Counting matrix points on curves and surfaces with partitions

Hasan Saad (University of Virginia)

(joint with Y. Huang and K. Ono)

PARTITIONS

1. Number theory

Partitions

1. Number theory
   - Asymptotics of the partition function (circle method)
   - Ramanujan's partition congruences

Partitions

1. Number theory
   - Asymptotics of the partition function (circle method)
   - Ramanujan's partition congruences
2. Representation theory

Partitions

1. Number theory
    - Asymptotics of the partition function (circle method)
    - Ramanujan's partition congruences
2. Representation theory
    - Representation theory of the symmetric group S_n
    - Symmetric polynomials

Partitions

1. Number theory
   - Asymptotics of the partition function (circle method)
   - Ramanujan's partition congruences
2. Representation theory
   - Representation theory of the symmetric group S_n
   - Symmetric polynomials
3. Physics/Computer Science
   - Quantum states
   - Sorting (analogue of binary search tree)

Partitions

1. Number theory
   - Asymptotics of the partition function (circle method)
   - Ramanujan's partition congruences
2. Representation theory
   - Representation theory of the symmetric group S_n
   - Symmetric polynomials
3. Physics/Computer Science
   - Quantum states
   - Sorting (analogue of binary search tree)

Question

Do partitions show up in arithmetic geometry?

q-SERIES FORMULAS

QUESTION

What is the number of commuting square matrices A, B in $\mathbb{F}_q$?

q-SERIES FORMULAS

Question

What is the number of commuting square matrices A, B in $\mathbb{F}_q$?

Example

of 1×1 commuting "matrices" (elements) is q^2

q-SERIES FORMULAS

QUESTION

What is the number of commuting square matrices A, B in $\mathbb{F}_q$?

EXAMPLE

of 1×1 commuting "matrices" (elements) is $q^2 = q \cdot \left(1 - \frac{1}{q}\right) \cdot \frac{q}{1-\frac{1}{q}}$.

q-SERIES FORMULAS

Question

What is the number of commuting square matrices A, B in $\mathbb{F}_q$?

Example

of 1×1 commuting "matrices" (elements) is $q^2 = q \cdot \left(1 - \frac{1}{q}\right) \cdot \frac{q}{1 - \frac{1}{q}}$.

Remark

$q \cdot \left(1 - \frac{1}{q}\right) = q - 1$ *is the number of nonzero elements of* $\mathbb{F}_q$.

Counting commuting 2×2 matrices

Example (Brute force)

For $\mathbb{F}_2$, we find that

$$\#\{(A, B) \in \mathrm{Mat}_2(\mathbb{F}_2)^2, AB = BA\} = 88.$$

Counting commuting 2×2 matrices

Example (Brute force)

For $\mathbb{F}_2$, we find that

$$\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_2)^2, AB = BA\} = 88.$$

$$q^{2^2}\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)\cdot\frac{q}{1-\frac{1}{q}} = 24,$$

$$q^{2^2}\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)\cdot\frac{q^2}{(1-\frac{1}{q})(1-\frac{1}{q^2})} = 64,$$

COUNTING COMMUTING 2×2 MATRICES

EXAMPLE (BRUTE FORCE)

For $\mathbb{F}_2$, we find that

$$\#\{(A, B) \in \mathrm{Mat}_2(\mathbb{F}_2)^2, AB = BA\} = 88.$$

$$q^{2^2}\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right) \cdot \frac{q}{1-\frac{1}{q}} = 24,$$

$$q^{2^2}\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right) \cdot \frac{q^2}{(1-\frac{1}{q})(1-\frac{1}{q^2})} = 64,$$

and $24 + 64 = 88$. Is this an accident?

Counting commuting 2×2 matrices

Example (Brute force)

$$\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_3)^2, AB = BA\} = 945.$$

Counting commuting 2×2 matrices

Example (Brute force)

$$\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_3)^2, AB = BA\} = 945.$$

$$945 = 3^{2^2}\left(1-\frac{1}{3}\right)\left(1-\frac{1}{3^2}\right)\left(\frac{3}{1-\frac{1}{3}} + \frac{3^2}{(1-\frac{1}{3})(1-\frac{1}{3^2})}\right).$$

Counting commuting 2×2 matrices

Example (Brute force)

$$\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_3)^2, AB = BA\} = 945.$$

$$945 = 3^{2^2}\left(1-\frac{1}{3}\right)\left(1-\frac{1}{3^2}\right)\left(\frac{3}{1-\frac{1}{3}} + \frac{3^2}{(1-\frac{1}{3})(1-\frac{1}{3^2})}\right).$$

Example (Brute force)

$$\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_5)^2, AB = BA\} = 18625.$$

Counting commuting 2×2 matrices

Example (Brute force)

$$\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_3)^2, AB = BA\} = 945.$$

$$945 = 3^{2^2}\left(1-\frac{1}{3}\right)\left(1-\frac{1}{3^2}\right)\left(\frac{3}{1-\frac{1}{3}} + \frac{3^2}{(1-\frac{1}{3})(1-\frac{1}{3^2})}\right).$$

Example (Brute force)

$$\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_5)^2, AB = BA\} = 18625.$$

$$18625 = 5^{2^2}\left(1-\frac{1}{5}\right)\left(1-\frac{1}{5^2}\right)\left(\frac{5}{1-\frac{1}{5}} + \frac{5^2}{(1-\frac{1}{5})(1-\frac{1}{5^2})}\right).$$

Counting commuting 2×2 matrices

Observation

For 2×2 matrices and $q = 2, 3, 5$, we have observed

$$\frac{\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_q)^2, AB = BA\}}{q^{2^2}\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)} = \left(\frac{q}{1-\frac{1}{q}} + \frac{q^2}{(1-\frac{1}{q})(1-\frac{1}{q^2})}\right).$$

Counting commuting 2×2 matrices

Observation

For 2×2 matrices and $q = 2, 3, 5$, we have observed

$$\frac{\#\{(A, B) \in \mathrm{Mat}_2(\mathbb{F}_q)^2, AB = BA\}}{q^{2^2}\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right)} = \left(\frac{q}{1 - \frac{1}{q}} + \frac{q^2}{(1 - \frac{1}{q})(1 - \frac{1}{q^2})}\right).$$

Question

Is this a coincidence?

Counting commuting 2×2 matrices

Observation

For 2×2 matrices and $q = 2, 3, 5$, we have observed

$$\frac{\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_q)^2, AB = BA\}}{q^{2^2}\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)} = \left(\frac{q}{1-\frac{1}{q}} + \frac{q^2}{(1-\frac{1}{q})(1-\frac{1}{q^2})}\right).$$

Question

Is this a coincidence? Is this a partitions phenomenon?

Counting commuting 2×2 matrices

Observation

For 2×2 matrices and $q = 2, 3, 5$, we have observed

$$\frac{\#\{(A,B) \in \mathrm{Mat}_2(\mathbb{F}_q)^2, AB = BA\}}{q^{2^2}\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)} = \left(\frac{q}{1-\frac{1}{q}} + \frac{q^2}{(1-\frac{1}{q})(1-\frac{1}{q^2})}\right).$$

Question

Is this a coincidence? Is this a partitions phenomenon?
What about $n \times n$ matrices for all n?

PARTITIONS OF n AND $n \times n$ MATRICES

THEOREM (FEIT, FINE (1960))

If $P(n,q) := \#\{(A,B) \in \mathrm{Mat}_n(\mathbb{F}_q)^2, AB = BA\}$, *then*

Partitions of n and $n \times n$ matrices

Theorem (Feit, Fine (1960))

If $P(n,q) := \#\{(A,B) \in \mathrm{Mat}_n(\mathbb{F}_q)^2, AB = BA\}$, *then*

$$P(n,q) = q^{n^2}(q^{-1};q^{-1})_n \cdot \sum_{\lambda \vdash n} \frac{q^{l(\lambda)}}{(q^{-1};q^{-1})_{b(\lambda,1)} \cdot \ldots \cdot (q^{-1};q^{-1})_{b(\lambda,n)}},$$

PARTITIONS OF n AND $n \times n$ MATRICES

THEOREM (FEIT, FINE (1960))

If $P(n,q) := \#\{(A,B) \in \mathrm{Mat}_n(\mathbb{F}_q)^2, AB = BA\}$, *then*

$$P(n,q) = q^{n^2}(q^{-1};q^{-1})_n \cdot \sum_{\lambda \vdash n} \frac{q^{l(\lambda)}}{(q^{-1};q^{-1})_{b(\lambda,1)} \cdot \ldots \cdot (q^{-1};q^{-1})_{b(\lambda,n)}},$$

where

$$(a;q)_n := (1-a)(1-aq)\ldots(1-aq^{n-1}),$$

and $n = 1 \cdot b(\lambda,1) + \ldots + n \cdot b(\lambda,n)$ *and* $l(\lambda) = \sum b(\lambda,i)$.

Matrix points on curves and surfaces

Questions

1. *Do partitions count equations other than* $AB - BA = 0$*?*

Matrix points on curves and surfaces

Questions

1. *Do partitions count equations other than* $AB - BA = 0$*?*
2. *Distributions of matrix points for families of curves and surfaces?*

Matrix points on curves and surfaces

Questions

1. *Do partitions count equations other than* $AB - BA = 0$*?*
2. *Distributions of matrix points for families of curves and surfaces?*

Answer (Our work)

We answer these questions for "elliptic curves"

$$B^2 = A(A - I_n)(A - aI_n),$$

Matrix points on curves and surfaces

Questions

1. *Do partitions count equations other than* $AB - BA = 0$*?*
2. *Distributions of matrix points for families of curves and surfaces?*

Answer (Our work)

We answer these questions for "elliptic curves"

$$B^2 = A(A - I_n)(A - aI_n),$$

and AOP K3 surfaces

$$C^2 = AB(A + I_n)(B + I_n)(A + aB),$$

where I_n *is the identity matrix and* $a \in \mathbb{F}_q$.

Partitions and Nilpotent Matrices

Definition

Let A be a **nilpotent** $n \times n$ matrix.

Partitions and Nilpotent Matrices

Definition

Let A be a **nilpotent** $n \times n$ matrix.
There is a basis $\{v_s^i\}, i = 1, \ldots, k, s = 1, \ldots, r_i$ with

$$Av_s^i = v_{s-1}^i.$$

Partitions and Nilpotent Matrices

Definition

Let A be a **nilpotent** $n \times n$ matrix.
There is a basis $\{v_s^i\}, i = 1, \ldots, k, s = 1, \ldots, r_i$ with

$$Av_s^i = v_{s-1}^i.$$

We associate with A the partition

$$\pi(A) : n = r_1 + \ldots + r_k.$$

Example

Consider the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

Example

Consider the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

We have that $A^3 = 0$.

Example

Consider the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

We have that $A^3 = 0$. Consider the basis

$$\begin{aligned} v_1^1 &= e_3 \\ v_2^1 &= e_2 \\ v_3^1 &= e_1 - e_2. \end{aligned}$$

with e_1, e_2, e_3 the standard basis.

Example

Consider the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

We have that $A^3 = 0$. Consider the basis

$$\begin{aligned} v_1^1 &= e_3 \\ v_2^1 &= e_2 \\ v_3^1 &= e_1 - e_2. \end{aligned}$$

with e_1, e_2, e_3 the standard basis.Then, we have

$$Av_3^1 = v_2^1$$

and

$$Av_2^1 = Av_1^1.$$

Partitions and nilpotent matrices

Lemma

$A_1 \sim A_2$ *if and only if* $\pi(A_1) = \pi(A_2)$.

Partitions and nilpotent matrices

Lemma

$A_1 \sim A_2$ *if and only if* $\pi(A_1) = \pi(A_2)$.

Lemma

If $N(s,q) := \#\{(A,B) \in \mathrm{Mat}_s(\mathbb{F}_q)^2, AB = BA, A \text{ nilpotent}\}$, *then*

Partitions and nilpotent matrices

Lemma

$A_1 \sim A_2$ *if and only if* $\pi(A_1) = \pi(A_2)$.

Lemma

If $N(s,q) := \#\{(A,B) \in \mathrm{Mat}_s(\mathbb{F}_q)^2, AB = BA, A \text{ nilpotent}\}$, *then*

$$N(s,q) = q^{s^2}(q^{-1};q^{-1})_s \cdot \sum_{\lambda \vdash s} \frac{1}{(q^{-1};q^{-1})_{b(\lambda,1)} \cdot \dots \cdot (q^{-1};q^{-1})_{b(\lambda,s)}}.$$

Partitions and nilpotent matrices

Lemma

$A_1 \sim A_2$ if and only if $\pi(A_1) = \pi(A_2)$.

Lemma

If $N(s,q) := \#\{(A,B) \in \mathrm{Mat}_s(\mathbb{F}_q)^2, AB = BA, A \text{ nilpotent}\}$, then

$$N(s,q) = q^{s^2}(q^{-1};q^{-1})_s \cdot \sum_{\lambda \vdash s} \frac{1}{(q^{-1};q^{-1})_{b(\lambda,1)} \cdot \ldots \cdot (q^{-1};q^{-1})_{b(\lambda,s)}}.$$

Sketch of Proof.

1. Fix a matrix A with $\pi(A) = \lambda$.

Partitions and nilpotent matrices

Lemma

$A_1 \sim A_2$ if and only if $\pi(A_1) = \pi(A_2)$.

Lemma

If $N(s,q) := \#\{(A,B) \in \mathrm{Mat}_s(\mathbb{F}_q)^2, AB = BA, A$ nilpotent$\}$, then

$$N(s,q) = q^{s^2}(q^{-1};q^{-1})_s \cdot \sum_{\lambda \vdash s} \frac{1}{(q^{-1};q^{-1})_{b(\lambda,1)} \cdot \ldots \cdot (q^{-1};q^{-1})_{b(\lambda,s)}}.$$

Sketch of Proof.

1. Fix a matrix A with $\pi(A) = \lambda$.
2. If B commutes with A then B is determined by $Bv^i_{r_i}$.

Partitions and nilpotent matrices

Lemma

$A_1 \sim A_2$ *if and only if* $\pi(A_1) = \pi(A_2)$.

Lemma

If $N(s,q) := \#\{(A,B) \in \mathrm{Mat}_s(\mathbb{F}_q)^2, AB = BA, A \text{ nilpotent}\}$, *then*

$$N(s,q) = q^{s^2}(q^{-1};q^{-1})_s \cdot \sum_{\lambda \vdash s} \frac{1}{(q^{-1};q^{-1})_{b(\lambda,1)} \cdot \ldots \cdot (q^{-1};q^{-1})_{b(\lambda,s)}}.$$

Sketch of Proof.

1. Fix a matrix A with $\pi(A) = \lambda$.
2. If B commutes with A then B is determined by $Bv^i_{r_i}$.
3. Determine possible images of $Bv^i_{r_i}$.

Partitions and nilpotent matrices

Lemma

$A_1 \sim A_2$ if and only if $\pi(A_1) = \pi(A_2)$.

Lemma

If $N(s,q) := \#\{(A,B) \in \mathrm{Mat}_s(\mathbb{F}_q)^2, AB = BA, A \text{ nilpotent}\}$, then

$$N(s,q) = q^{s^2}(q^{-1};q^{-1})_s \cdot \sum_{\lambda \vdash s} \frac{1}{(q^{-1};q^{-1})_{b(\lambda,1)} \cdot \ldots \cdot (q^{-1};q^{-1})_{b(\lambda,s)}}.$$

Sketch of Proof.

1. Fix a matrix A with $\pi(A) = \lambda$.
2. If B commutes with A then B is determined by $Bv^i_{r_i}$.
3. Determine possible images of $Bv^i_{r_i}$.
4. B is nonsingular if and only if Bv^i_1 are linearly independent.

Partitions and nilpotent matrices

Lemma

$A_1 \sim A_2$ *if and only if* $\pi(A_1) = \pi(A_2)$.

Lemma

If $N(s,q) := \#\{(A,B) \in \mathrm{Mat}_s(\mathbb{F}_q)^2, AB = BA, A \text{ nilpotent}\}$, *then*

$$N(s,q) = q^{s^2}(q^{-1};q^{-1})_s \cdot \sum_{\lambda \vdash s} \frac{1}{(q^{-1};q^{-1})_{b(\lambda,1)} \cdot \dots \cdot (q^{-1};q^{-1})_{b(\lambda,s)}}.$$

Sketch of Proof.

1. Fix a matrix A with $\pi(A) = \lambda$.
2. If B commutes with A then B is determined by $Bv^i_{r_i}$.
3. Determine possible images of $Bv^i_{r_i}$.
4. B is nonsingular if and only if Bv^i_1 are linearly independent.
5. Determine possible Bv^1_i for nonsingular B.

□

Partitions and Nonsingular Matrices

Lemma

If $R(t,q) := \#\{(A,B) \in \mathrm{Mat}_t(\mathbb{F}_q)^2, AB = BA, A \text{ nonsingular}\}$, *then*

Partitions and Nonsingular Matrices

Lemma

If $R(t,q) := \#\{(A,B) \in \mathrm{Mat}_t(\mathbb{F}_q)^2, AB = BA, A \text{ nonsingular}\}$, *then*

$$R(t,q) = q^{t^2}(q^{-1};q^{-1})_t \cdot \#\{\beta\},$$

where $\#\{\beta\}$ *denotes the number of similarity classes of* $t \times t$*-matrices.*

Partitions and Nonsingular Matrices

Lemma

If $R(t,q) := \#\{(A,B) \in \mathrm{Mat}_t(\mathbb{F}_q)^2, AB = BA, A \text{ nonsingular}\}$, *then*

$$R(t,q) = q^{t^2}(q^{-1};q^{-1})_t \cdot \#\{\beta\},$$

where $\#\{\beta\}$ *denotes the number of similarity classes of* $t \times t$*-matrices.*

Proof.

1. $AB = BA$ is equivalent to $ABA^{-1} = B$.

Partitions and Nonsingular Matrices

Lemma

If $R(t,q) := \#\{(A,B) \in \mathrm{Mat}_t(\mathbb{F}_q)^2, AB = BA, A \text{ nonsingular}\}$, *then*

$$R(t,q) = q^{t^2}(q^{-1};q^{-1})_t \cdot \#\{\beta\},$$

where $\#\{\beta\}$ *denotes the number of similarity classes of* $t \times t$*-matrices.*

Proof.

1. $AB = BA$ is equivalent to $ABA^{-1} = B$.
2. Fix $B \in \beta$.

Partitions and Nonsingular Matrices

Lemma

If $R(t,q) := \#\{(A,B) \in \mathrm{Mat}_t(\mathbb{F}_q)^2, AB = BA, A \text{ nonsingular}\}$, *then*

$$R(t,q) = q^{t^2}(q^{-1};q^{-1})_t \cdot \#\{\beta\},$$

where $\#\{\beta\}$ *denotes the number of similarity classes of* $t \times t$*-matrices.*

Proof.

1. $AB = BA$ is equivalent to $ABA^{-1} = B$.
2. Fix $B \in \beta$.
3. $\#\{A \text{ is nonsingular and } ABA^{-1} = B\}$

Partitions and Nonsingular Matrices

Lemma

If $R(t,q) := \#\{(A,B) \in \mathrm{Mat}_t(\mathbb{F}_q)^2, AB = BA, A \text{ nonsingular}\}$*, then*

$$R(t,q) = q^{t^2}(q^{-1};q^{-1})_t \cdot \#\{\beta\},$$

where $\#\{\beta\}$ *denotes the number of similarity classes of* $t \times t$*-matrices.*

Proof.

1. $AB = BA$ is equivalent to $ABA^{-1} = B$.
2. Fix $B \in \beta$.
3. $\#\{A \text{ is nonsingular and } ABA^{-1} = B\} = \frac{q^{t^2}(q^{-1};q^{-1})_t}{\#\beta}$.

Partitions and Nonsingular Matrices

Lemma

If $R(t,q) := \#\{(A,B) \in \mathrm{Mat}_t(\mathbb{F}_q)^2, AB = BA, A \text{ nonsingular}\}$, *then*

$$R(t,q) = q^{t^2}(q^{-1};q^{-1})_t \cdot \#\{\beta\},$$

where $\#\{\beta\}$ *denotes the number of similarity classes of* $t \times t$*-matrices.*

Proof.

1. $AB = BA$ is equivalent to $ABA^{-1} = B$.
2. Fix $B \in \beta$.
3. $\#\{A \text{ is nonsingular and } ABA^{-1} = B\} = \frac{q^{t^2}(q^{-1};q^{-1})_t}{\#\beta}$.
4. Sum over $B \in \beta$.

□

Partitions and nonsingular matrices

Lemma

$$\#\{\beta\} = \sum_{\lambda \vdash t} q^{l(\lambda)}.$$

Partitions and nonsingular matrices

Lemma

$$\#\{\beta\} = \sum_{\lambda \vdash t} q^{l(\lambda)}.$$

Proof.

1. Similarity class is determined by rational canonical form $g_1, \ldots, g_{t-1}$. '

PARTITIONS AND NONSINGULAR MATRICES

LEMMA

$$\#\{\beta\} = \sum_{\lambda \vdash t} q^{l(\lambda)}.$$

PROOF.

1. Similarity class is determined by rational canonical form $g_1, \ldots, g_{t-1}$.
2. Take $h_i = g_{t+1-i}/g_{t-i}$ and $b_i = \deg h_i$.

Partitions and nonsingular matrices

Lemma

$$\#\{\beta\} = \sum_{\lambda \vdash t} q^{l(\lambda)}.$$

Proof.

1. Similarity class is determined by rational canonical form $g_1, \ldots, g_{t-1}$.
2. Take $h_i = g_{t+1-i}/g_{t-i}$ and $b_i = \deg h_i$.
3. $\sum ib_i = t$ is the only restriction on h_i.

$\square$

Proof of Feit-Fine Theorem

Proof.

1. By elementary linear algebra,

$$P(n,q) = \sum_{s+t=n} h(s,t,q)N(s,q)R(t,q),$$

where $h(s,t,q) := \#$ of complementary subspaces of dim s and t.

Proof of Feit-Fine Theorem

Proof.

1. By elementary linear algebra,

$$P(n,q) = \sum_{s+t=n} h(s,t,q) N(s,q) R(t,q),$$

   where $h(s,t,q) := \#$ of complementary subspaces of dim s and t.

2. Write $\sum \frac{P(n,q)}{q^{n^2}(q^{-1},q^{-1})_n} x^n$ in terms of $N(s,q)$ and $R(t,q)$.

Proof of Feit-Fine Theorem

Proof.

1. By elementary linear algebra,

$$P(n,q) = \sum_{s+t=n} h(s,t,q)N(s,q)R(t,q),$$

   where $h(s,t,q) := \#$ of complementary subspaces of dim s and t.

2. Write $\sum \frac{P(n,q)}{q^{n^2}(q^{-1},q^{-1})_n} x^n$ in terms of $N(s,q)$ and $R(t,q)$.

3. Use Euler's partition formula

$$\prod_{j\geq 1}(1-tq^{-j})^{-1} = \sum_{m\geq 0} \frac{t^m}{(q^{-1};q^{-1})_m},$$

   where $(a;q)_n := (1-a)(1-aq)\dots(1-aq^{n-1})$.

□

$\mathbb{F}_q$-RATIONAL POINTS (i.e. $n = 1$)

QUESTION

How do we count $\mathbb{F}_q$-solutions to

$$E_a^{\text{Leg}}: \quad y^2 = x(x-1)(x-a)$$

and

$$X_a: \quad s^2 = xy(x+1)(y+1)(x+ay)?$$

$\mathbb{F}_q$-RATIONAL POINTS (i.e. $n = 1$)

Question

How do we count $\mathbb{F}_q$-solutions to

$$E_a^{\mathrm{Leg}}: \quad y^2 = x(x-1)(x-a)$$

and

$$X_a: \quad s^2 = xy(x+1)(y+1)(x+ay)?$$

Answer

The number of points is given by finite field hypergeometric functions.

Finite field Hypergeometric Functions

Definition (Greene)

If $A_1, A_2, \ldots, A_n$ and $B_1, B_2, \ldots, B_{n-1}$ are characters of $\mathbb{F}_q^\times$, then their **Gaussian hypergeometric function** is

$$
{}_nF_{n-1}\left(\begin{matrix} A_1, & A_2, & \ldots, & A_n \\ & B_1, & \ldots, & B_{n-1} \end{matrix} \;\middle|\; x\right)_{\mathbb{F}_q} :=
$$

$$
\frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}}_q^\times} \binom{A_1\chi}{\chi}\binom{A_2\chi}{B_1\chi}\cdots\binom{A_n\chi}{B_{n-1}\chi} \cdot \chi(x),
$$

Finite field Hypergeometric Functions

Definition (Greene)

If $A_1, A_2, \ldots, A_n$ and $B_1, B_2, \ldots, B_{n-1}$ are characters of $\mathbb{F}_q^\times$, then their **Gaussian hypergeometric function** is

$$
{}_nF_{n-1}\left(\begin{matrix} A_1, & A_2, & \ldots, & A_n \\ & B_1, & \ldots, & B_{n-1} \end{matrix} \;\middle|\; x\right)_{\mathbb{F}_q} :=
$$

$$
\frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}}_q^\times} \binom{A_1\chi}{\chi} \binom{A_2\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_{n-1}\chi} \cdot \chi(x),
$$

where

$$
\binom{A}{B} := \frac{B(-1)}{q} J(A, \overline{B}) = \frac{B(-1)}{q} \sum_{y \in \mathbb{F}_q} A(y)\overline{B}(1-y).
$$

is a normalized Jacobi sum.

Finite Field Hypergeometric Functions

Example

1. $${}_2F_1\left(\begin{matrix}\phi & \phi \\ & \varepsilon\end{matrix} \;\middle|\; a\right)_{\mathbb{F}_q} = \frac{\phi(-1)}{q}\sum_{x\in\mathbb{F}_q}\phi(x(x-1)(x-a)).$$

Finite Field Hypergeometric Functions

Example

1. $$ {}_2F_1\left(\begin{matrix} \phi & \phi \\ & \varepsilon \end{matrix} \;\middle|\; a\right)_{\mathbb{F}_q} = \frac{\phi(-1)}{q} \sum_{x \in \mathbb{F}_q} \phi(x(x-1)(x-a)). $$

2. $$ {}_3F_2\left(\begin{matrix} \phi & \phi & \phi \\ & \varepsilon & \varepsilon \end{matrix} \;\middle|\; -a\right)_{\mathbb{F}_q} = \frac{1}{q^2} \sum_{x,y \in \mathbb{F}_q} \phi(x(x+1)y(y+1)(x+ay)). $$

Finite Field Hypergeometric Functions

Example

1. $$ {}_2F_1\left(\begin{matrix} \phi & \phi \\ & \varepsilon \end{matrix} \;\middle|\; a\right)_{\mathbb{F}_q} = \frac{\phi(-1)}{q} \sum_{x \in \mathbb{F}_q} \phi(x(x-1)(x-a)). $$

2. $$ {}_3F_2\left(\begin{matrix} \phi & \phi & \phi \\ & \varepsilon & \varepsilon \end{matrix} \;\middle|\; -a\right)_{\mathbb{F}_q} = \frac{1}{q^2} \sum_{x,y \in \mathbb{F}_q} \phi(x(x+1)y(y+1)(x+ay)). $$

Theorem (Greene (1984), Ono (1998))

(1) If $a \in \mathbb{F}_q \setminus \{0,1\}$ and $\mathrm{char}(\mathbb{F}_q) \geq 5$, then

$$ \#E_a^{\mathrm{Leg}}(\mathbb{F}_q) = q + 1 + \phi(-1)q \cdot {}_2F_1(a)_{\mathbb{F}_q}. $$

Finite Field Hypergeometric Functions

Example

1. $$ {}_2F_1\left(\begin{matrix} \phi & \phi \\ & \varepsilon \end{matrix} \mid a\right)_{\mathbb{F}_q} = \frac{\phi(-1)}{q} \sum_{x \in \mathbb{F}_q} \phi(x(x-1)(x-a)). $$

2. $$ {}_3F_2\left(\begin{matrix} \phi & \phi & \phi \\ & \varepsilon & \varepsilon \end{matrix} \mid -a\right)_{\mathbb{F}_q} = \frac{1}{q^2} \sum_{x,y \in \mathbb{F}_q} \phi(x(x+1)y(y+1)(x+ay)). $$

Theorem (Greene (1984), Ono (1998))

(1) If $a \in \mathbb{F}_q \setminus \{0,1\}$ *and* $\mathrm{char}(\mathbb{F}_q) \geq 5$, *then*

$$ \#E_a^{\mathrm{Leg}}(\mathbb{F}_q) = q + 1 + \phi(-1)q \cdot {}_2F_1(a)_{\mathbb{F}_q}. $$

(2) If $a \in \mathbb{F}_q \setminus \{0,-1\}$ *and* $\mathrm{char}(\mathbb{F}_q) \geq 5$, *then*

Finite Field Hypergeometric Functions

Example

1. $$ {}_2F_1\left(\begin{matrix}\phi & \phi \\ & \varepsilon\end{matrix} \mid a\right)_{\mathbb{F}_q} = \frac{\phi(-1)}{q}\sum_{x\in\mathbb{F}_q}\phi(x(x-1)(x-a)). $$

2. $$ {}_3F_2\left(\begin{matrix}\phi & \phi & \phi \\ & \varepsilon & \varepsilon\end{matrix} \mid -a\right)_{\mathbb{F}_q} = \frac{1}{q^2}\sum_{x,y\in\mathbb{F}_q}\phi(x(x+1)y(y+1)(x+ay)). $$

Theorem (Greene (1984), Ono (1998))

(1) If $a\in\mathbb{F}_q\setminus\{0,1\}$ *and* $\mathrm{char}(\mathbb{F}_q)\geq 5$, *then*

$$ \#E_a^{\mathrm{Leg}}(\mathbb{F}_q) = q+1+\phi(-1)q\cdot {}_2F_1(a)_{\mathbb{F}_q}. $$

(2) If $a\in\mathbb{F}_q\setminus\{0,-1\}$ *and* $\mathrm{char}(\mathbb{F}_q)\geq 5$, *then*

$$ \#X_a(\mathbb{F}_q) = 1+q^2+19q+q^2\cdot {}_3F_2(-a)_{\mathbb{F}_q}. $$

Matrix Varieties

Definition

Let q be a prime power, $n \geq 1$, and consider the system of equations

$$f_1(t_1, \ldots, t_m) = \ldots = f_r(t_1, \ldots, t_m) = 0.$$

Matrix Varieties

Definition

Let q be a prime power, $n \geq 1$, and consider the system of equations

$$f_1(t_1, \ldots, t_m) = \ldots = f_r(t_1, \ldots, t_m) = 0.$$

Its **affine variety** is

$$X(M_n(\mathbb{F}_q)) := \left\{ (A_1, \ldots, A_m) \;\middle|\; \begin{array}{l} A_i \in \mathrm{Mat}_n(\mathbb{F}_q), A_i A_j = A_j A_i \\ f_s(A_1, \ldots, A_m) = 0 \text{ for } 1 \leq s \leq r \end{array} \right\}.$$

MATRIX POINTS ON ELLIPTIC CURVES

QUESTION

What is the number of points $N_n^{\mathrm{Leg}}(a;q) := \#E_a^{\mathrm{Leg}}(M_n(\mathbb{F}_q))$?

MATRIX POINTS ON ELLIPTIC CURVES

Question

What is the number of points $N_n^{\mathrm{Leg}}(a;q) := \#E_a^{\mathrm{Leg}}(M_n(\mathbb{F}_q))$?

Theorem (Huang, Ono, S.)

If $q = p^r$ *with* $p \geq 5$ *and* $a \in \mathbb{F}_q \setminus \{0,1\}$, *then*

$$N_n^{\mathrm{Leg}}(a;q) = \sum_{k=0}^{n} \phi_{q^k}(-1) \cdot P(n,k)_q \cdot {}_2F_1(a)_{q^k},$$

MATRIX POINTS ON ELLIPTIC CURVES

Question

What is the number of points $N_n^{\mathrm{Leg}}(a;q) := \#E_a^{\mathrm{Leg}}(M_n(\mathbb{F}_q))$?

Theorem (Huang, Ono, S.)

If $q = p^r$ *with* $p \geq 5$ *and* $a \in \mathbb{F}_q \setminus \{0,1\}$, *then*

$$N_n^{\mathrm{Leg}}(a;q) = \sum_{k=0}^{n} \phi_{q^k}(-1) \cdot P(n,k)_q \cdot {}_2F_1(a)_{q^k},$$

where

$$P(n,k)_q := (-1)^k q^{n(n-k)+\frac{k(k+1)}{2}} \sum_{s=0}^{\lfloor \frac{n-k}{2} \rfloor} q^{2s(s-n+k)} \cdot \frac{(q;q)_n}{(q;q)_s (q;q)_{k+s} (q;q)_{n-k-2s}}.$$

Sato-Tate Distribution

Theorem (Huang, Ono, S.)

If $n \geq 1$, $q = p^r$ *with* $p \geq 5$ *and* $a \in \mathbb{F}_q$, *then write*

$$a_{L,n}(a;q) := N_n^{\mathrm{Leg}}(a;q) - P(n,0)_q.$$

Sato-Tate Distribution

Theorem (Huang, Ono, S.)

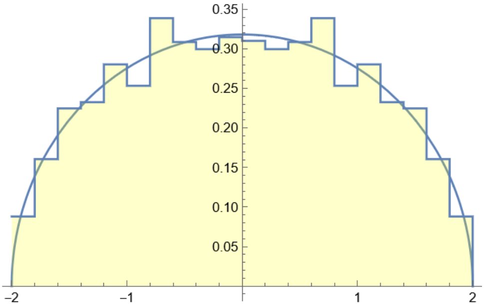
If $n \geq 1$, $q = p^r$ *with* $p \geq 5$ *and* $a \in \mathbb{F}_q$, *then write*

$$a_{L,n}(a;q) := N_n^{\mathrm{Leg}}(a;q) - P(n,0)_q.$$

If $-2 \leq b < c \leq 2$, *then*

$$\lim_{p\to\infty} \frac{\#\{a \in \mathbb{F}_q : q^{\frac{1}{2}-n^2} a_{L,n}(a;q) \in [b,c]\}}{q} = \frac{1}{2\pi}\int_b^c \sqrt{4-t^2}\,dt.$$

Histogram for Legendre ECs



2×2 matrices on Legendre elliptic curves

Matrix points on K3 surfaces

Question

What is the number of points $N_n^{\mathrm{K3}}(a;q) := \#X_a(M_n(\mathbb{F}_q))$?

Matrix points on K3 surfaces

Question

What is the number of points $N_n^{\mathrm{K3}}(a;q) := \#X_a(M_n(\mathbb{F}_q))$?

Theorem (Huang, Ono, S.)

If $q = p^r$ *with* $p \geq 5$ *and* $a \in \mathbb{F}_q \setminus \{0, -1\}$, *then*

$$N_n^{\mathrm{K3}}(a;q) = R(n, \phi_q(a+1))_q + \sum_{k=0}^{n} \phi_{q^k}(-1) \cdot Q(n, k, \phi_{q^k}(a+1))_q \cdot {}_3F_2\left(\frac{a}{a+1}\right)_{q^k},$$

Matrix points on K3 surfaces

Question

What is the number of points $N_n^{\mathrm{K3}}(a;q) := \#X_a(M_n(\mathbb{F}_q))$?

Theorem (Huang, Ono, S.)

If $q = p^r$ *with* $p \geq 5$ *and* $a \in \mathbb{F}_q \setminus \{0,-1\}$, *then*

$$N_n^{\mathrm{K3}}(a;q) = R(n, \phi_q(a+1))_q + \sum_{k=0}^{n} \phi_{q^k}(-1) \cdot Q(n,k,\phi_{q^k}(a+1))_q \cdot {}_3F_2\left(\frac{a}{a+1}\right)_{q^k},$$

where

$$Q(n,k,\gamma)_q := q^{\frac{n(n-1)}{2}+k} \sum_{\substack{\lambda_1,\ldots,\lambda_4 \\ |\lambda_1|+\ldots+|\lambda_4|=n \\ l(\lambda_3)-l(\lambda_4)=k}} q^{l(\lambda_1)} \gamma^{l(\lambda_2)} (-1)^{n-m(\lambda_1,\ldots,\lambda_4)}$$

$$(q,q)_{n-m(\lambda_1,\ldots,\lambda_4)} \cdot q^{\sum \frac{b(\lambda_i,j)(b(\lambda_i,j)+1)}{2}} \cdot \frac{(q;q)_n}{\prod (q;q)_{b(\lambda_i,j)} (q;q)_{n-m(\lambda_1,\ldots,\lambda_4)}}$$

and $R(n,\gamma)_q$ *is an explicit polynomial in* q *and* $m(\lambda_1,\ldots,\lambda_4) = \sum_{i=1}^{4} l(\lambda_i)$.

Sato-Tate Distributions

Theorem (Huang, Ono, S.)

If $n \geq 1$, $q = p^r$ with $p \geq 5$ and $a \in \mathbb{F}_q$, then write

$$A_n(a;q) := N_n^{\mathrm{K3}}(a;q) - Q(n, 0, \phi_q(a+1))_q - R(n, \phi_q(a+1))_q.$$

Sato-Tate Distributions

Theorem (Huang, Ono, S.)

If $n \geq 1$, $q = p^r$ *with* $p \geq 5$ *and* $a \in \mathbb{F}_q$, *then write*

$$A_n(a;q) := N_n^{\mathrm{K3}}(a;q) - Q(n,0,\phi_q(a+1))_q - R(n,\phi_q(a+1))_q.$$

If $-3 \leq b < c \leq 3$, *then*

$$\lim_{p\to\infty} \frac{\#\{a \in \mathbb{F}_q : q^{1-n^2-n} A_n(a;q) \in [b,c]\}}{q} = \frac{1}{4\pi}\int_b^c f(t)dt,$$

Sato-Tate Distributions

Theorem (Huang, Ono, S.)

If $n \geq 1$, $q = p^r$ *with* $p \geq 5$ *and* $a \in \mathbb{F}_q$, *then write*

$$A_n(a;q) := N_n^{\mathrm{K3}}(a;q) - Q(n,0,\phi_q(a+1))_q - R(n,\phi_q(a+1))_q.$$

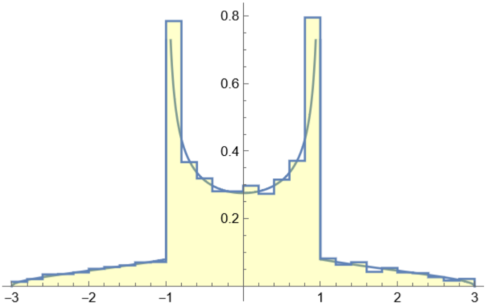
If $-3 \leq b < c \leq 3$, *then*

$$\lim_{p\to\infty} \frac{\#\{a \in \mathbb{F}_q : q^{1-n^2-n} A_n(a;q) \in [b,c]\}}{q} = \frac{1}{4\pi}\int_b^c f(t)dt,$$

where

$$f(t) = \begin{cases} \frac{3-|t|}{\sqrt{3+2|t|-t^2}} & \text{if } 1 < |t| < 3, \\ \frac{3+t}{\sqrt{3-2t-t^2}} + \frac{3-t}{\sqrt{3+2t-t^2}} & \text{if } |t| < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Histogram for AOP K3 surfaces



2×2 matrices on AOP K3 Surfaces

Traces of Frobenius

Definition

Let E be an elliptic curve. For prime powers q, define the **trace of Frobenius** $a(q) \in [-2\sqrt{q}, 2\sqrt{q}]$ by

$$a(q) := q + 1 - \#E(\mathbb{F}_q).$$

Traces of Frobenius

Definition

Let E be an elliptic curve. For prime powers q, define the **trace of Frobenius** $a(q) \in [-2\sqrt{q}, 2\sqrt{q}]$ by

$$a(q) := q + 1 - \#E(\mathbb{F}_q).$$

Definition

Let E be an elliptic curve and q a prime power. Take $\pi, \overline{\pi}$ such that

$$\pi + \overline{\pi} = a(q)$$

and

$$\pi\overline{\pi} = q.$$

Traces of Frobenius

Definition

Let E be an elliptic curve. For prime powers q, define the **trace of Frobenius** $a(q) \in [-2\sqrt{q}, 2\sqrt{q}]$ by

$$a(q) := q + 1 - \#E(\mathbb{F}_q).$$

Definition

Let E be an elliptic curve and q a prime power. Take $\pi, \overline{\pi}$ such that

$$\pi + \overline{\pi} = a(q)$$

and

$$\pi\overline{\pi} = q.$$

π and $\overline{\pi}$ are called the **eigenvalues of Frobenius.**

Zeta function of a variety

Definition

Let $V/\mathbb{F}_q$ be an affine variety. The zeta function of $V/\mathbb{F}_q$ is the power series

$$Z(V/\mathbb{F}_q;T) := \exp\left(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}\right).$$

Zeta function of a variety

Definition

Let $V/\mathbb{F}_q$ be an affine variety. The zeta function of $V/\mathbb{F}_q$ is the power series

$$Z(V/\mathbb{F}_q;T) := \exp\left(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}\right).$$

Classical Fact

Let E be an elliptic curve and $a(q)$ its trace of Frobenius at q.

Zeta function of a variety

Definition

Let $V/\mathbb{F}_q$ be an affine variety. The zeta function of $V/\mathbb{F}_q$ is the power series

$$Z(V/\mathbb{F}_q;T) := \exp\left(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}\right).$$

Classical Fact

Let E be an elliptic curve and $a(q)$ its trace of Frobenius at q.

$$Z(E/\mathbb{F}_q;T) = \frac{1-a(q)T+qT^2}{(1-qT)}.$$

Cohen-Lenstra Zeta series

Definition

Let $q = p^r$, $n \geq 1$ and $X/\mathbb{F}_q$ an affine variety.

Cohen-Lenstra Zeta series

Definition

Let $q = p^r$, $n \geq 1$ and $X/\mathbb{F}_q$ an affine variety. We define a **Cohen-Lenstra zeta series**

$$\widehat{Z}_X(t) := \sum_{n \geq 0} \frac{\#X(M_n(\mathbb{F}_q))}{\#\mathrm{GL}_n(\mathbb{F}_q)} \cdot t^n.$$

Cohen-Lenstra Zeta series

Proposition (Huang)

Assume the notation above.

Cohen-Lenstra Zeta series

Proposition (Huang)

Assume the notation above.

1. *If X is a smooth curve over $\mathbb{F}_q$, then*

$$\widehat{Z}_X(t) = \prod_{i=1}^{\infty} Z_X(q^{-i}t).$$

Cohen-Lenstra Zeta series

Proposition (Huang)

Assume the notation above.

1. *If X is a smooth curve over $\mathbb{F}_q$, then*

$$\widehat{Z}_X(t) = \prod_{i=1}^{\infty} Z_X(q^{-i}t).$$

2. *If X is a smooth surface over $\mathbb{F}_q$, then*

$$\widehat{Z}_X(t) = \prod_{i,j\geq 1} Z_X(q^{-j}t^i).$$

Cohen-Lenstra Zeta Series

Proof.

1. $\widehat{Z}_X(x) = \prod_{P \in X} \widehat{Z}_{\widehat{O}_{X,P}}.$

Cohen-Lenstra Zeta Series

Proof.

1. $\widehat{Z}_X(x) = \prod_{P \in X} \widehat{Z}_{\widehat{O}_{X,P}}.$
2. $\widehat{O}_{X,P} = \kappa_P[[t]].$

Cohen-Lenstra Zeta Series

Proof.

1. $\widehat{Z}_X(x) = \prod_{P \in X} \widehat{Z}_{\widehat{O}_{X,P}}$.
2. $\widehat{O}_{X,P} = \kappa_P[[t]]$.
3. $\widehat{Z}_{\kappa_P[[t]]}$ counts nilpotent matrices.

Cohen-Lenstra Zeta Series

Proof.

1. $\widehat{Z}_X(x) = \prod_{P \in X} \widehat{Z}_{\widehat{O}_{X,P}}$.
2. $\widehat{O}_{X,P} = \kappa_P[[t]]$.
3. $\widehat{Z}_{\kappa_P[[t]]}$ counts nilpotent matrices.
4. Using Young diagrams, Fine and Herstein compute this series.

□

Cohen-Lenstra Zeta Series

Proof.

1. $\widehat{Z}_X(x) = \prod_{P \in X} \widehat{Z}_{\widehat{O}_{X,P}}$.
2. $\widehat{O}_{X,P} = \kappa_P[[t]]$.
3. $\widehat{Z}_{\kappa_P[[t]]}$ counts nilpotent matrices.
4. Using Young diagrams, Fine and Herstein compute this series.

$\square$

Remark

For surfaces, the local zeta function counts pairwise commuting nilpotent matrices. Evaluating this zeta series also requires partitions.

Expanding zeta series

Classical Fact

Let E be an elliptic curve and $\pi, \overline{\pi}$ the eigenvalues of Frobenius at q.

$$Z(E/\mathbb{F}_q;T) = \frac{(1-\pi T)(1-\overline{\pi}T)}{(1-qT)}.$$

Expanding zeta series

Classical Fact

Let E be an elliptic curve and $\pi, \overline{\pi}$ the eigenvalues of Frobenius at q.

$$Z(E/\mathbb{F}_q;T) = \frac{(1-\pi T)(1-\overline{\pi}T)}{(1-qT)}.$$

Problem

We need to find the series expansion of

$$\prod_{j\geq 1}(1-\pi T q^{-j})$$

and

$$\prod_{j\geq 1}\frac{1}{1-q^{1-j}T}.$$

EULER'S q-SERIES IDENTITIES

LEMMA (EULER)

The following series expansions hold.

1. $$\prod_{j\geq 1}(1-cq^{-j}) = \sum_{m\geq 0} \frac{c^m}{(q;q)_m}.$$

Euler's q-series identities

Lemma (Euler)

The following series expansions hold.

1. $$\prod_{j\geq 1}(1-cq^{-j}) = \sum_{m\geq 0}\frac{c^m}{(q;q)_m}.$$

2. $$\prod_{j\geq 1}\frac{1}{1-cq^{-j}} = \sum_{m\geq 0}\frac{(-1)^m q^{m(m-1)/2}c^m}{(q;q)_m}.$$

Proof of point counts

1. Write the Cohen-Lenstra zeta series

$$\widehat{Z}_X(T) = \prod_{j\geq 1} \frac{(1-\pi T q^{-j})(1-\overline{\pi} T q^{-j})}{1-Tq^{1-j}}.$$

Proof of point counts

1. Write the Cohen-Lenstra zeta series

$$\widehat{Z}_X(T) = \prod_{j\geq 1} \frac{(1-\pi T q^{-j})(1-\overline{\pi} T q^{-j})}{1-Tq^{1-j}}.$$

2. Expand the product of each factor as a series in T.

Proof of point counts

1. Write the Cohen-Lenstra zeta series
$$\widehat{Z}_X(T) = \prod_{j\geq 1} \frac{(1-\pi T q^{-j})(1-\overline{\pi} T q^{-j})}{1-Tq^{1-j}}.$$
2. Expand the product of each factor as a series in T.
3. Multiply the three resulting series to get the coefficient of T^n.

Proof of point counts

1. Write the Cohen-Lenstra zeta series

$$\widehat{Z}_X(T) = \prod_{j\geq 1} \frac{(1-\pi T q^{-j})(1-\overline{\pi} T q^{-j})}{1-Tq^{1-j}}.$$

2. Expand the product of each factor as a series in T.
3. Multiply the three resulting series to get the coefficient of T^n.
4. Use $\pi\overline{\pi} = q$ and $\pi + \overline{\pi} = \phi_q(-1) \cdot q \cdot {}_2F_1(a)_q$.

Distributions of ${}_2F_1(a)_q$.

Theorem (Ono-S-Saikia)

If $-2 \leq b < c \leq 2$, and r is a fixed positive integer, then

$$\lim_{p \to \infty} \frac{\#\left\{a \in \mathbb{F}_{p^r} \ : \ \sqrt{p^r} \cdot {}_2F_1(a)_{p^r} \in [b, c]\right\}}{p^r} = \frac{1}{2\pi} \int_b^c \sqrt{4 - t^2} dt.$$

In other words, the limiting distribution is **semicircular**.

Deducing distributions

1. We have that

$$q^{\frac{1}{2}-n^2} a_{\mathrm{L},n}(a;q) = -\phi_q(-1) q^{\frac{1}{2}} {}_2F_1(a)_q + O_{r,n}(q^{-\frac{1}{2}}).$$

Deducing distributions

1. We have that
$$q^{\frac{1}{2}-n^2} a_{\mathrm{L},n}(a;q) = -\phi_q(-1) q^{\frac{1}{2}} {}_2F_1(a)_q + O_{r,n}(q^{-\frac{1}{2}}).$$

2. If m is a nonnegative integer, the moments are then
$$\frac{1}{q} \sum_{a \in \mathbb{F}_q \setminus \{0,1\}} \left(q^{\frac{1}{2}-n^2} a_{\mathrm{L},n}(a;q)\right)^m = \frac{1}{q} \sum_{a \in \mathbb{F}_q \setminus \{0,1\}} \left(-\phi_q(-1) q^{\frac{1}{2}} {}_2F_1(a)_q\right)^m + o(1).$$

DEDUCING DISTRIBUTIONS

1. We have that

$$q^{\frac{1}{2}-n^2} a_{\mathrm{L},n}(a;q) = -\phi_q(-1) q^{\frac{1}{2}} {}_2F_1(a)_q + O_{r,n}(q^{-\frac{1}{2}}).$$

2. If m is a nonnegative integer, the moments are then

$$\frac{1}{q} \sum_{a \in \mathbb{F}_q \setminus \{0,1\}} \left(q^{\frac{1}{2}-n^2} a_{\mathrm{L},n}(a;q)\right)^m = \frac{1}{q} \sum_{a \in \mathbb{F}_q \setminus \{0,1\}} \left(-\phi_q(-1) q^{\frac{1}{2}} {}_2F_1(a)_q\right)^m + o(1).$$

3. Use result for the case $n = 1$.

Zeta series for AOP K3 surfaces

Theorem (Ahlgren, Ono, Penniston, '02)

If $ord_p(a(a+1)) = 0$ and $\gamma = \phi_p(a+1)$, then local zeta-function for the affine part X of X_a is

$$Z_X(T) = \frac{1}{(1-p^2T)(1-\gamma pT)(1-\gamma\pi^2T)(1-\gamma\overline{\pi}^2T)},$$

Zeta series for AOP K3 surfaces

Theorem (Ahlgren, Ono, Penniston, '02)

If $ord_p(a(a+1)) = 0$ *and* $\gamma = \phi_p(a+1)$, *then local zeta-function for the affine part* X *of* X_a *is*

$$Z_X(T) = \frac{1}{(1-p^2T)(1-\gamma pT)(1-\gamma\pi^2T)(1-\gamma\overline{\pi}^2T)},$$

where π *and* $\overline{\pi}$ *are the Frobenius eigenvalues of the Clausen elliptic curve*

Zeta series for AOP K3 surfaces

Theorem (Ahlgren, Ono, Penniston, '02)

If $ord_p(a(a+1)) = 0$ and $\gamma = \phi_p(a+1)$, then local zeta-function for the affine part X of X_a is

$$Z_X(T) = \frac{1}{(1-p^2T)(1-\gamma pT)(1-\gamma\pi^2T)(1-\gamma\overline{\pi}^2T)},$$

where π and $\overline{\pi}$ are the Frobenius eigenvalues of the Clausen elliptic curve

$$E_{\mathrm{Cl}}(a) : y^2 = (x-1)(x^2+a).$$

Zeta series for AOP K3 surfaces

Theorem (Ahlgren, Ono, Penniston, '02)

If $\mathrm{ord}_p(a(a+1)) = 0$ and $\gamma = \phi_p(a+1)$, then local zeta-function for the affine part X of X_a is

$$Z_X(T) = \frac{1}{(1-p^2T)(1-\gamma pT)(1-\gamma\pi^2T)(1-\gamma\overline{\pi}^2T)},$$

where π and $\overline{\pi}$ are the Frobenius eigenvalues of the Clausen elliptic curve

$$E_{\mathrm{Cl}}(a) : y^2 = (x-1)(x^2+a).$$

Remark

The complicated part of $Z_X(T)$ is a symmetric square zeta-function.

Sketch of Proof

1. Write the Cohen-Lenstra zeta series

$$\widehat{Z}_X(T) = \prod_{i,j\geq 1} \frac{1}{(1-q^{2-j}T^i)(1-\gamma q^{1-j}T^i)(1-\gamma\pi^2 q^{-j}T^i)(1-\gamma\overline{\pi}^2 q^{-j}T^i)}.$$

Sketch of Proof

1. Write the Cohen-Lenstra zeta series
$$\widehat{Z}_X(T) = \prod_{i,j\geq 1} \frac{1}{(1-q^{2-j}T^i)(1-\gamma q^{1-j}T^i)(1-\gamma\pi^2 q^{-j}T^i)(1-\gamma\overline{\pi}^2 q^{-j}T^i)}.$$

2. Expand the product of each factor as a series in T.

Sketch of Proof

1. Write the Cohen-Lenstra zeta series

$$\widehat{Z}_X(T) = \prod_{i,j\geq 1} \frac{1}{(1-q^{2-j}T^i)(1-\gamma q^{1-j}T^i)(1-\gamma\pi^2 q^{-j}T^i)(1-\gamma\overline{\pi}^2 q^{-j}T^i)}.$$

2. Expand the product of each factor as a series in T.
3. Multiply the resulting series to get the coefficient of T^n.

Sketch of Proof

1. Write the Cohen-Lenstra zeta series

$$\widehat{Z}_X(T) = \prod_{i,j\geq 1} \frac{1}{(1-q^{2-j}T^i)(1-\gamma q^{1-j}T^i)(1-\gamma\pi^2 q^{-j}T^i)(1-\gamma\overline{\pi}^2 q^{-j}T^i)}.$$

2. Expand the product of each factor as a series in T.
3. Multiply the resulting series to get the coefficient of T^n.
4. Use $\pi\overline{\pi} = q$ and

$$\pi^{2k} + \overline{\pi}^{2k} = q^{2k}\phi_q(a+1)^k {}_3F_2\left(\frac{a}{a+1}\right)_{q^k} - q^k.$$

Distribution for AOP K3 surfaces

Theorem (Ono-S-Saikia)

If $-3 \leq b < c \leq 3$, and r is a fixed positive integer, then

$$\lim_{p\to\infty} \frac{\#\left\{a \in \mathbb{F}_{p^r} : p^r \cdot {}_3F_2(a)_{p^r} \in [b, c]\right\}}{p^r} = \frac{1}{4\pi}\int_b^c f(t)dt,$$

Distribution for AOP K3 surfaces

Theorem (Ono-S-Saikia)

If $-3 \leq b < c \leq 3$, *and* r *is a fixed positive integer, then*

$$\lim_{p\to\infty} \frac{\#\left\{a \in \mathbb{F}_{p^r} : p^r \cdot {}_3F_2(a)_{p^r} \in [b, c]\right\}}{p^r} = \frac{1}{4\pi}\int_b^c f(t)dt,$$

where

$$f(t) = \begin{cases} \frac{3-|t|}{\sqrt{3+2|t|-t^2}} & \text{if } 1 < |t| < 3, \\ \frac{3+t}{\sqrt{3-2t-t^2}} + \frac{3-t}{\sqrt{3+2t-t^2}} & \text{if } |t| < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Points of elliptic curves

Theorem (Huang, Ono, S.)

$$\#E_a^{\mathrm{Leg}}(M_n(\mathbb{F}_q)) = \sum_{k=0}^{n} \phi_{q^k}(-1) \cdot P(n,k)_q \cdot {}_2F_1(a)_{q^k},$$

where $P(n,k)_q$ are explicit polynomials in q arising from partitions of n.

Theorem (Huang, Ono, S.)

If we let

$$a_{L,n}(a;q) := \#E_a^{\mathrm{Leg}}(M_n(\mathbb{F}_q)) - P(n,0)_q$$

Points of elliptic curves

Theorem (Huang, Ono, S.)

$$\#E_a^{\mathrm{Leg}}(M_n(\mathbb{F}_q)) = \sum_{k=0}^{n} \phi_{q^k}(-1) \cdot P(n,k)_q \cdot {}_2F_1(a)_{q^k},$$

where $P(n,k)_q$ are explicit polynomials in q arising from partitions of n.

Theorem (Huang, Ono, S.)

If we let

$$a_{L,n}(a;q) := \#E_a^{\mathrm{Leg}}(M_n(\mathbb{F}_q)) - P(n,0)_q$$

and $-2 \leq b < c \leq 2$, then

$$\lim_{p\to\infty} \frac{\#\{a \in \mathbb{F}_q : q^{\frac{1}{2}-n^2} a_{L,n}(a;q) \in [b,c]\}}{q} = \frac{1}{2\pi}\int_b^c \sqrt{4-t^2}\,dt.$$

AOP K3 Surfaces

Theorem (Huang, Ono, S.)

$$\#X_a(M_n(\mathbb{F}_q)) = R(n, \phi_q(a+1))_q + \sum_{k=0}^{n} \phi_{q^k}(-1) \cdot Q(n, k, \phi_{q^k}(a+1))_q \cdot {}_3F_2\left(\frac{a}{a+1}\right)_{q^k},$$

AOP K3 Surfaces

Theorem (Huang, Ono, S.)

$$\#X_a(M_n(\mathbb{F}_q)) = R(n, \phi_q(a+1))_q + \sum_{k=0}^{n} \phi_{q^k}(-1)\cdot Q(n,k,\phi_{q^k}(a+1))_q \cdot {}_3F_2\left(\frac{a}{a+1}\right)_{q^k},$$

where $R(n,\gamma)_q$ and $Q(n,k,\gamma)_q$ are polynomials in q involving partitions of n.

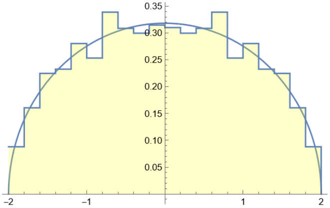
Theorem (Huang, Ono, S.)

$$\lim_{p\to\infty} \frac{\#\{a \in \mathbb{F}_q : q^{1-n^2-n} A_n(a;q) \in [b,c]\}}{q} = \frac{1}{4\pi}\int_b^c f(t)dt,$$

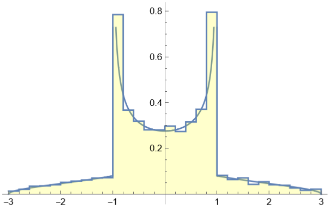
where

$$f(t) = \begin{cases} \frac{3-|t|}{\sqrt{3+2|t|-t^2}} & \text{if } 1 < |t| < 3, \\ \frac{3+t}{\sqrt{3-2t-t^2}} + \frac{3-t}{\sqrt{3+2t-t^2}} & \text{if } |t| < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Histograms



2×2 matrix points on Legendre ECs



2×2 matrix points on AOP $K3$s