2014 Arizona Winter School

March 15–19, 2014

Contents

1 Curves and zeta functions over finite fields

1.1 Motivating results

The biggest influence here is philosophy of Katz and Sarnak that statistics for zeros of L-functions should match the corresponding statistics for eigenvaluges of large random matrices. The main work of Katz and Sarnak here is [KS99].

Let's start with work of Montgomery from 1974. We assume the Riemann hypothesis, so that we can look at the set of $t \in \mathbf{R}$ such that $\zeta(\frac{1}{2} + it) = 0$. Let

$$N(T) = \#\{0 < t < T : \zeta(\frac{1}{2} + it)0\} \sim \frac{T \log T}{2\pi}.$$

For $\zeta(\frac{1}{2} + i\gamma) = 0$, put $\widetilde{\gamma} = \frac{\gamma \log \gamma}{2\pi}$. The *pair correlation* is

$$\frac{1}{N(T)} \sum_{0<\gamma,\gamma'<T} f(\widetilde{\gamma}' - \widetilde{\gamma}).$$

Theorem 1.1.1.

$$\frac{1}{N(T)} \sum_{0<\gamma,\gamma'<t} f(\widetilde{\gamma} - \widetilde{\gamma}') \to \int_{\mathbf{R}} f(x) \left(1 = \frac{\sin^2(\pi x)}{(\pi x)^2}\right) dx$$

for some test function f such that $\operatorname{supp}(\widehat{f}) \subset (-\delta, \delta)$.

Let $\mathrm{U}(N)$ be the group of $N \times N$ unitary matrices, i.e. U with $U^*U = UU^* = 1_N$. Any such matrix has eigenvalues $\lambda_j(U) = e^{i\theta_j(U)}$ for $i = 1, \ldots, N$. Put

$$C_f(U) = \sum_{1 \leqslant k < j \leqslant N} f\left(\frac{N}{2\pi}\theta_j - \frac{N}{2\pi}\theta_k\right).$$

Theorem 1.1.2.

$$\int_{\mathrm{U}(N)} C_f(U)\, dU \to \int_{-\infty}^{\infty} f(x) \left(1 - \frac{\sin^2(\pi x)}{(\pi x)^2}\right) dx.$$

The function $1 - \frac{\sin^2(\pi x)}{(\pi x)^2}$ appearing in this theorem is called the *scaling limit*.

There is numerical evidence – it has been checked up to 10^{20}. There are generalizations to zeros of automorphic representations of $GL(n)$ due to Rudrick and Sarnak. Finally, this was proven over function fields when $q \to \infty$.

1.2 One-level densities

Another statistic is the *one-level density*, which is the study of the "low lying zeros." Here you study these zeros for a family of L-functions. Our main examples come from families of elliptic curves over $\mathbf{Q}$, or families of L-functions attached to quadratic Dirichlet characters.

Chantal David

Define

$$W_f(E) = \sum_{L(1+i\gamma_E,E)=0} f\left(\frac{\gamma_E \log N_E}{2\pi} 2\pi\right).$$

for f a function in the Schwarz space. Let the *completed L-function of E* to be

$$\Lambda(s,E) = \left(\frac{\sqrt{N_E}}{2\pi}\right)^2 \Gamma(s)L(s,E) = \Lambda(2-s,E).$$

The *one-level density* is

$$\langle W_f(E)\rangle_{\mathscr{F}(X)} = \frac{1}{\#\mathscr{F}(X)} \sum_{E\in\mathscr{F}(X)} W_f(E)$$

where $\mathscr{F}(X)$ is a family of elliptic curves with conductor $\sim X$.

Conjecture 1.2.1 (Katz-Sarnak)**.**

$$\langle W_f(E)\rangle_{\mathscr{F}(X)} \to \int_{\mathbf{R}} f(x) W_G(x)\, dx,$$

where $W_G(x)$ depends on the "symmetry type" of the family.

Consider the following table for $W_g(x)$:

1	U unitary
$1 - \frac{\sin(\pi x)}{2\pi x}$	USp symplectic
$1 + \frac{1}{2}\delta_0(x)$	O orthogonal
$1 + delta_0(x) - \frac{\sin(\pi x)}{2\pi x}$	SO odd-dimensional
$1 + \frac{\sin(2\pi x)}{2\pi x}$	SO even-dimensional

These are the scaling densities for the one level density on the matrix groups.

Theorem 1.2.2.

$$\int_{O(N)} W_f(U)\, dU \to \int_{\mathbf{R}} f(x)\left(1 + \frac{1}{2}\delta_0(x)\right) dx = \widehat{f}(0) + \frac{1}{2}f(0).$$

The Fourier transforms of O and SO agree for $|U| < 1$.

Try the family $y^2 = x^3 + ax + b$ of elliptic curves, where $|a| \leqslant X^{1/3}$ and $b \leqslant X^{1/2}$, i.e. such that $\Delta_E \asymp X$. There is an explicit formula due to Weil.

$$\sum_{\gamma_E} f\left(\frac{\gamma_E \log N_E}{2\pi}\right) = \widehat{f}(0) + \frac{1}{2}f(0) - \sum_p \frac{2\log p}{p\log N_E} \widehat{f}\left(\frac{\log p}{\log N_E}\right) a_p(E) + O\left(\frac{\log\log N_E}{\log N_E}\right)$$

This comes from the integral

$$\int_{(2+\varepsilon)} \frac{\Lambda'}{\Lambda}(s) h(s)\, ds.$$

Recall that we have $\Lambda(s,E) = \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \Gamma(s)L(s,E)$. There is a sum

$$\frac{L'}{L}(s) = \sum_{p,k} \frac{\alpha_p^k + \overline{\alpha}_p^k}{kp^{ks}} p^s,$$

where $\alpha_p^2 + \overline{\alpha}_p^2 = a_p^2 - 2p$. Then

$$\langle W_f(E)\rangle_{\mathscr{F}(X)} = \widehat{f}(0) + \frac{1}{2}f(0) + \frac{2}{\log X}\sum_{p\leqslant X^\delta}\frac{\log p}{p}\sum_{E\in\mathscr{F}(X)}a_p$$

provided $\widehat{f}$ has support in $(-\delta,\delta)$.

Theorem 1.2.3 (Young). $\langle W_f(E)\rangle_{\mathscr{F}(X)} = \widehat{f}(0) + \frac{1}{2}f(0)$, *for* $\operatorname{supp}(\widehat{f}) \subset (-\frac{7}{9},\frac{7}{9})$.

This confirms "O symmetries" (well also, SO would also work).

Corollary 1.2.4. *The average analytic rank is at most* $\frac{1}{2}+\frac{9}{7} = \frac{25}{14} < 2$.

Example 1.2.5. In this example, the symmetry type is not clear a priori. Let

$$E_t : y^2 = x^3 + tx^2 - (t+3)x + 1 \qquad t \in \mathbf{Z}.$$

This is due to Washington-Rizzo. This family has rank one over $\mathbf{Q}(t)$. Also, $W(E_t) = -1$ for all $t \in \mathbf{Z}$.

Theorem 1.2.6 (Miller). *Let* $\mathscr{F}(X) = \{E_t : t \sim X^{1/4}\}$. *Then*

$$\langle W_f(E_t)\rangle_{\mathscr{F}(X)} \sim \widehat{f}(0) + \frac{3}{2}f(0)$$

for $\operatorname{supp}(\widehat{f}) \subset (-\frac{1}{3},\frac{1}{3})$.

This agrees with $W(x) = \delta_0(X) + \mathrm{SO}(\mathrm{odd})$.

Theorem 1.2.7 (Huyhn-Parks-David). *Assume the ratio conjectures. Then*

$$\langle W_f(E_t)\rangle_{\mathscr{F}(X)} \sim \int_{-\infty}^{\infty} f(x)\left(\delta_0(x) + 1 + \frac{\sin(2\pi x)}{2\pi x}\right)dx$$

i.e. $W(x) = \delta_0(x) + \mathrm{SO}(\mathit{even})(x)$.

Example 1.2.8. Consider $L(s,\chi_d)$, where $\chi_d = \left(\frac{d}{n}\right)$, where $d \sim X$ is a fundamental discriminant.

Theorem 1.2.9 (Sarnak, Ozlek Snyder).

$$\langle W_f(d)\rangle_{D(X)} = \int_{\mathbf{R}} f(x)\left(1 - \frac{\sin(2\pi x)}{2\pi x}\right)dx$$

when $\operatorname{supp}(f) \subset (-2,2)$.

These are symplectic symmetries. We would like to compute the n-level densities for this same family.

Theorem 1.2.10 (Rubenstein).

$$\langle W_f^{(n)}(d)\rangle_{D(X)} \to \int_{\mathbf{R}^n} f(x_1,\dots,x_n)W^{(n)}(x_1,\dots,x_n)dx_1,\dots,x_n.$$

when $\widehat{f}(u_1,\dots,u_n)$ *has support contained in* $\{\sum|u_i| < 1\}$.

Try to extend this to $\sum|u_i| < 2$. There is a theorem of Gao (for $n = 3,4$) and Miller (for $n = 5,6$) that

$$\langle W_f^{(n)}(d)\rangle_{D(X)} = A(f) + o(1).$$

Theorem 1.2.11. *This was proven for all n by Entin-Roddity-Gershon-Rudnick, using hyperelliptic curves (i.e. the Katz-Sarnak equidistribution theorem).*

1.3 L-functions over function fields

Consider the following list of analogies between number fields and function fields.

number fields	function fields
$\mathbf{Q}$	$k = \mathbf{F}_q(T)$
$\mathbf{Z}$	$A = \mathbf{F}_q[T]$
p prime	$P(T)$ irreducible monic
$\lvert n\rvert$	$q^{\deg F}$

The "Riemann zeta function" over $\mathbf{F}_q(T)$ is

$$\begin{aligned}\sum_F \frac{1}{|F|^s} &= \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1} \\ &= \sum_{d=0}^{\infty} \frac{q^d}{q^{ds}} \\ &= \sum_{d=0}^{\infty} (q^{1-s})^d \\ &= \frac{1}{1-q^{1-s}}\end{aligned}$$

So the "Riemann hypothesis" holds for $\mathbf{F}_q(T)$. We would like to use this to prove the "Prime Number Theorem" for $\mathbf{F}_q[T]$. Let a_d be the number of prime polynomials P of degree d. Put

$$\zeta_q(s) = \prod_{d=1}^{\infty} \left(1 - \frac{1}{q^{ds}}\right)^{-a_d} = \frac{1}{1-q^{1-s}}.$$

Make the substitution $u = q^{-s}$, and we get

$$\prod_{d=1}^{\infty} \left(1 - \frac{1}{u^d}\right)^{-a_d} = \frac{1}{1-qu}.$$

We can take the logarithmic derivative, and get

$$u \sum_{d=1}^{\infty} a_d \frac{d}{du} \log(1-u^d) = u \frac{d}{du} \log(1-qu).$$

This tells us that

$$\sum_{d=1}^{\infty} \frac{a_d d u^d}{1-u^d} = \frac{qu}{1-qu}.$$

Writing the geometric series,

$$\sum_{d=1}^{\infty} d a_d \sum_{n=1}^{\infty} u^{dn} = \sum_{d=1}^{\infty} (qu)^d.$$

We can equate the coefficients of powers of u, to obtain

$$q^d = \sum_{n|d} n a_n$$

Using Möbius inversion, we get

$$a_n = \frac{1}{n}\sum_{d|n}\mu(d)u^{n/d}.$$

This yields the Prime Number Theorem for function fields:

Theorem 1.3.1. $a_n = \frac{q^n}{n} + o(\frac{q^{n/2}}{n} + \frac{q^{n/3}}{n}\sum_{d|n}\ldots)$.

Let $\#\mathscr{F}_d$ be the number of square-free polynomials of degree d.

Lemma 1.3.2. *We have*

$$\#\mathscr{F}_d = \begin{cases} q^d - q^{d-1} = \frac{q^d}{\zeta_q(2)} & d \geqslant 2 \\ q^d & d = 0, 1 \end{cases}$$

Proof. Note that $\zeta_q(s) = \zeta_q(2s)\sum_{n=1}^{\infty}(\#\mathscr{F}_d)q^{-ds}$. □

Let K be a general function field, i.e. a finite extension of $k = \mathbf{F}_q(T)$. For example, we could have $K = k(\sqrt[\ell]{D(T)})$ for some irreducible $D \in \mathbf{F}_q[T]$. Let $\mathcal{P}_K$ be the set of primes of K. If $P \in \mathcal{P}_K$ has valuation ring R, we put $|P| = \#(R/P)$.

If $k = \mathbf{F}_q(T)$, then $\mathcal{P}_k$ is the set of irreducible polynomials in $\mathbf{F}_q[T]$, together with ∞ coming from the valuation ring $\mathbf{F}_q[\frac{1}{T}]$. Let $\mathcal{D}_k$ be the free abelian group on $\mathcal{P}_k$; we call $\mathcal{D}_k$ the *divisor group* of k. If $D = \sum a_P(P)$ is a divisor over k, define $\deg D = \sum a_P \deg P$, $|D| = q^{\deg D}$. We have $|D_1 + D_2| = |D_1| \cdot |D_2|$. Let $\mathcal{D}_k^+$ be the set of effective divisors ($D = \sum a_p(P)$ with $a_P \geqslant 0$ for all P). We define

$$\zeta_k(s) = \sum_{D\in\mathcal{D}_k^+}|D|^{-s} = \prod_{P\in\mathcal{P}_k}\left(1 - \frac{1}{|P|^s}\right)^{-1}.$$

Example 1.3.3. We have

$$\zeta_{\mathbf{F}_q(x)}(s) = \prod_{P\subset\mathbf{F}_q[x]}\left(1 - \frac{1}{|P|^s}\right)^{-1}\prod_{P=\infty}\left(1 - \frac{1}{q^s}\right)^{-1} = \frac{1}{(1-q^{1-s})(1-q^{-s})}.$$

Example 1.3.4. Let $K = \mathbf{F}_q(x)(\sqrt{D})$, where D is irreducible. Then

$$\frac{\zeta_K(s)}{\zeta_k(s)} = \prod_{\substack{P\in S_k \\ P \text{ inert in } k}}\frac{(1-|P|^{-2s})^{-1}}{(1-|P|^{-s})^{-1}}\prod_{\substack{P\in S_K \\ P \text{ splits in } K}}\frac{(1-|P|^{-s})^{-2}}{(1-|P|^{-s})^{-1}}$$

Write

$$\frac{\zeta_K(s)}{\zeta_k(s)} = \prod_{P\in S_k}(1-\chi_K(P)|P|^{-s})^{-1},$$

where

$$\chi_K(P) = \begin{cases} 1 & P \text{ splits} \\ -1 & P \text{ inert} \\ 0 & P \text{ ramifies} \end{cases}$$

We are looking at $y^2 - D(x) \mod P$, and putting $\chi_K(P) = \left(\frac{D}{P}\right)$, the Dirichet character modulo D. Thus

$$\frac{\zeta_K(s)}{\zeta_k(s)} = L(s, \chi_D)(1 - q^{-s})^{-\lambda_D}$$

where $\lambda_D = 1$ if $\deg D$ is even, and 0 if $\deg D$ is odd.

Theorem 1.3.5. *Let χ be a non-trivial Dirichlet character to the modulos $\mathfrak{m}$. Then $L(s,\chi) = \sum_F \frac{\chi(F)}{|F|^s}$ is a polynomial in q^{-s} of degree at most $\deg \mathfrak{m} - 1$.*

Proof. Write $L(s,\chi) = \sum_{n=0}^{\infty} A(n,\chi) q^{-ns}$, where $A(n,\chi) = \sum_{\deg F = n} \chi(n)$. If $n \geqslant \deg \mathfrak{m}$, then each residue class modulo $\mathfrak{m}$ is represented exactly $q^{n - \deg \mathfrak{m}}$ times. So

$$A(n,\chi) = q^{n-\deg \mathfrak{m}} \sum_{r \mod \mathfrak{m}} \chi(r) = 0.$$

□

This works in general.

Theorem 1.3.6. *Let $\zeta_k(s) = \frac{P_k(qs)}{(1-q^{-s})(1-q^{1-s})}$. Then P_k is a polynomial of degree at most $2g$ in q^{-s}.*

Proof. Use the Riemann-Roch theorem. Let $b_n(k)$ be the number of effective divisors of degree n. By the Riemann-Roch theorem, for $n > 2g - 2$, we have

$$b_n(k) = h_k \frac{q^{n-g+1} - 1}{q - 1}$$

so consider

$$Z_k(u) = \sum_{n=1}^{\infty} b_n u^n$$

and use the previous formula. We have $Z_k(u) = \frac{P_k(u)}{(1-u)(1-qu)}$. Let's look at the zeros of $P_k(u)$, so write $P_k(u) = \prod_{i=1}^{2g}(1 - u\alpha_j(k))$. If $\zeta_k(s) = 0$, then $q^{-s} = \alpha_j(k)^{-1}$ for some j. So the Riemann Hypothesis tells us that $\zeta_k(s) = 0$ iff $s = 1/2$¡ i.e. iff $|\alpha_j(k)| = \sqrt{q}$. □

Theorem 1.3.7 (Weil, Stephanov-Bombieri)**.** *The zetos of $\zeta_k(s)$ have $\Re(s) = \frac{1}{2}$, i.e. $|\alpha_j(k)| = \sqrt{q}$.*

Corollary 1.3.8. *If we let $a_n(k) = \#\{P \in S_k \text{ of degree } N\} = \frac{q^N}{N} + O(q^{N/2})$.*

There is another formulation for $Z_k(u)$. Recall that $-\log(1-u) = \sum_{n=1}^{\infty} \frac{u^n}{n}$. We compute

$$\begin{aligned}
\log Z_k(u) &= \log \prod_{d=1}^{\infty} (1 - u^d)^{-a_d(k)} \\
&= \sum_{d,m} a_d(k) \frac{u^{d_m}}{m} \\
&= \sum_{n=1}^{\infty} N_n(k) \frac{u^n}{n}
\end{aligned}$$

where $N_n(k) = \sum_{d|n} d a_d(k)$. Moreover,

$$\log Z_k(u) = \log\left(\frac{P_k(u)}{(1-u)(1-qu)}\right) = \sum \frac{u^n}{n} + \sum \frac{(qu)^n}{n} - \sum_{j=1}^{2g}\sum_n \frac{\alpha_j(C)^n}{n}u^n.$$

We can equate coefficients to get that $N_n(k)$ is the number of primes of degree 1 in $\mathbf{F}_{q^n}k$. Even better, $N_n(k) = q^n + 1 - \sum_{j=1}^{2g}\alpha_j(C)^n$. To relate this to Jordan's talks, we need to relate function fields with curves.

function fields $\mathbf{F}_q(C) = dF_q[x,y]/(F)$	curves over $\mathbf{F}_q$, given by $F(x,y) = 0$
$\mathbf{F}_q(\sqrt{D})$	$y^2 = D(x)$
primes in $\mathbf{F}_q(C)$	Galois orbits of points on $C(\overline{\mathbf{F}}_q)$
primes of degree one	points in $C(\mathbf{F}_q)$
primes of degree one in $\mathbf{F}_{q^n}k$	points in $C(\mathbf{F}_{q^n})$

So

$$Z_k(u) = \exp\left(\sum_{n=1}^{\infty} \#C(\mathbf{F}_{q^n})\frac{u^n}{n}\right) = Z_C(u).$$

So instead of talking about zeta functions of function fields, we will talk about zeta functions of curves.

Recall the following theorem of Weil.

Theorem 1.3.9 (Weil)**.** *Let C be a smooth projective curve of genus g over $\mathbf{F}_q$, and let $Z_C(u) = \exp\left(\sum_n \#C(\mathbf{F}_{q^n})\frac{u^n}{n}\right)$. Then*

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)},$$

where $P_C(u) \in \mathbf{Z}[u]$ has degree $2g$. Moreover, if we write $P_C(u) = \prod_j(1-u\alpha_j(C))$, then $|\alpha_j(C)| = \sqrt{q}$.

So taking logarithmic derivatives, we get

$$\#C(\mathbf{F}_{q^n}) - (q^n+1) = -\sum_{j=1}^{2g}\alpha_j(C),$$

so statistics of the zeros give statistics on the number of points. Of course, we get the famous Weil bound:

$$|\#C(\mathbf{F}_{q^n}) - (q^n+1)| \leqslant 2g\sqrt{q}^n.$$

Let's introduce some notation. Let θ_C be the $2g \times 2g$ matrix with diagonal entries $e^{i\theta_j(C)}$, where $\alpha_j(C) = \sqrt{q}e^{i\theta_j(C)}$. We want to study the distribution of the zeros when C varies over a family of curves of genus g over $\mathbf{F}_q$. Let $\mathscr{F}(g,q)$ be such a family.

Theorem 1.3.10 (Deligne)**.** *Let $\mathcal{M}_g(\mathbf{F}_q)$ be the moduli space of curves of genus g over $\mathbf{F}_q$. Let f be any class function on $\mathrm{USp}(2g)$ (which is the monodromy group of the family). Then*

$$\lim_{q\to\infty}\frac{1}{\#\mathcal{M}_g(\mathbf{F}_q)}\sum_{C\in\mathcal{M}_g(\mathbf{F}_q)} f(\theta_C) = \int_{\mathrm{USp}(2g)} f(U)\,dU.$$

This is one of the key ingredients of Katz-Sarnak's proof of Montgomery's pair-correlation conjecture over function fields.

What if we fix q and let $g \to \infty$. What statistics do we get? The first work in this direction was due to Kurlberg-Rudnick on hyperelliptic curves. Let $\mathcal{H}_g(\mathbf{F}_q)$ be the moduli space of hyperelliptic curves over $\mathbf{F}_q$. Such a curve is $y^2 = F(x)$, where $F(x)$ is square-free. The genus is $g = \left\lfloor \frac{d-1}{2} \right\rfloor$, where $d = \deg F$. We ware interested in

$$\lim_{g\to\infty} \frac{\#\{C \in \mathcal{H}_g(\mathbf{F}_q) : \#C(\mathbf{F}_q) = m\}}{\#\{C \in \mathcal{H}_g(\mathbf{F}_q)\}} \sim \text{Prob}\left(\sum_{i=1}^{q+1} X_i = m\right),$$

where the X_i are independent and identically distributed random variables such that

$$X_i = \begin{cases} 0 & \text{probability } \frac{q}{2(q+1)} \\ 1 & \text{probability } \frac{1}{q+1} \\ 2 & \text{probability } \frac{q}{2(q+1)} \end{cases}$$

At the end, this depends on $\text{Prob}(F(a) = 0)$ for $a \in \mathbf{F}_q$. This is just

$$\frac{\#\{F \in \mathscr{F}_d : F(a) = 0\}}{\#\mathscr{F}_d} = \frac{1}{q+1}$$

where $\mathscr{F}_d$ is the set of square-free monic polynomials of degree d. Note that $\frac{1}{q+1} = \frac{1-q}{q^2-1}$. We have that

$$\#C(\mathbf{F}_q) = \sum_{a\in\mathbf{P}^1(\mathbf{F}_q)} (1 + \chi_2(F(a))) = q + 1 + \sum_{a\in\mathbf{P}^1(\mathbf{F}_q)} \chi_2(F(a)).$$

To get the distribution, we average over this family.

Theorem 1.3.11.

$$\frac{\#\{F \in \mathscr{F}_d : F(a_i) = \alpha_i \text{ for } 1 \leqslant i \leqslant q\}}{\#\mathscr{F}_d} \sim \left(\frac{1}{q+1}\right)^m \left(\frac{q}{(q+1)(q-1)}\right)^{q-m}$$

where m is the number of α_i which are zero.

...stopped taking notes...

2 Geometric analytic number theory

2.1 Analytic number theory

The first order of business is to clarify what is meant by "analytic number theory." We will do this via example.

Question 2.1.1. *How many pairs of integers in $[1, N] \times [1, N]$ are coprime?*

Question 2.1.2. *If X is a projective variety over $\mathbf{Q}$, how many points are there in $X(\mathbf{Q})$ of height at most N?*

If $X = \mathbf{P}^1_{\mathbf{Q}}$, then the first question is seen to be a special case of the second.

Question 2.1.3. *How many primes are there $\leqslant N$?*

Question 2.1.4. *How many totally real cubic fields are there with discriminant $\leqslant N$?*

We can combine the previous two questions.

Question 2.1.5. *How many real totally real cubic fields are there with* prime *discriminant $\leqslant N$?*

Some of these questions could also be said to fall under "arithmetic statistics," or "geometric arithmetic statistics."

Question 2.1.6 (Autocorrelation of Möbius)**.** *Is $\sum_{n \leqslant N} \mu(n)\mu(n+1) = o(N)$?*

This falls under the general framework of the *Chowla conjectures*.

Question 2.1.7. *What is the probability that a quadratic imaginary field $\mathbf{Q}(\sqrt{-d})$ (d chosen randomly in $[N, 2N]$) has class number prime to 7?*

In this question, there is the implicit conjecture that such a probability is well-defined. This falls under the *Cohen-Lenstra heuristics*.

Question 2.1.8. *If n is a random square-free integer in $[N, 2N]$, what is the probability that there exists a totally real quintic field $K/\mathbf{Q}$ with discriminant n?*

The answer is expected to be $e^{-1/120}$.

All of these problems fall under "analytic number theory," or "arithmetic statistics." The main idea is that they can all be fruitfully attacked using the tools of arithmetic geometry (étale cohomology, ...). The phrase "how many" is meant *asymptotically*. For example, in the first question the answer is $6/\pi^2$, but we do *not* mean that $\#\{(x, y) \in [1, N] \times [1, N] \text{ coprime}\} = \frac{6}{\pi^2} N^2$. Rather, we mean that

$$\lim_{N \to \infty} N^{-2} \#\{(x, y) \in [1, N] \times [1, N] \text{ coprime}\} = \frac{6}{\pi^2}.$$

Even better,

$$\#\{(x, y) \text{ coprime in } [1, N] \times [1, N]\} = \frac{6}{\pi^2} N^2 + O(N^{2-\delta})$$

for some $\delta > 0$. This is called a *power-saving error term*. Making δ as large as possible is a big part of analytic number theory.

The work "geometric" in "geometric analytic number theory" should be taken as the same word in "geometric Langlands." We will take geometric analogues of these problems, and attack these problems geometrically.

Jordan Ellenberg

2.2 Number fields and function fields

The following definition is standard.

Definition 2.2.1. *A* global field *is either*

- *a* number field *(i.e. a finite extension of* $\mathbf{Q}$*)*
- *the function field of a curve over a finite field* $\mathbf{F}_q$ *(i.e. a field isomorphic to a finite extension of* $\mathbf{F}_q(t)$*)*

The reason for this slightly complicated definition is that any number field is such in a unique way (i.e. $\mathbf{Q}$ sits inside fields uniquely). On the other hand, function fields contain $\mathbf{F}_q(t)$ in many different (i.e. non-isomorphic) ways. We will be mostly be interested in the function field $\mathbf{F}_q(t)$.

There is a long list of analogies between these two types of fields. See the table in [Poo13]. Think of the fields $\mathbf{Q}$ and $\mathbf{F}_q(t)$. The ring $\mathbf{Z} \subset \mathbf{Q}$ can be defined as

$$\{x \in \mathbf{Q} : |x|_p \leqslant 1 \text{ for all absolute values except } |\cdot|_\infty\}.$$

Similarly, we can "pin down" $\mathbf{F}_q[t]$ as a subring of $\mathbf{F}_q(t)$. For each $x \in \mathbf{F}_q(t)$ and for each point P of $\mathbf{P}^1$, we have an absolute value

$$|x|_P = q^{-v_P(x)}$$

If $P = \infty$, we have $v_\infty(f/g) = \deg g - \deg f$. The analogous definition of $\mathbf{F}_q[t]$ is

$$\begin{aligned}\mathbf{F}_q[t] &= \{x : |x|_P \leqslant 1 \text{ for all } P \text{ except } \infty\} \\ &= \{x : x \text{ has no denominator}\} \\ &= \{x : x \text{ has no poles away from } \infty\} \\ &= \{x : x \text{ is a polynomial } P \text{ with } |x|_\infty = q^{\deg P}\}.\end{aligned}$$

There is a major difference between $\mathbf{Q}$ and $\mathbf{F}_q(t)$. In $\mathbf{Q}$, there is only one archimedean place ∞. In $\mathbf{F}_q(t)$, the valuation ∞ is *not* special – we can apply any automorphism of $\mathbf{P}^1$ to move it around, e.g. arriving at $\mathbf{F}_q\left[\frac{1}{1-t}\right]$.

Over $\mathbf{Q}$, we think of the "positive integers" $\mathbf{N}$ as a set of coset representatives for $\mathbf{Z}/\mathbf{Z}^\times$. Over $\mathbf{F}_q(t)$, we will think of "monic polynomials" as a set of coset representatives for $\mathbf{F}_q[t]/\mathbf{F}_q[t]^\times$. An interval in $\mathbf{Z}$ can be thought of as $\{n : |n - n_0| \leqslant d\}$ for some d. Similarly, an *interval* in $\mathbf{F}_q[t]$ will be a set of the form $\{f : |f - f_0| \leqslant e\}$. Recall that $|f - f_0| = |f - f_0|_\infty = q^{\deg(f-f_0)}$. For example, $\{f : |f - x^n| \leqslant q^{n-1}\}$ is precisely the set of monic polynomials of degree n.

2.3 Square-free integers and square-free polynomials

Question 2.3.1. *How many integers in* $[N, 2N]$ *are squarefree?*

One might expect this probability to be

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{25}\right)\cdots$$

and indeed this is correct. Namely, if we call

$$\mathrm{sf}(N) = \#\{n \in [N, 2N] : n \text{ is square-free}\},$$

then

$$\lim_{N\to\infty} N^{-1}\,\mathrm{sf}(N) = \prod_p (1 - p^{-2}) = \frac{1}{\zeta(2)}.$$

Over $\mathbf{F}_q[t]$, we consider the intervals consisting of monic polynomials of degree n, i.e. polynomials of the form $x^n + a_1 x^{n-1} + \cdots + a_n$. This is an interval of "size" (i.e. cardinality) q^n. (So think of q^n as N.) Let

$$\mathrm{sf}_q(n) = \#\{\text{square-free polynomials in } \mathbf{F}_q[t] \text{ of degree } n\}.$$

It is known that

$$\lim_{n\to\infty} q^{-n}\,\mathrm{sf}_q(n) = 1 - \frac{1}{q}.$$

Contrary to appearances, this is the same as the previous answer. Heuristically, one might have expected

$$\lim_{n\to\infty} q^{-n}\,\mathrm{sf}_q(n) = \prod_{P \text{ irreducible}} (1 - q^{-2\deg P}) = \prod_P (1 - |P|^{-2}) =: \frac{1}{\zeta_{\mathbf{F}_q[t]}(2)}.$$

Here, the miracle is that this giant infinite product defining $\zeta_{\mathbf{F}_q[t]}(2)^{-1}$ collapses to the simple rational number $1 - q^{-1}$. It remains to justify the use of the word "geometric" when talking about function fields.

The above follows from this surprising lemma.

Lemma 2.3.2. *We have* $\mathrm{sf}_q(n) = q^n(1 - \frac{1}{q})$ *for all* $n > 1$.

Proof. Let $\Sigma_{n,e}$ be the number of monic polynomials of degree n of the form $a(t)b^2(t)$, where a is squarefree and $\deg(b) = e$. All q^n polynomials can be factored (uniquely) in this way, so $q^n = \sum_{e=1}^{\lceil n/2 \rceil} \#\Sigma_{n,e}$. We have $\#\Sigma_{n,e} = q^e\,\mathrm{sf}_q(n-2e)$. By induction, starting from $\mathrm{sf}_q(0) = 1$ and $\mathrm{sf}_q(1) = q$, we get the desired result. □

In some ways, this is the "motivic proof" of our result. We'd like to give a more obviously "geometric" proof.

The absence of an error term is misleading. For a general function field $\mathbf{F}_q(C)$, the natural analogue $\mathrm{sf}_C(n) = \zeta_C(2)^{-1} \cdot q^n + \text{error}$, where the error is non-zero. It was worked out in great detail by Byunjchul Cha in 2011.

2.4 Configuration spaces of polynomials

How do you tell whether an integer / polynomial is square-free? In $\mathbf{Z}$, this is somewhat hard. For polynomials in $k[t]$, we compute the discriminant. For example, suppose $P(t) = t^3 + a_1 t^2 + a_2 t + a_3$. The polynomial P is square-free if and only if

$$a_2^2 a_1^2 - 4a_3 a_1^3 - 4a_2^3 + 18a_3 a_2 a_1 - 27a_3^2 \neq 0.$$

In fact, this is $\Delta(P) = \prod_{i \neq j}(\theta_i - \theta_j)$, where the θ_i are the roots of P. Clearly Δ is a polynomial in the θ_i which is fixed under permutations of the θ_i. Thus it follows abstractly that it is a polynomial in the a_i. The same argument works for polynomials of arbitrary degree.

We can construct the *moduli space of square-free polynomials*. This is the open subvariety of $\mathbf{A}^n_{a_1,\ldots,a_n}$ (the "moduli space of monic degree-n polynomials") where Δ does not vanish. Denote this space by Conf^n. In general, $\mathrm{Conf}^n(k)$ is the set of square-free monic polynomials of degree n with coefficients in k. Note that $\mathrm{sf}_q(n) = \#\mathrm{Conf}^n(\mathbf{F}_q)$. We will think of Conf^n as a scheme over $\mathrm{Spec}(\mathbf{Z})$.

Note that $\mathrm{Conf}^n(\mathbf{C})$ is the set of *unordered* n-tuples of *distinct* complex numbers via the isomorphism

$$P \mapsto \{\text{roots of } P\}.$$

We could think of $\mathrm{Conf}^n(\mathbf{C})$ as the "configuration space of n distinct points in $\mathbf{C}$." The set $\mathrm{Conf}^n(\mathbf{C})$ is a manifold, so we can investigate its topology. Note that $\mathrm{Conf}^1(\mathbf{C}) = \mathbf{C}$. The space $\mathrm{Conf}^2(\mathbf{C})$ of unordered pairs of distinct points can be understood as the quotient of the space of *unordered* pairs of distinct points is homotopy-equivalent to S^1. Forgetting the ordering corresponds to quotienting out by the antipodal map, so $\mathrm{Conf}^2(\mathbf{C}) \approx S^1$.

As n grows, the spaces Conf^n get more complicated, e.g. the fundamental group $\pi_1(\mathrm{Conf}^n(\mathbf{C}))$ can be described as follows. A loop in $\mathrm{Conf}^n(\mathbf{C})$ is a way of "moving around" a collection of n distinct points, ending up with the same configuration of n points. These are exactly braids on n points, and composition of loops corresponds to the standard composition of braids. Thus $\pi_1(\mathrm{Conf}^n(\mathbf{C})) \simeq \mathrm{Br}_n$, the Artin braid group on n strands.

Theorem 2.4.1 (Arnol'd)**.** *For all $n > 1$,*

$$\begin{aligned} \mathrm{H}^0(\mathrm{Conf}^n(\mathbf{C}), \mathbf{Q}) &= \mathbf{Q} \\ \mathrm{H}^1(\mathrm{Conf}^n(\mathbf{C}), \mathbf{Q}) &= \mathbf{Q} \\ \mathrm{H}^i(\mathrm{Conf}^n(\mathbf{C}), \mathbf{Q}) &= 0 \qquad (i > 1). \end{aligned}$$

In other words, $\mathrm{H}^\bullet(\mathrm{Conf}^n(\mathbf{C}), \mathbf{Q}) \simeq \mathrm{H}^\bullet(S^1, \mathbf{Q})$. If we allow integral coefficients, things become much more interesting. This theorem can be interpreted as a result in homological stability. The same phenomenon occurs for $\mathcal{M}_g$, the moduli space of genus g curves for $g \gg 0$.

2.5 Étale cohomology of configuration spaces

We'll start with the Grothendieck-Lefschetz trace formula. It says that for any variety X over $\mathbf{F}_q$, we have

$$\#X(\mathbf{F}_q) = \sum_i (-1)^i \,\mathrm{tr}\left(\mathrm{Frob} \mid \mathrm{H}^i_{\text{ét},c}(X_{\overline{\mathbf{F}}_q}, \mathbf{Q}_\ell)\right).$$

Here ℓ is any prime not dividing q. The vector space $\mathrm{H}^i_{\text{ét},c}(X_{\overline{\mathbf{F}}_q}, \mathbf{Q}_\ell)$ carries an action of the pro-cyclic group $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) = \langle \mathrm{Frob} \rangle$.

When X is a variety that "makes sense" over both $\mathbf{C}$ and $\mathbf{F}_q$ (e.g. a proper smooth variety over $\mathrm{Spec}\,\mathbf{Z}$), we may hope

$$\dim_{\mathbf{Q}_\ell} \mathrm{H}^i_{\text{ét}}(X_{\overline{\mathbf{F}}_q}, \mathbf{Q}_\ell) = \dim_{\mathbf{Q}} \mathrm{H}^i(X(\mathbf{C}), \mathbf{Q}).$$

Under "good circumstances," this is the case. The configuration spaces Conf^n fit into these circumstances, so we have (for all $n > 2$)

$$\begin{aligned}
\mathrm{H}^0_{\text{ét}}(\mathrm{Conf}^n_{\overline{\mathbf{F}}_q}, \mathbf{Q}_\ell) &= \mathbf{Q}_\ell \\
\mathrm{H}^1_{\text{ét}}(\mathrm{Conf}^n_{\overline{\mathbf{F}}_q}, \mathbf{Q}_\ell) &= \mathbf{Q}_\ell \\
\mathrm{H}^i_{\text{ét}}(\mathrm{Conf}^n_{\overline{\mathbf{F}}_q}, \mathbf{Q}_\ell) &= 0 \qquad (i > 1)
\end{aligned}$$

Moreover, Frobenius acts as 1 on $\mathrm{H}^0_{\text{ét}}\, 0$, and as q on $\mathrm{H}^1_{\text{ét}}$.

Poincaré duality relates $\mathrm{H}^i_{\text{ét}}$ with $\mathrm{H}^{2n-i}_{\text{ét},c}$. It follows that

$$\begin{aligned}
\#\,\mathrm{Conf}^n(\mathbf{F}_q) = q^n &= \sum (-1)^i \operatorname{tr}(\mathrm{Frob}\, \mathrm{H}^i_{\text{ét}}(\mathrm{Conf}^n_{\overline{\mathbf{F}}_q}, \mathbf{Q}_\ell)^\vee) \\
&= q^n \left(\operatorname{tr}(\mathrm{Frob}\, |\mathrm{H}^{0\,\vee}) - \operatorname{tr}(\mathrm{Frob}\, |\mathrm{H}^{1\,\vee}) \right) \\
&= q^n \left(1 - \frac{1}{q} \right) \\
&= q^n - q^{n-1}.
\end{aligned}$$

So the reason for the lack of error term in our formula for $\mathrm{Conf}_n(q)$ is the fact that Conf^n satisfies an "Arnol'd theorem."

Recall that we were interested in counting square-free integers in $[N, 2N]$, monic square-free polynomials of degree n in $\mathbf{F}_q[t]$, and computing the cohomology of the moduli space of degree-n square-free polynomials in $\mathbf{C}[t]$.

We are in a position to clarify what is meant by geometric analytic number theory. Start with some problem over $\mathbf{Z}$ (or over some number field). Consider the analogous problem over $\mathbf{F}_q(t)$. Hope that this problem can be interpreted as the problem of studying $\#X_n(\mathbf{F}_q)$ for some sequence $\{X_n\}$ of varieties. Finally, we formulate a geometric / topological assertion about $X_\bullet$ over $\mathbf{C}$ which implies the above.

2.6 Chowla conjecture

Let μ the Möbius function defined by

$$\mu(n) = \begin{cases} 0 & n \text{ not squarefree} \\ (-1)^k & n \text{ a product of } k \text{ distinct primes} \end{cases}$$

We would expect this to be a random sign (from an additive point of view). For example, we would expect

$$\sum_{i=N}^{2N} \mu(n) = o(N),$$

i.e. that $\lim_{N\to\infty} \frac{1}{N} \sum_{i=N}^{2N} \mu(i) = 0$. The question of whether

$$\frac{1}{N} \sum_{N}^{2N} \mu(n)\mu(n+1) \to 0$$

is wide open.

Conjecture 2.6.1 (Chowla)**.**

$$\sum_{n=N}^{2N} \mu(n+a_1)^{\varepsilon_1} \cdots \mu(n+a_1)^{\varepsilon_r} = o(N).$$

The analogue of the Chowla conjecture over finite fields is also open. The slogan is: facts about arithmetic statistics in function fields in the "large q limit" correspond to facts about irreducible components (i.e. H^0) of moduli spaces.

As a specific example, consider sums

$$\sum_{\deg f = n} \mu(f)\mu(f+1).$$

Note that $\mu(f) = 0$ if and only if $\Delta(f) = 0$ if and only if f is not square-free. In fact, $\mu(f) = (-1)^n \chi(\Delta(f))$, were $\chi : \mathbf{F}_q^\times \to \mathbf{Z}^\times$ is the unique non-trivial character. So

$$\begin{aligned}\mu(f)\mu(f+1) &= \chi(\Delta(f))\chi(\Delta(f+1)) \\ &= \chi(\Delta(f)\Delta(f+1)) \\ &= \#\{\text{square roots of } \Delta(f)\Delta(f+1)\} - 1.\end{aligned}$$

So let Y_n be the moduli space of pairs (f, y), where y is a square root of $\Delta(f)\Delta(f+1)$. In other words, Y^n has equation $y^2 = \Delta(f)\Delta(f+1)$. So $Y_n \to \mathbf{A}^n$ is a double cover ramified at $V(\Delta(f)\Delta(f+1))$, the map being $(f, y) \mapsto f$. So

$$\begin{aligned}\sum_f \mu(f)\mu(f+1) &= \sum_f (\#\{\text{square roots of } \Delta(f)\Delta(f+1)\} - 1) \\ &= \#Y_n(\mathbf{F}_q) - q^n.\end{aligned}$$

We hope that this is $o(q^n)$, i.e. we want $\#Y_n(\mathbf{F}_q) = q^n + o(q^n)$.

Conjecture 2.6.2 (geometric Chowla)**.** *For all $n \geqslant 0$, the variety Y_n is irreducible, and there is a constant $\alpha > 0$ such that $H^{2n-i}_{\text{ét},c}(Y_n, \mathbf{Q}_\ell) = 0$ for all $i < \alpha n$.*

Instead of asking about $\lim_{n\to\infty} q^{-n}\#Y_n(\mathbf{F}_q)$, what about $\lim_{q\to\infty} q^{-n}\#Y_n(\mathbf{F}_q)$? Or what about

$$\lim_{n\to\infty} \lim_{q\to\infty} q^{-n}\#Y_n(\mathbf{F}_q).$$

Theorem 2.6.3 (Cerman-Rudnick)**.** *Let $\mathbf{F}_q$ have odd characteristic, and let $a_1, \ldots, a_m$ be distinct polynomials in $\mathbf{F}_q[t]$. Then*

$$\sum_{\deg f = n} \mu(f + a_1)^{\varepsilon_1} \cdots \mu(f + a_m)^{\varepsilon_m} \leqslant 2mnq^{n-1/2} + 3mn^2q^{n-1}.$$

if not all the ε_i are even

Note that the upper bound is $o(q^n)$ as $q \to \infty$ with n fixed. The main idea is that

$$\#Y_n(\mathbf{F}_q) = \sum (-1)^i \operatorname{tr}(\text{Frob}, H^{2n-i}_{\text{ét},c}(Y_n, \mathbf{Q}_\ell)).$$

The Weil bounds (a theorem of Deligne) give upper bounds for the eigenvalues of Frobenius acting on $H^{2n-i}_{\text{ét},c}(Y_n, \mathbf{Q}_\ell)$. These eigenvalues have absolute value at most $q^{n-i/2}$. The

sum of all Betti numbers can be bounded independently of q by some B. So the contribution of H^{2n-i} for all $i > 0$ is at most $Bq^{n-1/2}$, while $H^{2n}(Y_n, \mathbf{Q}_\ell)$ contributes something a bit more complicated. The space $H^{2n}_{\text{ét},c}(Y_n, \mathbf{Q}_\ell)$ is spanned by irreducible components of Y_n. Frobenius acts by q^n times a permutation action on components.

So $\text{tr}(\text{Frob}, H^{2n}) = \#\{\mathbf{F}_q\text{-rational irreducible components}\}$. So one needs to show that Y_n is geometrically irreducible. This is true unless $\Delta(f)\Delta(f+1)$ is a perfect square (as a polynomial). It's not, and this is the geometric heart of the argument.

One way to think of this: the étale double cover of $\mathbf{A}^n \smallsetminus V(\Delta(f)\Delta(f+1))$ given by adjoining $\sqrt{\Delta(f)\Delta(f+1)}$. This is given by a map

$$\text{Gal}(k(a_1, \ldots, a_n)) \to \mathbf{Z}/2.$$

We are interested in the image of this Galois representation. We need to know that it is surjective (i.e. that we have *big monodromy*).

2.7 Geometric analytic number theory that will not appear

We could look at the question of geometric twin primes / prime clusters. The variety involved would be the moduli space of *factored* f and factored g such that $g = f + 1$. In other words, we would look at the moduli space of tuples $(z_1, \ldots, z_n, w_1, \ldots, w_n)$ such that $(x - z_1) \cdots (x - z_n) + 1 = (x - w_1) \cdots (x - w_n)$. This variety admits an action of $S_n \times S_n$, and we would want to understand the cohomology of the variety together with its $S_n \times S_n$-action. Pollack and Barry-Soroker have proved "large q-limit" versions of these theorems.

There is also a geometric Limik / Malle / Bhargava conjecture. The relevant moduli spaces are X_n being the moduli space of degree-d covers (or G-covers) of $\mathbf{P}^1$ with n branch points (Hurwitz spaces).

There is a geometric Poonen-Rains conjecture, involving a moduli space of elliptic surfaces together with elements of $H^2(E, \mathbf{Z}/p)$.

There is a geometric Limik-Duke, on equidistribution of Heegner points. A recent paper of Shende and Tsimerman does this for "generalized theta divisors inside abelian varieties."

Finally, there is a geometric Batyrev-Manin. The relevant moduli space has $X(\mathbf{F}_q(t))$ classifying maps from $\mathbf{P}^1 \to X$, and X_n classifying degree-n maps from $\mathbf{P}^1$ to X.

2.8 Geometric Cohen-Lenstra

Conjecture 2.8.1 (Cohen, Lenstra)**.** *Let ℓ be an odd prime, and $E_{r,\ell,N}$ be the expected value, as d ranges over square-free integers in $[N, 2N]$, of*

$$\text{Surj}(\text{Cl}(\mathbf{Q}(\sqrt{-d})), (\mathbf{Z}/\ell)^r)$$

Then

$$\lim_{N \to \infty} E_{N,\ell,r} = 1.$$

For example, $E_{N,\ell,1}$ is the expected value of $\#\,\text{Cl}[\ell] - 1$.

The function field Cohen-Lenstra works as follows. Start with the following analogy:

number field	function field
$\mathbf{Q}(\sqrt{-d})$	$C_f : y^2 = f(x)$
$\mathcal{O} \subset \mathbf{Q}(\sqrt{-d})$	$U = C_f - \infty_f$
ideal of $\mathcal{O}$	effective divisor on U
class group of $\mathcal{O}$	$\mathrm{Pic}(U) = \mathrm{Jac}(C_f)(\mathbf{F}_q)$
$\mathrm{Cl}(\mathcal{O})[\ell]$	$\mathrm{Jac}(C_f)[\ell](\mathbf{F}_q)$

This suggests a definition: $\mathrm{Conf}^n(\ell)$ is the moduli space of hyperelliptic curves with ℓ-level structure, i.e. pairs (f, P), where f is squarefree monic of degree n and $P \in \mathrm{Jac}(C_f)[\ell]$ nonzero. The space $\mathrm{Conf}^n(\ell)$ is a cover of Conf^n via $(f, P) \mapsto f$. It is in fact a finite étale map of degree $\ell^{2g} - 1$. Let $E_{q,\ell,r,n}$ be

$$\mathbf{E}_f \left(\mathrm{Surj}(\mathrm{Jac}(C_f)(\mathbf{F}_q), (\mathbf{Z}/\ell)^r) \right) \qquad (\text{“expected value”}).$$

For example, $E_{q,\ell,q,n}$ is the average of $\#\mathrm{Jac}(C_f)(\mathbf{F}_q)[\ell] - 1$. This is the average of

$$\#\pi^{-1}(f)(\mathbf{F}_q) = \frac{\#\mathrm{Conf}^n(\ell)(\mathbf{F}_q)}{\#\mathrm{Conf}^n(\mathbf{F}_q)},$$

where $\pi : \mathrm{Conf}^n(\ell) \to \mathrm{Conf}^n$ is the canonical cover. So Cohen-Lenstra predicts that

$$\lim_{n\to\infty} \frac{\#\mathrm{Conf}^n(\ell)(\mathbf{F}_q)}{\mathrm{Conf}^n(\mathbf{F}_q)} = 1.$$

A “large q-limit” version of this has already been done. It works only if $\mathrm{Conf}^n(\ell)$ is geometrically irreducible (i.e. connected). Think of $\mathrm{Conf}^n(\ell) \xrightarrow{\pi} \mathrm{Conf}^n$ as the action of $\pi_1(\mathrm{Conf}^n) = \mathrm{Br}_n$ on $\pi^{-1}(f) = (\mathbf{Z}/\ell)^{2g}$. After choosing bases, this is just a representation $\mathrm{Br}_n \to \mathrm{Sp}_{2g}(\mathbf{F}_\ell)$. Saying that $\mathrm{Conf}^n(\ell)$ is connected is identical to saying that Br_n acts transitively on $(\mathbf{Z}/\ell)^{2g} \smallsetminus 0$. This is true, because we know that $\mathrm{Br}_n \to \mathrm{Sp}_{2g}(\mathbf{F}_\ell)$ is surjective! This is a theorem of A'Cumpo, Yu, Achter-Pries, and Hall. In fact, the big monodromy result gives

$$\lim_{q\to\infty} \text{average } \mathrm{Surj}(\mathrm{Jac}(C_f), (\mathbf{Z}/\ell)^r) = 1.$$

for all r. This amounts to studying the action of $\mathrm{Sp}_{2g}(\mathbf{F}_\ell)$ on surjections from $(\mathbf{Z}/\ell)^{2g}$ to $(\mathbf{Z}/\ell)^r$. Dually, we could look at the action on $\mathrm{Inj}((\mathbf{Z}/\ell)^r, (\mathbf{Z}/\ell)^{2g})$. But this action is *not* transitive. In other words, given an action $Q : (\mathbf{Z}/\ell)^r \to (\mathbf{Z}/\ell)^{2g}$, $Q^*\omega$ could be.... What's going on is not $\mathrm{Sp}_{2g}(\mathbf{F}_\ell)$, but a coset $\mathrm{Sp}_{2g}^{(q)}(\mathbf{F}_\ell) \subset \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$.

It turns out that the action of Frobenius on these components to multiply $Q^*\omega$ by q. The only fixed ones are those with $Q^*\omega = 0$, i.e. the orbit of isotropic subspaces of $(\mathbf{Z}/\ell)^{2g}$. The symplectic group $\mathrm{Sp}_{2g}(\mathbf{F}_\ell)$ *does* act transitively on those isotropic subspaces.

This works unless $q \equiv 1 \mod \ell$, in which case *all* orbits are fixed, and the Cohen-Lenstra heuristics fail.

3 Selmer group heuristics and sieves

3.1 Sieves in arithmetic geometry

Sieves form a very large topic, so we will only touch on a specific example, called the *closed point sieve*. We'll start by counting square-free integers. For a subset $\mathcal{P} \subset \mathbf{N}$, the *density* of $\mathcal{P}$, written $\mathrm{Prob}(\mathcal{P})$, is the limit

$$\mathrm{Prob}(\mathcal{P}) = \lim_{B\to\infty} \frac{\#\mathcal{P} \cap [1, B]}{B}.$$

Theorem 3.1.1. $\mathrm{Prob}(n \text{ is squarefree}) = \prod_p (1 - p^{-2}) = \zeta(2)^{-2} = \frac{6}{\pi}$.

Proof. The basic idea is to "sieve out the integers divisible by p^2," one prime a time. Choose cutoffs r and $\sqrt{B}$. We consider primes $\leqslant p$ to be "small," primes between r and $\sqrt{B}$ "medium," and primes $> \sqrt{B}$ to be "large." Fix r. Then

$$\mathrm{Prob}(p^2 \nmid n \text{ for all } p \leqslant r) = \prod_{p\leqslant r} \left(1 - \frac{1}{p^2}\right).$$

All that remains is to show that

$$\lim_{r\to\infty} \overline{\mathrm{Prob}}(n \text{ is divisible by } p^2 \text{ for some } p > r) = 0.$$

Concretely, this is saying that

$$\lim_{r\to\infty} \limsup_{B\to\infty} \frac{\#\{n \leqslant B : n \text{ is divisible by } p^2 \text{ for some } p > r\}}{B} = 0.$$

Since all we need is an upper bound, we can use stupid upper bounds. We can start out with the medium primes. We have

$$\begin{aligned}
\#\{n \leqslant B : n \text{ is divisible by } p^2 \text{ for some } p \in (r, \sqrt{B}]\} &\leqslant \sum_{p\in(r,\sqrt{B}]} \left\lfloor \frac{n}{p^2} \right\rfloor \\
&\leqslant \sum_{p\in(r,\sqrt{B})} \frac{B}{p^2} \\
&\leqslant B \int_r^\infty \frac{dx}{x^2} \\
&= \frac{B}{r}.
\end{aligned}$$

All that remains is the large primes. But

$$\#\{n \leqslant B : n \text{ is divisible b } p^2 \text{ for some } p > \sqrt{B}\} = 0,$$

so we are done. □

Bjorn Poonen

Next we look at square-free values of a polynomial, e.g. Prob(n^4+1 is square-free).

Conjecture 3.1.2. *The probability is* $\prod_p \left(1-\frac{c_p}{p^4}\right)$, *where* $c_p = \#\{n \in \mathbf{Z}/p^2 : n^4+1 \equiv 0\}$.

Proof? We start with small primes as before. We get

$$\text{Prob}(p \nmid n^4+1 \text{ for all } p \leqslant r) = \prod_{p \leqslant r} \left(1-\frac{c_p}{p^2}\right).$$

Let's attack the large primes. Here *large* means $p > B^2$. As before,

$$\#\{n \leqslant B : p^2 \nmid n^4+1 \text{ for some } p > B^2\} = 0.$$

All that remains are the medium primes, where *medium* means $r < p \leqslant B^2$. If we try to repeat the naïve bound, we get, for each p not dividing $\text{Disc}(x^4+1)$,

$$\#\{n \leqslant B : p^2 \mid n^4\} \leqslant 4 \cdot \left\lceil \frac{B}{p^2} \right\rceil$$

It follows that

$$\begin{aligned}\#\{n \leqslant B : p^2 \mid n \text{ for some } p \in (r, B^2)\} &\leqslant \sum_{p \in (r,B^2)} 4\left\lceil \frac{B}{p^2} \right\rceil \\ &\leqslant \sum_{p \in (r,B^2)} \left(4\frac{B}{p^2}+4\right) \\ &\leqslant \frac{4}{r}B + 4\frac{B^2}{\log B^2},\end{aligned}$$

which is *not* small enough relative to B for the proof to work. □

This conjecture follows from the ABC conjecture due to the work of many people (Browking, Filaseta, Greaves, Schinzel, Granville). They worked with arbitrary cyclotomic polynomials.

3.2 Closed points and zeta functions

Let k be a field, and X a scheme of finite type over k. A *closed point* of X is exactly that – a point in X which is closed. In an affine chart $\text{Spec}(A)$, closed points P correspond to maximal ideals $\mathfrak{m} \subset A$. Let $\kappa(P)$ be the *residue field* of P, i.e. the field $A/\mathfrak{m}$. The weak nullstellensatz tells us that $\kappa(P)$ is a finite extension of k. These notions also make sense if X is a scheme of finite type over $\text{Spec}(\mathbf{Z})$. In that case, the residue fields will be finite.

If X/k is of finite type and P is a closed point in X, then we define the *degree* of P, written $\deg P$, to be the integer $[\kappa(P) : k]$. If $\kappa(P) = A/\mathfrak{m}$ for some affine chart $\text{Spec}(A)$, then $\deg P = [A/\mathfrak{m} : k]$.

Example 3.2.1. A closed point on $\mathbf{A}^1$ corresponds to a maximal ideal of $k[t]$. Such ideals are generated by unique monic irreducible polynomials in $k[t]$, which are in bijection with $\text{Gal}(\bar{k}/k)$-orbits in $\mathbf{A}^1(\bar{k})$.

More generally, if X is a k-scheme, a closed point of X will correspond to a $\mathrm{Gal}(\overline{k}/k)$-orbit in $X(\overline{k})$. Write $|X|$ for the set of closed points in X.

We can reinterpret the Riemann zeta function as

$$\zeta_{\operatorname{Spec}\mathbf{Z}}(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1} = \prod_{P \in |\operatorname{Spec}\mathbf{Z}|} (1 - \#\kappa(P)^{-s})^{-1}.$$

In general, if X is a scheme of finite type over $\mathbf{Z}$, we define

$$\zeta_X(s) = \prod_{P \in |X|} (1 - \#\kappa(P)^{-s})^{-1}.$$

This Euler product converges for $\Re(s) > \dim X$. As a special case, any scheme of finite type over $\mathbf{F}_q$ has a zeta function. In that case, $\#\kappa(P) = q^{\deg P}$, so

$$\zeta_X(s) = \prod_{P \in |X|} (1 - q^{-s \deg P})^{-1}.$$

As a power series in $T = q^{-s}$, this turns out to be

$$Z_X(T) = \exp\left(\sum_{r \geqslant 1} \frac{\#X(\mathbf{F}_{q^r})}{r} T^r \right).$$

3.3 Bertini smoothness theorems

Let $X \subset \mathbf{P}^n$ be defined over a field k. Suppose X is smooth of dimension m over k. We only assume X is quasi-projective. Then there exists a dense open $U \subset (\mathbf{P}^n)^\vee$ such that for all $u \in U$, the corresponding hyperplane $H_u \subset \mathbf{P}^n_{\kappa(u)}$ has $H_u \cap X$ smooth of dimension $n-1$ over $\kappa(u)$.

Corollary 3.3.1. *If k is infinite, there exists H/k such that $H \cap X$ is smooth.*

If k is finite, this corollary is wrong! To fix this, we will change the problem. Let $S = \mathbf{F}_q[x_0, \ldots, x_n]$ and $\mathbf{P}^n = \operatorname{Proj}(S)$. Let

$$S_d = \{\text{homogeneous polynomials of degree } d \text{ in } S\},$$

and put $S_{\text{hom}} = \bigcup_{d \geqslant 0} S_d$. For $f \in S_d$, let $H_f = \operatorname{Proj}(S/f)$. For $\mathcal{P} \subset S_{\text{hom}}$, define the *density* of $\mathcal{P}$ to be

$$\mu(\mathcal{P}) = \lim_{d \to \infty} \frac{\#\mathcal{P} \cap S_d}{\#S_d}.$$

Theorem 3.3.2 (Bertini smoothness over $\mathbf{F}_q$)**.** *Let X be a smooth m-dimensional quasi-projective subscheme of $\mathbf{P}^m$ over $\mathbf{F}_q$. Then*

$$\mathcal{P} = \{f \in S_{\text{hom}} : H_f \cap X \text{ is smooth of dimension } m-1\}$$

has density $\mu(\mathcal{P}) = \zeta_X(m+1)^{-1} \in \mathbf{Q} \cap [0,1]$.

For comparison,

$$\operatorname{Prob}(n \neq 0 \text{ in } \operatorname{Spec}\mathbf{Z} \text{ is regular}) = \zeta(2)^{-1}$$

where $2 = \dim(\operatorname{Spec}\mathbf{Z}) + 1$. There is a conjectural joint generalization of these two facts.

Example 3.3.3. Let $X + \mathbf{P}^2$ over $\mathbf{F}_2$. The question in this example is: what is the probability that a plane curve is smooth? It turns out that $\#\mathbf{P}^2(\mathbf{F}_{2^r}) = 4^r + 2^r + 1$, so $Z_X(T) = ((1-T)(1-2T)(1-4T))^{-1}$, so we get the following theorem.

Theorem 3.3.4. *μ(smooth plane curves in $\mathbf{P}^2$ over $\mathbf{F}_2$) $= \frac{21}{64}$.*

Proof of Bertini theorem. We'll do the case $X = \mathbf{A}^2 \subset \mathbf{P}^2$. Identify $f \in S_{\text{hom}}$ with its dehomogenization $f(1, x, y) \in \mathbf{F}_q[x, y]$. Recall that $f \in \mathcal{P}$ if and only if H_f is smooth (of dimension 1) at each closed point $P \in \mathbf{A}^2$. For each P, H_f is smooth at P if and only if $f(P)$, $\frac{\partial f}{\partial x}(P)$, $\frac{\partial f}{\partial y}(P)$ are not all zero in $\kappa(P) = \mathbf{F}_{q^{\deg P}}$. A fake proof is:

$$\text{Prob}(H_f \text{ is smooth at } P) = 1 - \frac{1}{q^{3\deg P}} \Rightarrow \text{Prob}(H_f \text{ smooth}) = \prod_{P \in \mathbf{A}^2} \left(1 - \frac{1}{q^{3\deg P}}\right),$$

which is our zeta value $\zeta_{\mathbf{A}^2}(3)^{-1}$.

As with square-free integers, we'll choose a cutoff r, and call degree $\leqslant r$ *low*, degree between r and $d/3$ *medium*, and degree $> d/3$ *high*. We will treat these cases separately. Let

$$\mathcal{P}_r = \{f \in S_{\text{hom}} : H_f \text{ is smooth at all } P \text{ with } \deg P \leqslant r\}$$

Lemma 3.3.5. $\mu(\mathcal{P}_r) = \prod_{\deg P \leqslant r} \left(1 - \frac{1}{q^{3\deg P}}\right)$.

Proof. Let $\mathfrak{m}_P \subset \mathbf{F}_q[x, y]$ be the maximal ideal corresponding to P. Let $I = \prod_{\deg P \leqslant r} \mathfrak{m}_P^2$. Then $f \in S_d$ belongs to $\mathcal{P}_r$ if and only if the image of f under

$$\mathbf{F}_q[x, y]_{\leqslant d}/I \xrightarrow{\phi_d} \prod_{\deg P \leqslant r} \mathbf{F}_q[x, y]/\mathfrak{m}_P^2$$

is non-zero in each factor. For this to work, we need ϕ_d to be surjective when $d \gg 0$, but this is obvious. □

How large must d be? Let $V_d = \text{im}(\phi_d)$. Then $V_{d+1} = V_d + xV_d + yV_d$. The sequence $V_0 \subset V_1 \subset \cdots \subset \cdots$ must terminate at some D. In fact, once $V_D = V_{D+1}$, we know that ϕ_D is surjective. In fact, $D \leqslant \dim_{\mathbf{F}_q}(\mathbf{F}_q[x, y]/I)$. Thus ϕ_d is surjective for $d \geqslant \dim_{\mathbf{F}_q}(\mathbf{F}_q[x, y]/I)$.

Now we look at points of medium degree. Let

$$Q_r = \bigcup_d \{f \in S_d : \text{there is } P \text{ with } r < \deg P \leqslant d/3 \text{ at which } H_f \text{ not smooth}\}.$$

Lemma 3.3.6. *$\overline{\mu}(Q_r) \to 0$ as $r \to \infty$.*

Proof. The map $\mathbf{F}_q[x, y]_{\leqslant d} \to \mathbf{F}_p[x, y]/\mathfrak{m}_P^2$ is surjective for all P with $d \geqslant 3 \deg P$. Thus

$$\overline{\mu}(Q_r) \leqslant \limsup_{d \to \infty} \sum_{r < \deg P \leqslant d/3} \frac{1}{q^{3\deg P}} \to 0.$$

□

The tricky part is handling large degree points.

Lemma 3.3.7. *Fix a curve $Z \subset \mathbf{A}^2$, i.e. $\dim Z = 1$. Then*

$$\frac{\#\{f \in \mathbf{F}_q[x,y]_{\leqslant d} : f|_Z = 0\}}{\#\mathbf{F}_q[x,y]_{\leqslant d}} \leqslant q^{-d}.$$

Proof. Choose a coordinate, say x, such that x is non-constant on Z. We would like to bound the size of the kernel in

$$0 \to \ker \to \mathbf{F}_q[x,y]_{\leqslant d} \to \mathrm{H}^0(\mathscr{O}_Z).$$

Note that the image has dimension at least $d+1$, because it contains $1, x, \ldots, x^d$. □

We are trying to bound the size of the set

$$\mathcal{R} = \bigcup_d \{f \in S_d : H_f \text{ is not smooth at some deg } P > d/3\}.$$

Lemma 3.3.8. $\mu(\mathcal{R}) = 0$.

Proof. Write $f = f_0 + g_1^p x + g_2^p y + h^p$, for random f_0, g_1, g_2, h of degrees $\leqslant d, \leqslant \frac{d-1}{p}, \leqslant \frac{d-1}{p}$, $\leqslant \frac{d}{p}$. This is a random element of $\mathbf{F}_q[x,y]_{\leqslant d}$. We have

$$\frac{\partial f}{\partial x} = \frac{\partial f_0}{\partial x} + g_1^p$$
$$\frac{\partial f}{\partial y} = \frac{\partial f_0}{\partial y} + g_2^p.$$

Given f_0, there is at most one g_1 with $\partial_x f = 0$. So

$$\text{Prob}(g_1 \text{ is s.t. } \dim\{\partial_x f = 0\} \leqslant 1 | \text{choice of } f_0) \approx 1$$
$$\text{Prob}(g_g \text{ is s.t. } \dim\{\partial_x f = \partial_y f = 0\} \leqslant 0 | \text{choice of } f_0, g_1) \approx 1.$$

The condition $\dim\{\partial_x f = \partial_y f = 0\} \leqslant 0$ fails if and only if $\partial_y f_0 + g_2^q$ vanishes on some component of $\{\partial_x f = 0\}$. □

We know that $\mathcal{P} = \mathcal{P}_r \smallsetminus Q_r \smallsetminus \mathcal{R}$. As $r \to \infty$, $\mu(\mathcal{P}_r \to \zeta_{\mathbf{A}^2}(3)^{-1}$, $\overline{\mu}(Q - r) \to 0$, and $\mu(\mathcal{R}) = 0$. Thus we have proved that $\mu(\mathcal{P}) = \zeta_{\mathbf{A}^2}(3)^{-1}$. □

There are variants of the Bertini theorem. For example, we could prescribe the Taylor coefficients at finitely many points. This lets us answer a question of Nick Katz (the question was also resolved by Ofer Gabber). Given a nice variety X over $\mathbf{F}_q$ of dimension $\geqslant 1$ (Here, "nice" means "smooth, projective and geometrically integral.), there is a nice curve $Y \subset X$ such that $Y(\mathbf{F}_q) = X(\mathbf{F}_q)$.

Also, you can use the Bertini theorem to obtain abelian varieties as quotients of Jacobians of curves (which are themselves contained in the abelian variety). Let A be of dimension $\geqslant 1$ over $\mathbf{F}_q$. Then there is a nice curve $X \subset A$ such that $\mathrm{Jac}\, X \to A$ is surjective. The trick is to find X passing through all ℓ-torsion points of A. This forces $\mathrm{Jac}\, X$ to have $\ell^{2\dim A}$ torsion points, i.e. it has the same dimension as A.

In Nguyen's thesis, we have a Whitney embedding theorem for finite fields. Let X be a nice curve over $\mathbf{F}_q$. Then there is a closed immersion $X \hookrightarrow \mathbf{P}_{\mathbf{F}_{q^3}}$ if and only if for each $e \geqslant 1$, $\#X(\mathbf{F}_{q^e}) \leqslant \mathbf{P}^3(\mathbf{F}_{q^e})$.

3.4 Selmer group heuristics

Let $G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be the absolute Galois group of $\mathbf{Q}$. Let

$$\mathbf{Q}_v = \begin{cases} \mathbf{R} & v = \infty \\ \mathbf{Q}_p & v = p \end{cases}$$

Let $\mathbf{A}$ be the ring of adeles of $\mathbf{A}$, i.e.

$$\mathbf{A} = \prod_v{}'(\mathbf{Q}_v, \mathbf{Z}_v) = \{(a_v) \in \prod \mathbf{Q}_v : a_v \in \mathbf{Z}_v \text{ almost all } v\}.$$

Theorem 3.4.1. *Let E be an elliptic curve over $\mathbf{Q}$. Then $E(\mathbf{Q})$ is finitely generated.*

There is basically only one proof of this. First, one shows "weak Mordell-Weil." i.e. that $E(\mathbf{Q})/n$ is finite for some $n \geqslant 2$. Then one uses height functions to get the general case. Consider the exact sequence

$$0 \to E[n] \to E \xrightarrow{n} E \to 0$$

of sheaves on the étale site of $\mathbf{Q}$. We can take G-invariants (i.e. $\mathrm{H}^0_{\text{ét}}$) we get a sequence

$$0 \to E[n](\mathbf{Q}) \to E(\mathbf{Q}) \xrightarrow{n} E(\mathbf{Q}) \to \mathrm{H}^1(\mathbf{Q}, E[n]) \to \mathrm{H}^1(\mathbf{Q}, E) \xrightarrow{n} \mathrm{H}^1(\mathbf{Q}, E) \to \cdots$$

We use $\mathrm{H}^1(\mathbf{Q}, E)$ as an abbreviation for $\mathrm{H}^1_{\text{ét}}(\mathbf{Q}, E) = \mathrm{H}^1(G_{\mathbf{Q}}, E(\overline{\mathbf{Q}}))$. So we have a sequence

$$0 \to E(\mathbf{Q})/n \to \mathrm{H}^1(\mathbf{Q}, E[n]) \to \mathrm{H}^1(\mathbf{Q}, E).$$

Unfortunately, $\mathrm{H}^1(\mathbf{Q}, E[n])$ is infinite. We have the same sequence at all places of $\mathbf{Q}$:

$$E(\mathbf{Q}_v)/n \to \mathrm{H}^1(\mathbf{Q}_v, E[n]) \to \mathrm{H}^1(\mathbf{Q}_v, E).$$

Combine all these to get a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(\mathbf{Q})/n & \longrightarrow & \mathrm{H}^1(\mathbf{Q}, E[n]) & \longrightarrow & \mathrm{H}^1(\mathbf{Q}, E) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod_v E(\mathbf{Q}_v)/n & \longrightarrow & \prod_v \mathrm{H}^1(\mathbf{Q}_v, E[n]) & \longrightarrow & \prod_v \mathrm{H}^1(\mathbf{Q}_v, E) \end{array}$$

We can actually use restricted direct products on the bottom, so we put

$$E(\mathbf{A})/n = \prod_v{}' E(\mathbf{Q}_v)/n$$

$$\mathrm{H}^1(\mathbf{A}, E[n]) = \prod_v{}' \mathrm{H}^1(\mathbf{Q}_v, E[n])$$

$$\mathrm{H}^1(\mathbf{A}, E) = \prod_v{}' \mathrm{H}^1(\mathbf{Q}_v, E)$$

To sum up, we have a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(\mathbf{Q})/n & \longrightarrow & \mathrm{H}^1(\mathbf{Q}, E[n]) & \longrightarrow & \mathrm{H}^1(\mathbf{Q}, E) \\ & & \downarrow & & \downarrow \beta & & \downarrow \gamma \\ 0 & \longrightarrow & E(\mathbf{A})/n & \xrightarrow{\alpha} & \mathrm{H}^1(\mathbf{A}, E[n]) & \longrightarrow & \mathrm{H}^1(\mathbf{A}, E) \end{array}$$

Define the *n-Selmer group* and *Tate-Shafarevich group* of E by

$$\mathrm{Sel}_n(E) = \beta^{-1}(\mathrm{im}\,\alpha)$$
$$Ш(E) = \ker \gamma.$$

Standard theorems of algebraic number theory yield the finiteness (and computability) of $\mathrm{Sel}_n E$.

For an elliptic curve E over $\mathbf{Q}$, find a model $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbf{Z}$ minial, and put $h(E) = \max(|A|^3, |B|^2)$. Let $\mathcal{E}$ be the set of isomorphism classes of elliptic curves over $\mathbf{Q}$. For any x, put $\mathcal{E}_{<x} = \{E \in \mathcal{E} : h(E) < x\}$.

Definition 3.4.2. *If $S \subset \mathcal{E}$, put*

$$\mathrm{Prob}(S) = \lim_{X \to \infty} \frac{\#(S \cap \mathcal{E}_{<X})}{\#\mathcal{E}_{<X}}.$$

Given p and s, we are interested in computing

$$\mathrm{Prob}(\dim_{\mathbf{F}_p} \mathrm{Sel}_p E = s).$$

3.5 Maximal isotropic subspaces

Let $V = \mathbf{F}_p^{\oplus 2n}$, and let

$$Q(x_1, \ldots, x_n, y_1, \ldots, y_n).$$

We call V a *hyperbolic quadratic space* over $\mathbf{F}_p$. The function Q induces a pairing $\langle -, - \rangle$ on V by

$$\langle v, w \rangle = Q(v + w) - Q(v) - Q(w).$$

For $Z \subset V$ an $\mathbf{F}_p$-subspace, put

$$Z^\perp = \{v \in V : \langle v, z \rangle = 0 \text{ for all } z \in Z\}.$$

We call Z *isotropic* if $Q|_Z = 0$. The space Z is *maximal isotropic* if $Q|_Z = 0$ and $Z = Z^\perp$. All maximal isotropic subspaces of V have dimension n.

Example 3.5.1. The space $\{(x_1, \ldots, x_n, 0, \ldots, 0) : x_i \in \mathbf{F}_p\}$ is maximal isotropic.

Put

$$\mathrm{OGr}_n(\mathbf{F}_p) = \{\text{maximal isotropic subspaces of } V\}.$$

Choose $Z, W \in \mathrm{OGr}_n(\mathbf{F}_p)$ at random. This gives us a random variable $\dim_{\mathbf{F}_p}(Z \cap W)$.

Conjecture 3.5.2 (Poonen, Rains)**.** *For each $s \in \mathbf{Z}_{\geqslant 0}$,*

$$\mathrm{Prob}_{E \in \mathcal{E}}(\dim \mathrm{Sel}_p E = s) = \lim_{n \to \infty} \mathrm{Prob}_{Z, W \in \mathrm{OGr}_n(\mathbf{F}_p)}(\dim(Z \cap W) = s).$$

Our goal is to show that $\mathrm{Sel}_p E$ actually is an intersection of maximal isotropic subspaces in an infinite-dimensional quadratic space. For simplicity, we assume p is odd.

We'll start with a construction for local fields. Let E be an elliptic curve over some $\mathbf{Q}_v$. Put $V_v = \mathrm{H}^1(\mathbf{Q}_v, E[p])$; this is a finite-dimensional $\mathbf{F}_p$-vector space. Recall the *Weil pairing* is a bilinear pairing

$$e : E[p] \times E[p] \to \mathbf{G}_m$$

This induces a pairing

$$\langle \cdot, \cdot \rangle_v : V_v \times V_v \xrightarrow{\smile} \mathrm{H}^2(\mathbf{Q}_v, E[p]^{\otimes 2}) \xrightarrow{e} \mathrm{H}^2(\mathbf{Q}_v, \mathbf{G}/m) = \mathrm{Br}\, \mathbf{Q}_v \hookrightarrow \mathbf{Q}/\mathbf{Z}.$$

So we have $Q_v : V_v \to \mathbf{R}/\mathbf{Z}$. Define $W_v = \mathrm{im}(E(\mathbf{Q}_v)/p \subset V_v)$. It is a theorem of O'Neil (using Tate local duality) that W_v is a maximal isotropic subspace of V_v.

Over global fields, let $V_v = \mathrm{H}^1(\mathbf{Q}_v, E[p])$ for each v. Let

$$V = \prod_v{}' (V_v, W_v) \simeq \mathrm{H}^1(\mathbf{A}, E[p]).$$

As before, we have a commutative diagram

$$\begin{array}{ccc} & & \mathrm{H}^1(\mathbf{Q}, E[p]) \\ & & \downarrow \beta \\ E(\mathbf{A})/p & \xrightarrow{\alpha} & \mathrm{H}^1(\mathbf{A}, E[p]) \end{array}$$

Let $Q = \sum Q_v : V \to \mathbf{R}/\mathbf{Z}$.

Theorem 3.5.3. *The images of α and β are maximal isotropic. Moreover, β is injective, and* $\mathrm{im}(\alpha) \cap \mathrm{im}(\beta) = \beta(\mathrm{Sel}_p E) \simeq \mathrm{Sel}_p E$.

So in some sense, $\mathrm{Sel}_p E$ "is" the intersection of two maximal isotropic subspaces of $\mathrm{H}^1(\mathbf{A}, E[p])$.

To show that α has maximal isotropic image, simply note that $\mathrm{im}(\alpha) = \prod_v W_v$. To show the same about $\mathrm{im}(\beta)$, use some global duality theorems (9-term Poitu-Tate exact sequence). To show that β is injective, use Čebotarev, plus the fact that the Sylow p-subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$ is cyclic. The third part follows from the first two and the definition of $\mathrm{Sel}_p(E)$.

4 Asymptotics for number fields and class groups

4.1 Counting number fields

Theorem 4.1.1 (Hermite)**.** *Given $X > 0$, there are finitely many number fields K (up to isomorphism, or in $\overline{\mathbf{Q}}$) with $|\operatorname{Disc} K| < X$.*

Question 4.1.2. *What are the asymptotics in X of the function $N(X) = \#\{K : |\operatorname{Disc} K| < X\}$?*

These types of questions turn out to be easiest to address after restricting to number fields with some fixed invariant. The most obvious of these is the *Galois group*. If K is a number field of degree n, the Galois group of K, denoted $\operatorname{Gal}(K)$, is the image of $\operatorname{Gal}(\widetilde{K}/\mathbf{Q}) \to S_n$, where $\widetilde{K}$ is the Galois closure of K. The representation $\operatorname{Gal}(\widetilde{K}/\mathbf{Q}) \to S_n$ is given by the action of $\operatorname{Gal}(\widetilde{K}/\mathbf{Q})$ on the n homomorphisms $K \to \overline{\mathbf{Q}}$.

Example 4.1.3. Write $K = \mathbf{Q}(\theta)$, and let $\theta_1, \dots, \theta_n$ be the n conjugates of θ in $\overline{\mathbf{Q}}$. Then we are interested in the action of $\operatorname{Gal}(\widetilde{K}/\mathbf{Q})$ on the set $\{\theta_1, \dots, \theta_n\}$.

So for us, $\operatorname{Gal}(K)$ is not just an abstract group – it is a group of permutations.

Example 4.1.4. Let K be a cubic field. Then $\operatorname{Gal}(K) \subset S_3$. We call K a *cyclic cubic field* if K is Galois and $\operatorname{Gal}(K) = A_3 \simeq \mathbf{Z}/3$. If K is non-Galois, then $\operatorname{Gal}(K) = S_3$.

We are interested in the asymptotics of the function

$$N_\Gamma(X) = \#\{K : |\operatorname{Disc} K| < X \text{ and } \operatorname{Gal}(K) \simeq \Gamma\}.$$

4.2 Local behavior

Given a place p of $\mathbf{Q}$ (so p is a prime or $p = \infty$), we can form the completion $K_p = K \otimes_{\mathbf{Q}} \mathbf{Q}_p$. (Recall that $\mathbf{Q}_\infty = \mathbf{R}$). This is bigger than the "honest completion" of K at a place of K. If p is a finite prime, we would have $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ in $\mathfrak{o}_K$. The ring K_p is a direct product of field extensions of $\mathbf{Q}_p$. More precisely,

$$K_p = \prod_i K_{\mathfrak{p}_i},$$

where $K_{\mathfrak{p}_i}$ is the completion of K at the prime $\mathfrak{p}_i$. So K_p is an étale $\mathbf{Q}_p$-algebra. The ring K_p captures the splitting, inertia, etc. or p in K.

Question 4.2.1. *What are the asymptotics of*

$$N_{\Gamma,M}(X) = \#\{K : |\operatorname{Disc} K| < X, \operatorname{Gal}(K) \simeq \Gamma, \textit{ and } K_p \simeq M\},$$

for some group Γ and étale $\mathbf{Q}_p$-algebra M?

Example 4.2.2. How many quadratic number fields are there split completely at 7? This is essentially the study of the function $N_{S_2, \mathbf{Q}_7^{\times 2}}$.

We can also ask probabilistic questions. Define

$$\begin{aligned}\mathbf{P}_{\text{Disc}}&(\text{quadratic } K \text{ split completely at } 7)\\ &= \lim_{X\to\infty} \frac{\#\{K : |\operatorname{Disc} K| < X, \operatorname{Gal}(K) \simeq S_2 \text{ and } K \text{ s.c. at } 7\}}{\#\{K : |\operatorname{Disc} K| < X \text{ and } \operatorname{Gal}(K) \simeq S_2\}}\end{aligned}$$

4.3 Independence

Are the probabilities above independent of the prime involved? Consider the following diagram:

	2	3	5	7
$\mathbf{Q}(\sqrt{-3})$	i	r	i	s
$\mathbf{Q}(i)$	r	i	s	i
$\mathbf{Q}(\sqrt{5})$	i	i	r	i
$\mathbf{Q}(\sqrt{-7})$	s	i	i	r

Here "s" denotes "split," "i" denotes "inert," and "r" denotes "ramified." Čebotarev's density theorem tells us that if we look in a single row, we get $\frac{1}{2}$ split, none (probabilistically) ramified, and one-half inert. On the other hand,

$$\mathbf{P}_{\text{Disc}}(K \text{ quadratic split at } 7) = \frac{7}{16}$$
$$\mathbf{P}_{\text{Disc}}(K \text{ quadratic inert at } 7) = \frac{7}{16}$$
$$\mathbf{P}_{\text{Disc}}(K \text{ quadratic ramified at } 7) = \frac{1}{8}.$$

So *Čebotarev independence* for us means the (asymptotic) independence of the rows in the chart. This is known. More generally, if we listed all (Galois) number fields in the rows, we have *Čebotarev dependence* between two fields if and only if they have no common subfield larger than $\mathbf{Q}$.

Question 4.3.1. *What do we expect for primes?*

In other words, if we fix a prime p, how does the ramification data above p vary with the fields.

4.4 Counting class groups

Let's begin with a precise question. Consider imaginary quadratic fields.

Question 4.4.1. *Given an odd prime p and a finite abelian p-group G, what proportion of imaginary quadratic fields K (ordered by discriminant) have Sylow p-subgroup of the* $\mathrm{Cl}(K)$ *isomorphic to G?*

Recall that the *class group* of K, $\mathrm{Cl}(K)$ is a finite abelian group. Such groups are the direct sum of their Sylow p-subgroups. So we are interested in what, asymptotically, the p-part of $\mathrm{Cl}(K)$ looks like. We restrict to odd primes because *genus theory* tells us something about the case $p = 2$. We can also ask for averages of other f over class groups (where f is a characteristic function).

Example 4.4.2. What are

$$\lim_{X\to\infty} \frac{\sum_K \left(\frac{\#\mathrm{Cl}(K)}{p\cdot\mathrm{Cl}(K)}\right)^k}{\#\{K : K \text{ imaginary quadratic and } |\operatorname{Disc} K| < X\}}$$
$$\lim_{X\to\infty} \frac{\sum K\#\operatorname{Sur}(\mathrm{Cl}(K), A)}{\text{same}}?$$

were A is a finite abelian group and $\mathrm{Sur}(A, B)$ is the number of surjections $A \to B$.

For a function f on finite abelian groups, write $M_{\mathrm{field}}(f)$ for this average.

4.5 Cohen-Lenstra Heuristics

The main idea is that "some things in nature" occur with frequency inversely proportional to their number of automorphisms.

Example 4.5.1. Consider cubic fields in $\overline{\mathbf{Q}}$. The Galois fields occur appear once, but have three automorphisms, while the non-Galois fields appear three times, but have only one automorphism.

Conjecture 4.5.2 (Cohen-Lenstra, Gerth for $p = 2$)**.** *For any "reasonable" f, we have*

$$M_{\mathit{field}}(f) = \lim_{n\to\infty} \frac{\displaystyle\sum_{\mathit{fin.\ ab.\ gp.}\ |\cdot| \leqslant n} \frac{f(G)}{\#\operatorname{Aut}(G)}}{\displaystyle\sum_{\mathit{fin.\ ab.\ gp.}\ |\cdot| \leqslant n} \frac{1}{\#\operatorname{Aut}(G)}}$$

where the average is taken over $2\operatorname{Cl}(K)$.

Cohen and Lenstra compute $M_{\mathrm{group}}(f)$ for many examples of f.

Example 4.5.3. If f is the characteristic function of the "odd cyclic part," then $M_{\mathrm{group}}(f) \approx 0.977575\ldots$.

Example 4.5.4. If A is a finite abelian group and $f(G) = \#\mathrm{Surj}(G, A)$, then $M_{\mathrm{group}}(f) = 1$.

. . . stopped taking notes. . .

References

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RA, 1999.

[Poo13] Bjorn Poonen. Rational points on varieties, 2013. available at `http://www-math.mit.edu/~poonen/papers/Qpoints.pdf`.