Weil's Three Columns & The Cohen-Lenstra Heuristics

Scott Williams

March 4, 2014

From Weil's 1940 Letter:

"The purely algebraic theory of algebraic functions in any *arbitrary* field of constants is not rich enough so that one might draw useful lessons from it. The 'classical' theory (that is, Riemannian) of algebraic functions over the field of constants of the complex numbers is infinitely richer; but on the one had it is too much so, and in the mass of facts some real analogies become lost; and above all, it is too far from the theory of numbers. One would be totally obstructed if there were not a bridge between the two. And just as God defeats the devil: this bridge exists; it is the theory of the field of algebraic functions over a finite field of constants."

– André Weil

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
{Square-free integers}		

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
{Square-free integers}		
1,2,3,5,6,7,10,11,... Infinitely many...		

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{\text{Square-free integers in } [N, 2N]\}$		

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{\text{Square-free integers in } [N, 2N]\}$		
$sf(10) = 7$ $sf(100) = 61$ $sf(1000) = 607$ $sf(10000) = 6077$ $sf(100000) = 60787$		

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{\text{Square-free integers in } [N, 2N]\}$		
$sf(10) = 7$ $sf(100) = 61$ $sf(1000) = 607$ $sf(10000) = 6077$ $sf(100000) = 60787$ $\approx 61\%$		

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{\text{Square-free integers in } [N, 2N]\}$		
$sf(10) = 7$ $sf(100) = 61$ $sf(1000) = 607$ $sf(10000) = 6077$ $sf(100000) = 60787$ $\approx 61\%$		
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$		

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{\text{Square-free integers in } [N, 2N]\}$		
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$		

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$		

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$	

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$	

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$ $= \left(1 - \frac{1}{q}\right) q^n$	

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n$ $\zeta_{\mathbb{F}_q}(s) = \frac{1}{1 - q^{-s}}$ $\zeta_{\mathbb{A}^1/\mathbb{F}_q}(s) = \zeta_{\mathbb{F}_q}(s-1)$	

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n$ $\zeta_{\mathbb{F}_q}(s) = \frac{1}{1 - q^{-s}}$ $\zeta_{\mathbb{A}^1/\mathbb{F}_q}(s) = \zeta_{\mathbb{F}_q}(s-1)$ $\zeta_{\mathbb{A}^1/\mathbb{F}_q}(2) = \frac{q}{q-1}$	

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n$	

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$ $= \left(1 - \frac{1}{q}\right) q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\begin{aligned} \lvert S\rvert &= q^n - q^{n-1} \\ &= \left(1 - \frac{1}{q}\right) q^n \\ &= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n \\ &= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N \end{aligned}$	

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$ $= \left(1 - \frac{1}{q}\right) q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	$\Vert$ Space of unordered n-tuples of distinct points on $\mathbb{C}$

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	$\Vert$ Space of unordered n-tuples of distinct points on $\mathbb{C}$ $\Vert$ $\mathrm{Conf}^n\mathbb{C}$

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	$\Vert$ Space of unordered n-tuples of distinct points on $\mathbb{C}$ $\Vert$ $\mathrm{Conf}^n\mathbb{C}$ $\pi_1(\mathrm{Conf}^n\mathbb{C}) = B_n$ (Artin's Braid Group on n strands)

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\begin{aligned} \lvert S\rvert &= q^n - q^{n-1} \\ &= \left(1 - \frac{1}{q}\right) q^n \\ &= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n \\ &= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N \end{aligned}$	Theorem of Arnol'd: $H^0(B_n, \mathbb{Q}) = H^1(B_n, \mathbb{Q}) = \mathbb{Q}$ $H^i(B_n, \mathbb{Q}) = 0 \quad i > 1$

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	Theorem of Arnol'd: $H^0(B_n, \mathbb{Q}) = H^1(B_n, \mathbb{Q}) = \mathbb{Q}$ $H^i(B_n, \mathbb{Q}) = 0 \quad i > 1$ $\mathrm{Conf}^n\mathbb{C}$ is a scheme over Spec $\mathbb{Z}$ whose $\mathbb{F}_q$-rational points are elements of S

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$ $= \left(1 - \frac{1}{q}\right) q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	Can identify the ℓ-adic cohomology of $\mathrm{Conf}^n/\mathbb{C}$ and $\mathrm{Conf}^n/\mathbb{F}_q$

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$ $= \left(1 - \frac{1}{q}\right) q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	Can identify the ℓ-adic cohomology of $\mathrm{Conf}^n/\mathbb{C}$ and $\mathrm{Conf}^n/\mathbb{F}_q$ $H^0(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^1(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^i(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = 0, \ i > 1$

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$ $= \left(1 - \frac{1}{q}\right) q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	Can identify the ℓ-adic cohomology of $\mathrm{Conf}^n/\mathbb{C}$ and $\mathrm{Conf}^n/\mathbb{F}_q$ $H^0(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^1(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^i(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = 0, \ i > 1$ Lefschetz trace formula $\Downarrow$ $\lvert\mathrm{Conf}^n(\mathbb{F}_q)\rvert = q^n - q^{n-1}$

The Three Columns

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$ $= \left(1 - \frac{1}{q}\right) q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	$H^0(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^1(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^i(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = 0, \ i > 1$ Lefschetz trace formula $\Downarrow$ $\lvert\mathrm{Conf}^n(\mathbb{F}_q)\rvert = q^n - q^{n-1}$

The Three Columns

theorems

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1}$ $= \left(1 - \frac{1}{q}\right) q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n$ $= \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	$H^0(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^1(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^i(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = 0, \ i > 1$ Lefschetz trace formula $\Downarrow$ $\lvert\mathrm{Conf}^n(\mathbb{F}_q)\rvert = q^n - q^{n-1}$

The Three Columns

conjectures ⟵ ⟶ theorems

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	$H^0(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^1(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^i(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = 0, \ i > 1$ Lefschetz trace formula $\Downarrow$ $\lvert\mathrm{Conf}^n(\mathbb{F}_q)\rvert = q^n - q^{n-1}$

The Three Columns

conjectures

theorems

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$ $\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	$H^0(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^1(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ $H^i(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = 0, \ i > 1$ Lefschetz trace formula $\Downarrow$ $\lvert\mathrm{Conf}^n(\mathbb{F}_q)\rvert = q^n - q^{n-1}$

Analytic Number Theory

The Three Columns

conjectures

theorems

$\mathbb{Z}$	$\mathbb{F}_q[T]$	$\mathbb{C}[T]$
$S = \{$Square-free integers in $[N, 2N]\}$	$S = \{$Square-free monic poly. of degree $n\}$	Space of square-free monic poly. of degree n
$\lvert S\rvert = \zeta(2)^{-1}N + O(N^{1/2})$	q^n poly. of degree n $\Rightarrow N = q^n$	$H^0(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$
	$\lvert S\rvert = q^n - q^{n-1} = \left(1 - \frac{1}{q}\right) q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} q^n = \zeta_{\mathbb{A}^1/\mathbb{F}_q}(2)^{-1} N$	$H^1(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$
		$H^i(\mathrm{Conf}^n/\mathbb{F}_q, \mathbb{Q}_\ell) = 0, \ i > 1$
		Lefschetz trace formula $\Downarrow$ $\lvert\mathrm{Conf}^n(\mathbb{F}_q)\rvert = q^n - q^{n-1}$

Analytic Number Theory

Algebraic Geometry

The Cohen-Lenstra Heuristics

The Cohen-Lenstra Heuristics are a family of conjectures concerning the distribution of class groups of quadratic number fields among all finite abelian groups.

The Cohen-Lenstra Heuristics

The Cohen-Lenstra Heuristics are a family of conjectures concerning the distribution of class groups of quadratic number fields among all finite abelian groups.

When K is an imaginary quadratic field Cohen and Lenstra predict: For every odd prime p:

1. The probability that $|\mathrm{Cl}(K)|$ is not a multiple of p is $(1-\frac{1}{p})(1-\frac{1}{p^2})(1-\frac{1}{p^3})\cdots$.
2. The number of elements of exact order p in $\mathrm{Cl}(K)$ is, on average, 1.

The Cohen-Lenstra Heuristics

The Cohen-Lenstra Heuristics are a family of conjectures concerning the distribution of class groups of quadratic number fields among all finite abelian groups.

When K is an imaginary quadratic field Cohen and Lenstra predict: For every odd prime p:

1. The probability that $|\mathrm{Cl}(K)|$ is not a multiple of p is $(1-\frac{1}{p})(1-\frac{1}{p^2})(1-\frac{1}{p^3})\cdots$.
2. The number of elements of exact order p in $\mathrm{Cl}(K)$ is, on average, 1.

1. is not known in any case
2. is only only for $p = 3$ (Davenport-Heilbronn)

Analogies in the Columns

What is the analogy of (2) over $k(t)$ where $k = \mathbb{F}_q$ or $\mathbb{C}$?

Analogies in the Columns

What is the analogy of ❷ over $k(t)$ where $k = \mathbb{F}_q$ or $\mathbb{C}$?

Question ($\mathbb{Q}$): What is the average size of $\mathrm{Cl}(K)/p\,\mathrm{Cl}(K)$ as K ranges over all imaginary quadratic fields with $N < \mathrm{disc}(K) < 2N$? Is it asymptotically of the form aN for some constant a?

Analogies in the Columns

What is the analogy of ❷ over $k(t)$ where $k = \mathbb{F}_q$ or $\mathbb{C}$?

Question ($\mathbb{Q}$): What is the average size of $\mathrm{Cl}(K)/p\,\mathrm{Cl}(K)$ as K ranges over all imaginary quadratic fields with $N < \mathrm{disc}(K) < 2N$? Is it asymptotically of the form aN for some constant a?

Class field theory $\Rightarrow$ a surjection from $\mathrm{Cl}(K)$ to $\mathbb{Z}/p\mathbb{Z}$ is naturally identified with an unramified $\mathbb{Z}/p\mathbb{Z}$-extension, L/K, which is a quadratic extension of $\mathbb{Q}$.

The Galois group G of $L/\mathbb{Q}$ is dihedral of order $2p$.

Analogies in the Columns

Question ($\mathbb{Q}$-2): How many G-extensions of $\mathbb{Q}$ are there with discriminant between N^p and $(2N)^p$? Is it asymptotically of the form aN for some constant a?

Analogies in the Columns

Question ($\mathbb{Q}$-2): How many G-extensions of $\mathbb{Q}$ are there with discriminant between N^p and $(2N)^p$? Is it asymptotically of the form aN for some constant a?

We now use the fact that $k(t)$ isn't just a field; it's the function field of the curve $\mathbb{P}^1/k$ and we have:

$$\{G\text{-extensions of } k(t)\} \longleftrightarrow \{\text{Branched } G\text{-covers of } \mathbb{P}^1\}$$

Branch points for which the monodromy action is the conjugacy class of an involution will be called **simple**.

Analogies in the Columns

Question ($\mathbb{Q}$-2): How many G-extensions of $\mathbb{Q}$ are there with discriminant between N^p and $(2N)^p$? Is it asymptotically of the form aN for some constant a?

We now use the fact that $k(t)$ isn't just a field; it's the function field of the curve $\mathbb{P}^1/k$ and we have:

$$\{G\text{-extensions of } k(t)\} \longleftrightarrow \{\text{Branched } G\text{-covers of } \mathbb{P}^1\}$$

Branch points for which the monodromy action is the conjugacy class of an involution will be called **simple**.

When $k = \mathbb{F}_q$ (q prime to $2p$) a G-cover with n simple branch points has discriminant q^{np}.

Analogies in the Columns

Question ($\mathbb{F}_q(t)$-1): How many G-covers of $\mathbb{P}^1/\mathbb{F}_q$ are there with n simple branch points? Is it asymptotically of the form aq^n for some constant a?

Analogies in the Columns

Question ($\mathbb{F}_q(t)$-1): How many G-covers of $\mathbb{P}^1/\mathbb{F}_q$ are there with n simple branch points? Is it asymptotically of the form aq^n for some constant a?

$$\begin{aligned} \text{Hurwitz Space} &= \mathsf{Hur}^c_{G,n} \\ &= \text{moduli space for } G\text{-covers of } \mathbb{P}^1 \\ &\quad \text{with } n \text{ simple branch points} \end{aligned}$$

Analogies in the Columns

Question ($\mathbb{F}_q(t)$-1): How many G-covers of $\mathbb{P}^1/\mathbb{F}_q$ are there with n simple branch points? Is it asymptotically of the form aq^n for some constant a?

$$\begin{aligned} \text{Hurwitz Space} &= \text{Hur}^c_{G,n} \\ &= \text{moduli space for } G\text{-covers of } \mathbb{P}^1 \\ &\quad \text{with } n \text{ simple branch points} \end{aligned}$$

Question ($\mathbb{F}_q(t)$-2): How many points does $\text{Hur}^c_{G,n}$ have over $\mathbb{F}_q$? Is it asymptotically of the form aq^n for some constant a?

Analogies in the Columns

Question ($\mathbb{F}_q(t)$-1): How many G-covers of $\mathbb{P}^1/\mathbb{F}_q$ are there with n simple branch points? Is it asymptotically of the form aq^n for some constant a?

$$\begin{aligned} \text{Hurwitz Space} &= \text{Hur}^c_{G,n} \\ &= \text{moduli space for } G\text{-covers of } \mathbb{P}^1 \\ &\quad \text{with } n \text{ simple branch points} \end{aligned}$$

Question ($\mathbb{F}_q(t)$-2): How many points does $\text{Hur}^c_{G,n}$ have over $\mathbb{F}_q$? Is it asymptotically of the form aq^n for some constant a?

Answer provided by the Weil conjectures when $q \to \infty$ and n is fixed – a is the number of connected components of $\text{Hur}^c_{G,n}$. However, for us, q is fixed!

Analogies in the Columns

Question ($\mathbb{F}_q(t)$-1): How many G-covers of $\mathbb{P}^1/\mathbb{F}_q$ are there with n simple branch points? Is it asymptotically of the form aq^n for some constant a?

$$\begin{aligned} \text{Hurwitz Space} &= \text{Hur}^c_{G,n} \\ &= \text{moduli space for } G\text{-covers of } \mathbb{P}^1 \\ &\quad \text{with } n \text{ simple branch points} \end{aligned}$$

Question ($\mathbb{F}_q(t)$-2): How many points does $\text{Hur}^c_{G,n}$ have over $\mathbb{F}_q$? Is it asymptotically of the form aq^n for some constant a?

Answer provided by the Weil conjectures when $q \to \infty$ and n is fixed – a is the number of connected components of $\text{Hur}^c_{G,n}$. However, for us, q is fixed!

Question ($\mathbb{C}(t)$): What is the cohomology of $\text{Hur}^c_{G,n}$?

Analogies in the Columns

The study of the cohomology of $\mathrm{Hur}^{c}_{G,n}$ is a topological question about the cohomology of a certain finite index subgroup of the braid group.

Analogies in the Columns

The study of the cohomology of $\mathrm{Hur}^c_{G,n}$ is a topological question about the cohomology of a certain finite index subgroup of the braid group.

Theorem (Ellenberg, Venkatesh, Westerland, 2009)

The cohomology of Hurwitz spaces is stable, i.e., for some positive real numbers A, B and positive integer D the natural map

$$\mathrm{Hur}^c_{G,n} \longrightarrow \mathrm{Hur}^c_{G,n+D}$$

induces an isomorphism in homology

$$H_p(\mathrm{Hur}^c_{G,n}) \longrightarrow H_p(\mathrm{Hur}^c_{G,n+D})$$

for all $p < An + B$.

Analogies in the Columns

The previous theorem implies something close to a positive answer for the $\mathbb{F}_q(t)$ version of our Question. It doesn't quite give the existence of the desired limit a, but it does give the existence of a lim inf and a lim sup, which approach a as q gets large.

Some Analogues

Arithmetic Problem	**Moduli Space**
Counting square-frees	Configuration space of unordered points
Cohen-Lenstra for p-torsion in class group	Moduli of hyperelliptic curves with p-level structure
Counting degree-d number fields	Classical Hurwitz spaces of d-gonal curves
Variation of Selmer groups	Moduli spaces of elliptic surfaces
Batyrev-Manin conjecture	Spaces of rational curves on Fano varieties
Prime number theorem	Representation stability for configuration space of ordered points

Questions?

Questions?

Thank you!