Betti number.*

Weil conjectures (for hypersurfaces)

X smooth, projective hypersurface in $\mathbb{P}^n$, we have:

Theorem (Deligne '73)

- $\text{Zeta}(X/\mathbb{F}_q, T) = \dfrac{P(T)^{\pm 1}}{(1-T)(1-qT)(1-q^2T)\cdots(1-q^{n-1}T)}$ *where* $\deg P(T) = b_{n-1} = \dim H^{n-1}_{dR}(X) =$ *Betti number.*
- *If* α *reciprocal root of* $P(T)$*, then so is* q^{n-1}/α*.*

Weil conjectures (for hypersurfaces)

X smooth, projective hypersurface in $\mathbb{P}^n$, we have:

Theorem (Deligne '73)

- $\mathrm{Zeta}(X/\mathbb{F}_q, T) = \dfrac{P(T)^{\pm 1}}{(1-T)(1-qT)(1-q^2T)\cdots(1-q^{n-1}T)}$ *where* $\deg P(T) = b_{n-1} = \dim H^{n-1}_{dR}(X) =$ *Betti number.*
- *If* α *reciprocal root of* $P(T)$*, then so is* q^{n-1}/α*.*
- *If* α *reciprocal root then* $|\alpha| = q^{(n-1)/2}$*. (Riemann hypothesis).*

The Legendre family

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

The Legendre family

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

- $\mathrm{Zeta}(E_\lambda/\mathbb{F}_p, T) = \dfrac{1 - a_{\lambda,p}T + pT^2}{(1-T)(1-pT)}$

The Legendre family

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

- $\mathrm{Zeta}(E_\lambda/\mathbb{F}_p, T) = \dfrac{1 - a_{\lambda,p}T + pT^2}{(1-T)(1-pT)}$
- $N_{\mathbb{F}_p}(\lambda) = 1 - a_{\lambda,p} + p$

The Legendre family

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

- $\mathrm{Zeta}(E_\lambda/\mathbb{F}_p, T) = \dfrac{1 - a_{\lambda,p}T + pT^2}{(1-T)(1-pT)}$
- $N_{\mathbb{F}_p}(\lambda) = 1 - a_{\lambda,p} + p$
- So $a_{\lambda,p} \equiv 1 - N_{\mathbb{F}_p}(\lambda) \bmod p$

The Legendre family

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

- $\mathrm{Zeta}(E_\lambda/\mathbb{F}_p, T) = \dfrac{1 - a_{\lambda,p}T + pT^2}{(1-T)(1-pT)}$
- $N_{\mathbb{F}_p}(\lambda) = 1 - a_{\lambda,p} + p$
- So $a_{\lambda,p} \equiv 1 - N_{\mathbb{F}_p}(\lambda) \mod p$
- If p large enough (not 2 or 3) $N_{\mathbb{F}_p}(\lambda) \mod p$ is all we need to know $a_{\lambda,p}$.

The Legendre family

Theorem (Igusa '58)

$$N_{\mathbb{F}_p}(\lambda) \equiv (-1)^{\frac{p-1}{2}} \left[{}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1 \middle| \lambda \right) \right]_0^{\frac{p-1}{2}} \bmod p.$$

NOTE: We also know that ${}_2F_1(\frac{1}{2}, \frac{1}{2}; 1|\lambda)$ is the only holomorphic solution around 0 of the Picard-Fuchs differential equation satisfied by the periods of E_λ.

Gauss sums

- Let $\chi_{1/(q-1)} : \mathbb{F}_q^* \to K^*$ be a fixed generator of the character group of $\mathbb{F}_q^*$ where K is $\mathbb{C}$ or $\mathbb{C}_p$.

Gauss sums

- Let $\chi_{1/(q-1)} : \mathbb{F}_q^* \to K^*$ be a fixed generator of the character group of $\mathbb{F}_q^*$ where K is $\mathbb{C}$ or $\mathbb{C}_p$.
- For $s \in \frac{1}{q-1}\mathbb{Z}/\mathbb{Z}$ we let $\chi_s = \left(\chi_{1/(q-1)}\right)^{s(q-1)}$, and for any s set $\chi_s(0) = 0$.

Gauss sums

- Let $\chi_{1/(q-1)} : \mathbb{F}_q^* \to K^*$ be a fixed generator of the character group of $\mathbb{F}_q^*$ where K is $\mathbb{C}$ or $\mathbb{C}_p$.
- For $s \in \frac{1}{q-1}\mathbb{Z}/\mathbb{Z}$ we let $\chi_s = \left(\chi_{1/(q-1)}\right)^{s(q-1)}$, and for any s set $\chi_s(0) = 0$.
- Let $\psi : \mathbb{F}_q \to K^*$ be a (fixed) additive character.

Gauss sums

- Let $\chi_{1/(q-1)} : \mathbb{F}_q^* \to K^*$ be a fixed generator of the character group of $\mathbb{F}_q^*$ where K is $\mathbb{C}$ or $\mathbb{C}_p$.
- For $s \in \frac{1}{q-1}\mathbb{Z}/\mathbb{Z}$ we let $\chi_s = \left(\chi_{1/(q-1)}\right)^{s(q-1)}$, and for any s set $\chi_s(0) = 0$.
- Let $\psi : \mathbb{F}_q \to K^*$ be a (fixed) additive character.
- For $s \in \frac{1}{(q-1)}\mathbb{Z}/\mathbb{Z}$ we let $g(s)$ denote the Gauss sum

$$g(s) = \sum_{x \in \mathbb{F}_q} \chi_s(x)\psi(x)$$

A family with a large group action

Let

$$X_\lambda : x_1^d + \cdots + x_n^d - d\lambda x_1^{h_1} \cdots x_n^{h_n} = 0$$

where each h_i is a positive integer, $\sum h_i = d$ and $\gcd(d, h_1, \ldots, h_n) = 1$.

A family with a large group action

Let

$$X_\lambda : x_1^d + \cdots + x_n^d - d\lambda x_1^{h_1} \cdots x_n^{h_n} = 0$$

where each h_i is a positive integer, $\sum h_i = d$ and $\gcd(d, h_1, \ldots, h_n) = 1$.

- Let μ_d^n be the group of n-tuples of d-th roots of unity in $\mathbb{F}_q^*$.

A family with a large group action

Let

$$X_\lambda : x_1^d + \cdots + x_n^d - d\lambda x_1^{h_1} \cdots x_n^{h_n} = 0$$

where each h_i is a positive integer, $\sum h_i = d$ and $\gcd(d, h_1, \ldots, h_n) = 1$.

- Let μ_d^n be the group of n-tuples of d-th roots of unity in $\mathbb{F}_q^*$.
- Let Δ be the diagonal elements of μ_d^n, i.e. elements of the form $(\xi, \cdots, \xi)$.

A family with a large group action

Let

$$X_\lambda : x_1^d + \cdots + x_n^d - d\lambda x_1^{h_1} \cdots x_n^{h_n} = 0$$

where each h_i is a positive integer, $\sum h_i = d$ and $\gcd(d, h_1, \ldots, h_n) = 1$.

- Let μ_d^n be the group of n-tuples of d-th roots of unity in $\mathbb{F}_q^*$.
- Let Δ be the diagonal elements of μ_d^n, i.e. elements of the form $(\xi, \cdots, \xi)$.

The varieties X_λ allow a faithful action of the group

$$G = \{\xi \in \mu_d^n | \xi^h = 1\}/\Delta,$$

by $\xi = (\xi_1, \ldots, \xi_n)$ taking the point $(x_1, \ldots, x_n)$ to $(\xi_1 x_1, \ldots, \xi_n x_n)$.

A large group action

$$char(G) \leftrightarrow W,$$

where

$$W = \{(w_1, \dots, w_n) | 0 \leq w_i < d, \sum w_i \equiv 0 \mod d\},$$

and $w' \sim w$ if $w - w'$ is a multiple (mod d) of h.
Here

$$\chi_w(\xi) := \chi(\xi^w), \qquad \xi^w = \xi_1^{w_1} \cdots \xi_n^{w_n}$$

and χ is a fixed primitive character of μ_d, which we can get for example by restricting $\chi_{1/(q-1)}$ to μ_d.

Koblitz's result

Assume $d|q-1$.

Theorem (Koblitz)

$$N_{\mathbb{F}_q}(\lambda) = N_{\mathbb{F}_q}(0) + \frac{1}{q-1} \sum_{\substack{s \in \frac{d}{q-1}\mathbb{Z}/\mathbb{Z} \\ w \in W}} \frac{g\left(\frac{w+sh}{d}\right)}{g(s)} \chi_s(d\lambda),$$

where we denote $g\left(\frac{w+sh}{d}\right) = \prod_i g\left(\frac{w_i+sh_i}{d}\right)$.

The Gross-Koblitz formula

Fix our attention on $\mathbb{F}_p$-points on our varieties.

The Gross-Koblitz formula

Fix our attention on $\mathbb{F}_p$-points on our varieties.
Suppose we want to find a way to compute $N_{\mathbb{F}_p}(\lambda)$ mod p. We use

The Gross-Koblitz formula

Fix our attention on $\mathbb{F}_p$-points on our varieties.
Suppose we want to find a way to compute $N_{\mathbb{F}_p}(\lambda)$ mod p. We use

Theorem (Gross-Koblitz)

For $s \in \frac{1}{p-1}\mathbb{Z}/\mathbb{Z}$, we have

$$g(s) = -(-p)^s \Gamma_p(s).$$

Here, Γ_p is the p-adic analog of the Gamma function.

The 0-dimensional family

Study $N_{\mathbb{F}_p}(\lambda)$ mod p for the family

$$Z_\lambda : x_1^d + x_2^d - d\lambda x_1 x_2^{d-1} = 0.$$

Assume p is a prime such that $d|p-1$. We use the following:

Formula (S)

$$N_{\mathbb{F}_p}(\lambda) = N_{\mathbb{F}_p}(0) + \frac{-1}{p-1}\sum_{a=0}^{p-2} \frac{(-p)^{\eta(a)}\Gamma_p\left(\frac{a}{p-1}\right)\Gamma_p\left(\left\{\frac{(d-1)a}{p-1}\right\}\right)}{\Gamma_p\left(\left\{\frac{da}{p-1}\right\}\right)}\omega(d\lambda)^{-da}$$

where $\eta(a) = \left(\frac{a}{p-1} + \{\frac{(d-1)a}{p-1}\} - \{\frac{da}{p-1}\}\right)$.

Notation

- $\omega : \mathbb{F}_p^* \to \mathbb{C}_p^*$ - Teichmüller character. ($\omega(x) \equiv x \bmod p$)
- $\{x\} = x - [x]$, fractional part of x.

The 0-dimensional family

Theorem (S)

Let $\alpha^{(0)} = (\frac{1}{d}, \ldots, \frac{d-1}{d}), \beta^{(0)} = (\frac{1}{d-1}, \ldots, \frac{d-2}{d-1})$.

$$N_{\mathbb{F}_p}(\lambda) - N_{\mathbb{F}_p}(0)$$
$$\equiv \sum_{i=0}^{d-2} \left[{}_dF_{d-1}(\alpha^{(i)}; \beta^{(i)} | (d-1)^{-(d-1)}\lambda^{-d}) \right]_{\frac{i(p-1)}{d-1}}^{\frac{(i+1)(p-1)}{d}-1} \bmod p,$$

where $\alpha^{(i)} = (\frac{1}{d}+1, \ldots, \frac{i}{d}+1, \frac{i+1}{d}, \ldots, \frac{d-1}{d})$, *and* $\beta^{(i)} = \left(\frac{1}{d-1}+1, \ldots, \frac{i}{d-1}+1, \frac{i+1}{d-1}, \ldots, \frac{d-2}{d-1}\right)$.

$[u(z)]_i^j$ denotes the polynomial which is the truncation of a series $u(z)$ from $n = i$ to j.

The 0-dimensional family

So for example in the case $d = 3$ we get that

$$\begin{aligned} N_{\mathbb{F}_p}(\lambda) - N_{\mathbb{F}_p}(0) \equiv & \left[{}_2F_1\left(\frac{1}{3}, \frac{2}{3}; \frac{1}{2} \middle| \frac{1}{2^2\lambda^3}\right)\right]_0^{\frac{p-1}{3}-1} \\ & + \left[{}_2F_1\left(\frac{4}{3}, \frac{2}{3}; \frac{3}{2} \middle| \frac{1}{2^2\lambda^3}\right)\right]_{\frac{p-1}{2}}^{\frac{2(p-1)}{3}-1} \mod p. \end{aligned}$$

The Dwork family of K3's

$$X_\lambda : x_1^4 + x_2^4 + x_3^4 + x_4^4 - 4\lambda x_1 x_2 x_3 x_4 = 0.$$

The set W is made up of 64 vectors, but we can split them up into 16 equivalence classes, and of those there are only three "types". These are

$$(0,0,0,0),(1,1,1,1),(2,2,2,2),(3,3,3,3)$$

$$(0,1,1,2),(1,2,2,3),(2,3,3,0),(3,0,0,1)$$

$$(0,0,2,2),(1,1,3,3),(2,2,0,0),(3,3,1,1)$$

The rest are permutations of these. So there is one class of the first type, 12 classes of the second type, and 3 classes of the third type.

The Dwork family of K3's

$$N_{\mathbb{F}_p}(\lambda) - N_{\mathbb{F}_p}(0) = \frac{1}{p-1} \sum_{s \in \frac{1}{p-1}\mathbb{Z}/\mathbb{Z}} \frac{g(s)^4}{g(4s)} \chi_{4s}(4\lambda) \qquad (S_1)$$

$$+\frac{12}{p-1} \sum_{s \in \frac{1}{p-1}\mathbb{Z}/\mathbb{Z}} \frac{g(s)g(s+\frac{1}{4})^2 g(s+\frac{1}{2})}{g(4s)} \chi_{4s}(4\lambda) \qquad (S_2)$$

$$+\frac{3}{p-1} \sum_{s \in \frac{1}{p-1}\mathbb{Z}/\mathbb{Z}} \frac{g(s)^2 g(s+\frac{1}{2})^2}{g(4s)} \chi_{4s}(4\lambda). \qquad (S_3)$$

The Dwork family of K3's

Using Gross-Koblitz and taking mod p leaves only (S_1), so

$$N_{\mathbb{F}_p}(\lambda) - N_{\mathbb{F}_p}(0) \equiv \left[{}_3F_2\left(\frac{1}{4}, \frac{1}{2}, \frac{3}{4}; 1, 1 \,\middle|\, \lambda^{-4} \right) \right]_0^{\frac{p-1}{4}-1} \bmod p$$

The Dwork family of K3's

Xenia de la Ossa and Shabnam Kadir:

The Dwork family of K3's

Xenia de la Ossa and Shabnam Kadir:

$$\mathrm{Zeta}(X/\mathbb{F}_p, T) = \frac{1}{(1-T)(1-pT)(1-p^2T)P(T)}$$

The Dwork family of K3's

Xenia de la Ossa and Shabnam Kadir:

$$\mathrm{Zeta}(X/\mathbb{F}_p, T) = \frac{1}{(1-T)(1-pT)(1-p^2T)P(T)}$$

$$P(T) = R_{(0,0,0,0)}(T) R^3_{(0,0,2,2)}(T) R^{12}_{(0,1,1,2)}(T)$$

The Dwork family of K3's

Xenia de la Ossa and Shabnam Kadir:

$$\mathrm{Zeta}(X/\mathbb{F}_p, T) = \frac{1}{(1-T)(1-pT)(1-p^2T)P(T)}$$

$$P(T) = R_{(0,0,0,0)}(T)R^3_{(0,0,2,2)}(T)R^{12}_{(0,1,1,2)}(T)$$

where

- $R_{(0,0,0,0)}(T) = (1 \pm pT)(1 - aT + p^2T)$
- $R_{(0,0,2,2)}(T) = (1 \pm pT)(1 \pm pT)$
- $R_{(0,1,1,2)}(T) =$
$$\begin{cases} [(1-pT)(1+pT)]^{1/2} & \text{when } p \equiv 3 \bmod 4 \\ (1 \pm pT) & \text{otherwise} \end{cases}$$

Let $N(\alpha)$ be the number of $\mathbb{F}_q$-points on the projective hypersurface defined by

$$\alpha_1 x_1^{h_1^{(1)}} \cdots x_n^{h_n^{(1)}} + \cdots + \alpha_r x_1^{h_1^{(r)}} \cdots x_n^{h_n^{(r)}} = 0,$$

where α is an r- tuple of nonzero elements of $\mathbb{F}_q$, and $q \not| h_i^{(j)}$.

Let $N(\alpha)$ be the number of $\mathbb{F}_q$-points on the projective hypersurface defined by

$$\alpha_1 x_1^{h_1^{(1)}} \cdots x_n^{h_n^{(1)}} + \cdots + \alpha_r x_1^{h_1^{(r)}} \cdots x_n^{h_n^{(r)}} = 0,$$

where α is an r- tuple of nonzero elements of $\mathbb{F}_q$, and $q \not| h_i^{(j)}$.
We abbreviate this as $\sum_{i=1}^r \alpha_i x^{h^{(i)}}$.

Let $N(\alpha)$ be the number of $\mathbb{F}_q$-points on the projective hypersurface defined by

$$\alpha_1 x_1^{h_1^{(1)}} \cdots x_n^{h_n^{(1)}} + \cdots + \alpha_r x_1^{h_1^{(r)}} \cdots x_n^{h_n^{(r)}} = 0,$$

where α is an r- tuple of nonzero elements of $\mathbb{F}_q$, and $q \not| h_i^{(j)}$.
We abbreviate this as $\sum_{i=1}^r \alpha_i x^{h^{(i)}}$.
Let $N^*(\alpha)$ denote the number of points with all coordinates nonzero on the hypersurface.

Theorem (Delsarte '51, Furtado Gomida '51)

$$N^*(\alpha) = \sum_w \chi_w^{-1}(\alpha) c_{\chi_w},$$

where the summation is over all $w \in (\mathbb{Z}/(q-1)\mathbb{Z})^r$, $\sum w_i \equiv 0 \bmod q$, *which index the characters of* μ_{q-1}^r/Δ, *for which*

$$\sum_i h_j^{(i)} w_i \equiv 0 \bmod q \qquad \textit{for all} \qquad j = 1, \ldots, n;$$

and for such w, $c_{\chi_w} = -\frac{1}{q}(q-1)^{n-r} J\left(\frac{w_1}{q-1}, \ldots, \frac{w_r}{q-1}\right)$, *unless* $w = (0, \ldots, 0)$, *in which case* $c_{\chi_0} = (q-1)^{n-r} \frac{(q-1)^{r-1} - (-1)^{r-1}}{q}$.

In terms of Gauss sums the expression for the coefficients becomes

$$c_{\chi_w} = (q-1)^{n-r}\chi_{w_r}(-1)\frac{g\left(\frac{w_1}{q-1}\right)\cdots g\left(\frac{w_{r-1}}{q-1}\right)}{g\left(\frac{w_1}{q-1}+\cdots+\frac{w_{r-1}}{q-1}\right)}.$$

The Klein-Mukai pencil

Let

$$X_\psi : x_1^3 x_2 + x_2^3 x_3 + x_3^3 x_1 + x_4^4 - 4\psi x_1 x_2 x_3 x_4 = 0.$$

Delsarte gives us a way to compute $N^*(1,1,1,1,-4\psi)$ in terms of Gauss sums. In fact, same formula works to find the number of points with some zero coordinates (just count points on a different variety!).

The Klein-Mukai pencil

If $7 \nmid q-1$:

$$N^*(\psi) = \frac{1}{q-1}\left[q^3 - 4q^3 + 6q - 4 - \sum_{k=1}^{q-2} \frac{g\left(\frac{k}{q-1}\right)^4}{g\left(\frac{4k}{q-1}\right)} \chi_{4k}(4\psi)\right].$$

The Klein-Mukai pencil

Considering only over $\mathbb{F}_p$ and using the Gross-Koblitz formula we get:

$$N(\psi) = 4p - 2 + \frac{1}{p-1}\left(p^3 - 4p^2 + 6p - 4 - \sum_{r=1}^{p-2} \frac{\Gamma_p(r/(p-1))^4}{\Gamma_p(\{4r/(p-1)\})}(-p)^{(4r/(p-1)-\{4r/(p-1)\})}\omega(4l)^r\right)$$

Which modulo p is exactly the same hypergeometric function we obtained for the Dwork family K3. That is

$$N(\psi) - 2 \equiv \left[{}_3F_2\left(\frac{1}{4}, \frac{1}{2}, \frac{3}{4}; 1, 1 \middle| \lambda^{-4}\right)\right]_0^{\frac{p-1}{4}-1} \mod p$$

The Klein-Mukai quartic

If $7|q-1$:

$$N^*(\psi) = \frac{1}{q-1}\left[q^3 - 4q^3 + 6q - 4 - \frac{1}{q}\sum_{i=1}^{6} J\left(\frac{k}{7}, \frac{2k}{7}, \frac{4k}{7}\right)\right.$$

$$-\sum_{k=1}^{q-2} \frac{g\left(\frac{k}{q-1}\right)^4}{g\left(\frac{4k}{q-1}\right)}\chi_{4k}(4\psi)$$

$$-\frac{3}{q-1}\sum_{k=1}^{q-2}\frac{g\left(\frac{k}{q-1}\right)g\left(\frac{k}{q-1}+\frac{1}{7}\right)g\left(\frac{k}{q-1}+\frac{2}{7}\right)g\left(\frac{k}{q-1}+\frac{4}{7}\right)}{g\left(\frac{4k}{q-1}\right)}\chi_{4k}(4\psi)$$

$$-\frac{3}{q-1}\sum^{q-2} g\left(\frac{k}{q-1}\right)g\left(\frac{k}{q-1}+\frac{3}{7}\right)g\left(\frac{k}{q-1}+\frac{5}{7}\right)g\left(\frac{k}{q-1}+\frac{6}{7}\right) \ldots (4\psi)$$

Zeta function of the mirror

de la Ossa:

$$\mathrm{Zeta}(Y/\mathbb{F}_p, T) = \frac{1}{(1-T)(1-pT)^{19}(1-p^2T)R_{(0,0,0,0)}(T)}$$

Conjecture: Factor corresponding to invariant period appears in mirror zeta function and alternate pencils.

We have a formula involving Jacobi sums. How can we compute these?

We have a formula involving Jacobi sums. How can we compute these?

1. Compute directly - By properties of Jacobi sums, an order r Jacobi sum can be expressed as a product of $r-1$ Jacobi sums of order 2. The total cost of the computation is of the order $O((r-1)q^2)$.

We have a formula involving Jacobi sums. How can we compute these?

1. Compute directly - By properties of Jacobi sums, an order r Jacobi sum can be expressed as a product of $r-1$ Jacobi sums of order 2. The total cost of the computation is of the order $O((r-1)q^2)$.
2. Can gain a factor of $(r-1)$ by fixing a generator of the multiplicative character group.

We have a formula involving Jacobi sums. How can we compute these?

1. Compute directly - By properties of Jacobi sums, an order r Jacobi sum can be expressed as a product of $r-1$ Jacobi sums of order 2. The total cost of the computation is of the order $O((r-1)q^2)$.
2. Can gain a factor of $(r-1)$ by fixing a generator of the multiplicative character group.
3. Louboutin - if $p=q$ (the largest part of the computation), Gauss sums are linked to the root numbers of θ-functions associated to the characters. Cost is $O(q^{3/2+\varepsilon})$.

We have a formula involving Jacobi sums. How can we compute these?

1. Compute directly - By properties of Jacobi sums, an order r Jacobi sum can be expressed as a product of $r-1$ Jacobi sums of order 2. The total cost of the computation is of the order $O((r-1)q^2)$.
2. Can gain a factor of $(r-1)$ by fixing a generator of the multiplicative character group.
3. Louboutin - if $p = q$ (the largest part of the computation), Gauss sums are linked to the root numbers of θ-functions associated to the characters. Cost is $O(q^{3/2+\varepsilon})$.
4. Use p-adic Gamma function. Cost is about $O(p^{1+\varepsilon})$, no more efficiend than theta functions a priori.

The main interest is we only need to compute values modulo p or p^2, since we know the number of points is an integer and we have the Weil-Deligne bounds. Although this is a $O(q^2)$ method, it is the best available when $p = q^2$, and even when $p = q$, since we can work mod p and the implicit constant of $O()$ is very small, it is quite competitive in practice ($p \leq 10^4$ for instance).

Things we can compute

- Basic: Convert Pari code to Sage code.
- Count points on hypersurfaces in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$.
- Count points on the mirror hypersurfaces.