SELMER GROUP HEURISTICS AND SIEVES

BJORN POONEN

These are expanded lecture notes for a series of four lectures at the Arizona Winter School on "Arithmetic statistics" held March 15–19, 2014 in Tucson, Arizona. They are not intended for publication; in fact, they are largely drawn from articles that have already been published: [Poo04, Poo07, PR12, BKL+13].

Part 1. Sieves in arithmetic geometry

1. Introduction

In the past decade or so, the most elementary of the sieve methods of analytic number theory has been adapted to a geometric setting. In this geometric setting, the primes are replaced by the closed points of a variety over a finite field or more generally of a scheme of finite type over $\mathbb{Z}$. We will present the method and some of the results that have been proved using it. For instance, the probability that a plane curve over $\mathbb{F}_2$ is smooth is asymptotically $21/64$ as the degree tends to infinity.

2. Squarefree integers

Before discussing the geometric sieve, let us recall a simple application of classical sieve techniques, to the counting of squarefree integers.

Consider the problem of determining the "probability" that a "random" positive integer is squarefree. To make sense of this problem, we should clarify what is meant by probability, since the set of positive integers is countably infinite. For any subset $S \subseteq \mathbb{N}$, define the density of S as the limit

$$\mu(S) := \lim_{B\to\infty} \frac{\#(S \cap [1, B])}{B}.$$

In other words, we compute the fraction of the integers from 1 to B that belong to S, and then let B tend to ∞.

From now on, interpret "the probability that a positive integer is squarefree" as the density of the set S of squarefree positive integers. We can guess the answer by using the following reasoning. An integer n is squarefree if and only if for all primes p, the integer p^2 does not divide n. For each prime p, the probability that an integer is divisible by p^2 is $1/p^2$, so the probability that the integer is *not* divisible by p^2 is $1 - 1/p^2$. These conditions for different p

Date: March 14, 2014.

should be independent, by the Chinese remainder theorem. Therefore one predicts that the density of squarefree integers equals

$$\prod_{\text{prime } p} (1 - p^{-2}) = \zeta(2)^{-1} = 6/\pi^2,$$

where $\zeta(s)$ is the Riemann zeta function, defined by

$$\zeta(s) := \sum_{n \geq 1} n^{-s} = \prod_{\text{prime } p} (1 - p^{-s})^{-1}$$

for $\mathrm{Re}(s) > 1$ (which is all we need).

It is not immediate that this heuristic prediction can be made rigorous. The Chinese remainder theorem does imply that for any *finite* set T of primes, the density of positive integers not divisible by p^2 for any $p \in T$ equals $\prod_{p \in T}(1 - p^{-2})$. But the argument breaks down if we try to apply the Chinese remainder theorem to infinitely many primes. In other words, the difficulty is that to prove a density result for squarefree integers, we must let T grow to include all primes *before* letting B tend to infinity, but the argument so far shows only that when B is *sufficiently large relative to the primes in* T, then the number of such integers in $[1, B]$ is approximately $B \prod_{p \in T}(1 - p^{-2})$.

One approach that works is to approximate the condition of being squarefree by the condition of being "squarefree as far as the primes $\leq r$ are concerned", and then to estimate the error in this approximation. As $B \to \infty$ for fixed r, the fraction of integers not divisible by p^2 for any prime $p \leq r$ indeed equals $\prod_{\text{prime } p \leq r}(1 - p^{-2})$, by the Chinese remainder theorem. Bounding the error amounts to bounding the upper density of the set of integers divisible by p^2 for a large prime p (that is, a prime $p > r$), i.e., showing that

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

This is easy to prove:

$$\begin{aligned}
&\#\{n \leq B : n \text{ is divisible by } p^2 \text{ for some } p > r\} \\
&\leq \sum_{\text{prime } p > r} \#\{n \leq B : n \text{ is divisible by } p^2\} \\
&= \sum_{\text{prime } p > r} \lfloor B/p^2 \rfloor \\
&\leq \sum_{\text{integers } n > r} B/n^2 \\
&\leq B \int_r^\infty \frac{1}{x^2}\, dx \\
&= B/r,
\end{aligned}$$

so if we divide by B, take the limit as $B \to \infty$, and then take the limit as $r \to \infty$, we get 0.

Thus the density of squarefree integers equals

$$\lim_{r\to\infty} \prod_{\text{prime } p \le r} (1-p^{-2}) = \prod_{\text{prime } p} (1-p^{-2}) = \zeta(2)^{-1}.$$

3. Squarefree values of polynomials

For more general problems, the hard part is in bounding the error arising from ignoring the large primes. Consider for instance the following problem: Given a polynomial $f(x) \in \mathbb{Z}[x]$, compute the density of integers n such that $f(n)$ is squarefree. The naïve heuristic above suggests that the answer should be $\prod_{\text{prime } p}(1-c_p/p^2)$ where c_p equals the number of integers $n \in [0, p^2-1]$ for which $p^2 \mid f(n)$.

For fixed r, the density of integers n satisfying the conditions for primes $\le r$ can be computed as before, by using the Chinese remainder theorem. Assuming that r exceeds the discriminant of f, if $p > r$, then Hensel's lemma shows that there are at most $\deg f$ solutions $x \bmod p^2$ to $f(x) \equiv 0 \pmod{p^2}$, so we can bound the number of integers $n \in [1, B]$ for which $p^2 | f(n)$ by $(\deg f)\lceil B/p^2 \rceil$. But $f(n)$ for $n \le B$ could be as large as (a constant times) $B^{\deg f}$, so we must consider all p up to about $B^{(\deg f)/2}$, and unfortunately the sum of $(\deg f)\lceil B/p^2 \rceil$ over these primes will be small compared to B only if $\deg f \le 2$.

Thus controlling the error is easy only if $\deg f \le 2$. A more complicated argument [Hoo67] shows that the error can be controlled and the predicted density proved correct also in the case $\deg f = 3$, but for irreducible f of degree ≥ 4, it is not yet clear whether one can prove that the conjectural density is correct (except in cases where there is an obstruction coming from a single prime, in which case the density is 0). There is only a theorem of Granville [Gra98] saying that the expected result follows from the *abc* conjecture.

4. A function field analogue

There is an obvious function field analogue of the result about the density of squarefree integers. Namely, for a fixed finite field $\mathbb{F}_q$, one can ask what fraction of elements of the polynomial ring $\mathbb{F}_q[t]$ are squarefree. In this context one defines the density of a subset $S \subseteq \mathbb{F}_q[t]$ as the limit

$$\mu(S) := \lim_{d\to\infty} \frac{\#(S \cap \mathbb{F}_q[t]_{\le d})}{\#\mathbb{F}_q[t]_{\le d}},$$

if the limit exists, where $\mathbb{F}_q[t]_{\le d}$ is the set of polynomials in $\mathbb{F}_q[t]$ of degree $\le d$.

The sieve argument works as before. One need only replace integer primes p by monic irreducible polynomials P of $\mathbb{F}_q[t]$. We find that the density of squarefree elements of $\mathbb{F}_q[t]$ equals

$$\prod_P \left(1 - q^{-2\deg P}\right),$$

which turns out to equal $1 - 1/q$, as we will explain later using zeta functions.

5. Closed points and zeta functions

To generalize, we will need to reinterpret the set of monic irreducible polynomials in $\mathbb{F}_q[t]$ in geometric terms. Namely, the following sets are in bijection:

- the set of monic irreducible polynomials of $\mathbb{F}_q[t]$,
- the set of maximal ideals of $\mathbb{F}_q[t]$, and
- the set of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbits in $\mathbb{A}^1(\overline{\mathbb{F}}_q)$.

Specifically, given a monic irreducible polynomial, one can take the ideal it generates in $\mathbb{F}_q[t]$, or one can take its set of zeros in $\mathbb{A}^1(\overline{\mathbb{F}}_q)$.

A closed point on a variety (or scheme of finite type) X over $\mathbb{F}_q$ corresponds to a maximal ideal of the affine coordinate ring of an affine open subscheme of X. The closed points of X are in bijection with the $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbits in $X(\overline{\mathbb{F}}_q)$. The degree of a closed point P is $[\kappa(P) : \mathbb{F}_q]$, where $\kappa(P)$ is the residue field of the corresponding maximal ideal: the degree equals the size of the corresponding $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbit. The zeta function of X can be defined either as an *Euler product* over closed points, or as a *generating function* for the sequence of integers $\#X(\mathbb{F}_q)$, $\#X(\mathbb{F}_{q^2})$, $\#X(\mathbb{F}_{q^3})$, ...:

$$\zeta_X(s) = Z_X(q^{-s}) := \prod_{\text{closed } P \in X} \left(1 - q^{-s \deg P}\right)^{-1} = \exp\left(\sum_{r=1}^{\infty} \frac{\#X(\mathbb{F}_{q^r})}{r} q^{-rs}\right)$$

for $\mathrm{Re}(s) > \dim X$. The power series $Z_X(T) \in \mathbb{Z}[[T]]$ is (the Taylor series of) a rational function [Dwo60], as was conjectured by A. Weil [Wei49]. The Euler product definition extends also to schemes X of finite type over $\mathbb{Z}$.

The density of squarefree elements of $\mathbb{F}_q[t]$ is $\zeta_{\mathbb{A}^1}(2)^{-1}$, as given by the product definition. The generating function definition shows that $Z_{\mathbb{A}^1}(T) = 1/(1 - qT)$, so this density equals

$$Z_{\mathbb{A}^1}(q^{-2})^{-1} = 1 - qq^{-2} = 1 - 1/q.$$

6. Smooth plane curves

We now consider a more geometric problem. What is the density of homogeneous polynomials $f \in \mathbb{F}_q[x, y, z]$ such that the plane curve $f = 0$ in $\mathbb{P}^2$ is smooth (of dimension 1)? (Density is defined as the limit as $d \to \infty$ of the fraction of the degree d homogeneous polynomials which satisfy the desired condition. We wrote "of dimension 1" to exclude the case where f is identically 0.)

Smoothness can be tested locally. Therefore we will start with all homogeneous polynomials f of degree d and sieve out, for each closed point $P \in \mathbb{P}^2$, those f for which the curve $f = 0$ has a singularity at P. The condition that $f = 0$ has a singularity at P amounts to 3 linear conditions on the Taylor coefficients of a dehomogenization $\bar{f}$ of f at P (namely, the vanishing of $\bar{f}$ and its two partial derivatives at P), and these linear conditions are over the residue

field of P. It follows that the density of f such that $f = 0$ has a singularity at P equals $q^{-3\deg P}$. This suggests the guess that the density of f defining a smooth plane curve equals

$$\prod_{\text{closed } P \in \mathbb{P}^2} \left(1 - q^{-3\deg P}\right) = \zeta_{\mathbb{P}^2}(3)^{-1}$$
$$= (1 - q^{-1})(1 - q^{-2})(1 - q^{-3}),$$

where the last equality comes from substituting $T = q^{-3}$ in

$$Z_{\mathbb{P}^2}(T)^{-1} = (1 - T)(1 - qT)(1 - q^2T).$$

Taking $q = 2$ gives $21/64$.

The guess turns out to be correct, although the proof is much more involved than the proof for squarefree integers or polynomials.

In the rest of Section 6, we will sketch the proof of the analogous result for plane curves in $\mathbb{A}^2$ over $\mathbb{F}_q$. Instead of homogeneous polynomials f, we now use $f \in \mathbb{F}_q[x, y]_{\le d}$ (i.e., arbitrary polynomials of total degree at most d). Define the density of a subset $\mathcal{P} \subseteq \mathbb{F}_q[x, y]$, as

$$\mu(\mathcal{P}) := \lim_{d\to\infty} \frac{\#\mathcal{P} \cap \mathbb{F}_q[x, y]_{\le d}}{\#\mathbb{F}_q[x, y]_{\le d}},$$

and define the upper density $\overline{\mu}(\mathcal{P})$ similarly using lim sup.

Theorem 6.1. *Let $\mathcal{P}$ be the set of $f \in k[x, y]$ such that $f = 0$ in $\mathbb{A}^2$ is smooth (by which we mean smooth of dimension 1, so $0 \notin \mathcal{P}$). Then $\mu(\mathcal{P}) = \zeta_{\mathbb{A}^2}(3)^{-1}$.*

The proof sketch will occupy the next few subsections.

6.1. **Low degree.** Given $r > 0$, define $\mathcal{P}_r$ as the set of $f \in k[x, y]$ such that $f = 0$ in $\mathbb{A}^2$ is smooth at all closed points P of $\mathbb{A}^2$ of degree $\le r$. Thus $\mathcal{P}_r$ is an approximation to $\mathcal{P}$, in which smoothness is imposed only at the low degree points.

Lemma 6.2. *We have $\mu(\mathcal{P}_r) = \prod_{\deg P\le r}(1 - q^{-3\deg P})$.*

Proof. Let $\mathfrak{m}_P \subseteq \mathbb{F}_q[x, y]$ be the maximal ideal corresponding to P. Let $I := \prod_{\deg P\le r} \mathfrak{m}_P^2$. The lemma follows from two observations:

1. The polynomial f belongs to $\mathcal{P}_r$ if and only if the image of f under
$$\mathbb{F}_q[x, y]_{\le d} \xrightarrow{\phi_d} \frac{\mathbb{F}_q[x, y]}{I} \simeq \prod_{\deg P\le r} \frac{\mathbb{F}_q[x, y]}{\mathfrak{m}_P^2}$$
is nonzero in each factor.
2. For sufficiently large d, the $\mathbb{F}_q$-linear map ϕ_d above is surjective. (Proof: Let $V_d = \mathrm{im}(\phi_d)$. Then V_{d+1} is obtained from V_d by a process independent of d, namely, $V_{d+1} = V_d + xV_d + yV_d$, so V_d strictly grows until it stabilizes, at which point V_d is the whole space $\frac{\mathbb{F}_q[x,y]}{I}$. Thus ϕ_d is surjective for $d \ge \dim_{\mathbb{F}_q} \frac{\mathbb{F}_q[x,y]}{I}$.) □

6.2. **Medium degree.** Let

$$\mathcal{Q}_r := \bigcup_d \{f \in \mathbb{F}_q[x,y]_{\le d} : \text{there exists } P \text{ with } r < \deg P \le d/3 \text{ at which } f = 0 \text{ is not smooth}\}.$$

Lemma 6.3. *We have $\overline{\mu}(\mathcal{Q}_r) \to 0$ as $r \to \infty$.*

Proof. By the argument in the final sentence of the proof of Lemma 6.2, $\mathbb{F}_q[x,y]_{\le d} \to \dfrac{\mathbb{F}_q[x,y]}{\mathfrak{m}_P^2}$ is surjective for $d \ge \dim_{\mathbb{F}_q} \dfrac{\mathbb{F}_q[x,y]}{\mathfrak{m}_P^2} = 3\deg P$. So when $\deg P \le d/3$, the fraction of elements of $\mathbb{F}_q[x,y]_{\le d}$ lying in $\mathfrak{m}_P^2$ is $q^{-3\deg P}$. Thus

$$\overline{\mu}(\mathcal{Q}_r) \le \limsup_{d\to\infty} \sum_{r<\deg P\le d/3} q^{-3\deg P},$$

which tends to 0 as $r \to \infty$ since $\sum_{\text{all closed points P}} q^{-3\deg P}$ converges (the number of closed points of degree e in $\mathbb{A}^2$ is $O(q^{2e})$). □

6.3. **High degree.** Define

$$\mathcal{R} := \bigcup_d \{f \in \mathbb{F}_q[x,y]_{\le d} : \text{there exists } P \text{ with } \deg P > d/3 \text{ at which } f = 0 \text{ is not smooth}\}.$$

Lemma 6.4. *We have $\mu(\mathcal{R}) = 0$.*

Proof. If f_0, g_1, g_2, h are chosen uniformly at random, from $\mathbb{F}_q[x,y]_{\le d}$, $\mathbb{F}_q[x,y]_{\le (d-1)/p}$, $\mathbb{F}_q[x,y]_{\le (d-1)/p}$, $\mathbb{F}_q[x,y]_{\le d/p}$, respectively, then

$$f := f_0 + xg_1^p + yg_2^p + h^p$$

is a uniform random polynomial in $\mathbb{F}_q[x,y]_{\le d}$, so we may generate f this way. The point of doing this is that by choosing f_0, g_1, g_2, h in that order, we partially decouple the partial derivatives. In particular, by bounding the number of irreducible components as we go along, we obtain as $d \to \infty$ that

(1) the probability, conditioned on a choice of f_0, that g_1 is such that $\dim\{\frac{\partial f}{\partial x} = 0\} = 1$ is $1 - o(1)$;
(2) the probability, conditioned on a choice of such f_0, g_1, that g_2 is such that $\dim\{\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0\} = 0$ is $1 - o(1)$; and
(3) the probability, conditioned on a choice of such f_0, g_1, g_2 that h is such that $\{f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0\}$ has no points of degree $> d/3$ is $1 - o(1)$ (this uses Bézout's theorem to bound the degree of the 0-dimensional subscheme in the previous item). □

6.4. **End of proof.** Now $\mathcal{P} = \mathcal{P}_r - \mathcal{Q}_r - \mathcal{R}$. As $r \to \infty$, we have

$$\begin{aligned} \mu(\mathcal{P}_r) &\to \zeta_{\mathbb{A}^2}^{-1}(3) \\ \overline{\mu}(\mathcal{Q}_r) &\to 0 \\ \mu(\mathcal{R}) &= 0, \end{aligned}$$

so $\mu(\mathcal{P}) = \zeta_{\mathbb{A}^2}^{-1}(3)$.

7. The Bertini smoothness theorem

A generalization of the argument of the previous section yields a "Bertini smoothness theorem" over finite fields.

The Bertini smoothness theorem says that if a subvariety $X \subseteq \mathbb{P}^n$ over a field k is smooth, then for a sufficiently general hyperplane $H \subset \mathbb{P}^n$, the variety $H \cap X$ is smooth too. "Sufficiently general" here means inside a Zariski dense open subset U of the dual projective space that parametrizes hyperplanes in $\mathbb{P}^n$. If k is infinite, then $U(k)$ is nonempty, so there exists a hyperplane H over k with $H \cap X$ smooth. But if k is finite, this last result can fail: it may happen that each of the finitely many hyperplanes over k is bad, tangent to X somewhere.

Katz [Kat99] asked whether the Bertini smoothness theorem over finite fields could be salvaged by allowing hypersurfaces of unbounded degree in place of hyperplanes. The closed point sieve yields such a result, and even gives an asymptotically positive fraction of good hypersurfaces of degree d, as $d \to \infty$. (The existence of a good hypersurface, for d sufficiently large and divisible by the characteristic p, was shown independently by Gabber [Gab01, Corollary 1.6].)

The result is that if X is a smooth quasiprojective subvariety of $\mathbb{P}^n$ of dimension m over $\mathbb{F}_q$, then the density of f such that $\{f = 0\} \cap X$ is smooth of dimension $m-1$ equals $\zeta_X(m+1)^{-1}$.

Perhaps surprisingly, the density is an intrinsic property of X, independent of how X is embedded in projective space. Taking $X = \mathbb{A}^1 \subseteq \mathbb{P}^1$, we recover the result that the density of squarefree polynomials in $\mathbb{F}_q[t]$ equals $\zeta_{\mathbb{A}^1}(2)^{-1}$.

Here are a few applications of the Bertini smoothness theorem and its variants:

- *Space-filling curves* (answering questions posed in [Kat99]): Given a smooth projective geometrically irreducible variety X of positive dimension over $\mathbb{F}_q$, there exists a smooth projective geometrically irreducible curve $Y \subseteq X$ passing through all the $\mathbb{F}_q$-points of X.
- *Space-avoiding varieties*: Given X as above, and an integer y satisfying $1 \leq y < \dim X$, there exists a smooth projective geometrically irreducible variety $Y \subseteq X$ of dimension y such that $Y(\mathbb{F}_q) = \emptyset$.

- *Abelian varieties as quotients of Jacobians*: For every nontrivial abelian variety A over $\mathbb{F}_q$, there is a smooth projective geometrically irreducible curve Y in A such that the induced map from the Jacobian of Y to A is surjective.
- *Brauer groups of surfaces*: Q. Liu, D. Lorenzini, and M. Raynaud [LLR05] used the Bertini smoothness theorem (and several other ingredients) to show that if X is a smooth projective geometrically irreducible surface over $\mathbb{F}_q$, then the order of $\operatorname{Br} X$ is a perfect square.

8. Extensions of the Bertini smoothness theorem

The Bertini smoothness theorem can be viewed as a statement about the probability that a random divisor in $|dA|$ is smooth as $d \to \infty$, where A is an ample divisor. A "semiample generalization" is to study random divisors in $|nA + dE|$ as $d \to \infty$, where A is ample, but E is only globally generated. Erman and Wood [EW12] prove that a statement along these lines holds, if n is sufficiently large.

The Bertini smoothness theorem also has a conjectural arithmetic analogue: If X is a quasiprojective subscheme of $\mathbb{P}^n_{\mathbb{Z}}$ that is regular of dimension m, then the density (suitably defined) of $f \in \mathbb{Z}[x_0, \ldots, x_n]$ such that $\{f = 0\} \cap X$ is regular of dimension $m - 1$ equals $\zeta_X(m+1)^{-1}$. This is proved in [Poo04] assuming the *abc* conjecture and one other conjecture, by making use of a multivariable extension [Poo03] of Granville's conditional result [Gra98] on squarefree values of polynomials. This statement implies both the finite field Bertini smoothness theorem and the fact that the squarefree integers have density $\zeta(2)^{-1}$ (take $X = \operatorname{Spec} \mathbb{Z}$ in $\mathbb{P}^0_{\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}$).

9. Whitney embedding theorems

If X is a smooth projective curve over an infinite field k, then there is a closed immersion $X \hookrightarrow \mathbb{P}^3$. To prove this, one starts with X in some large projective space $\mathbb{P}^N$, and iteratively performs projections. One shows that if $N > 3$, then composing the embedding $X \hookrightarrow \mathbb{P}^N$ with a sufficiently generic projection $\mathbb{P}^N \dashrightarrow \mathbb{P}^{N-1}$ yields an embedding $X \hookrightarrow \mathbb{P}^{N-1}$.

The analogous statement for a finite field $\mathbb{F}_q$ is false. There are some obvious obstructions to embedding a smooth curve X in $\mathbb{P}^3$. Namely, it can happen that X has more $\mathbb{F}_q$-points than $\mathbb{P}^3$ does! Even if $\#X(\mathbb{F}_q) \leq \#\mathbb{P}^3(\mathbb{F}_q)$, it could happen that X has more closed points of degree 2 than $\mathbb{P}^3$ does.

Nguyen [Ngu05] used the closed point sieve to prove that the obvious obstructions are the only ones. Namely, he proved that given a smooth curve X over $\mathbb{F}_q$ and an integer $n \geq 3$, there exists a closed immersion $X \hookrightarrow \mathbb{P}^n$ if and only if for every $e \geq 1$ the number of closed points of degree e on X is less than or equal to the number of closed points of degree e on $\mathbb{P}^n$. In fact, he also proved the higher-dimensional analogue: given a smooth variety X of dimension m and an integer $n \geq 2m + 1$, there is a closed immersion $X \hookrightarrow \mathbb{P}^n$ if and only if

the conditions on the number of closed points are satisfied. This proof was more involved than the proof of the Bertini smoothness theorem, because the conditions on homogeneous polynomials $f_0, \dots, f_n$ for the rational map $(f_0 : \cdots : f_n) \colon \mathbb{P}^N \dashrightarrow \mathbb{P}^n$ to restrict to a closed immersion $X \hookrightarrow \mathbb{P}^n$ are not local, as were the conditions defining smoothness. Nguyen had to sieve over *pairs* of closed points to get his result.

These embedding results are algebraic analogues of the *Whitney embedding theorem*, which states that every m-dimensional real manifold X can be embedded in $\mathbb{R}^{2m+1}$. (In fact, Whitney proved that $\mathbb{R}^{2m}$ suffices, but his methods for this stronger result are not algebraic, and indeed this result fails in the algebraic setting, even over infinite fields.)

10. Lefschetz pencils

One fruitful way to study a variety $X \subseteq \mathbb{P}^n$ is to choose a dominant rational map $(f : g) \colon X \dashrightarrow \mathbb{P}^1$, say defined by a pair of homogeneous polynomials $f, g \in k[x_0, \dots, x_n]$ of the same degree. The fibers (after blowing up the indeterminacy locus) form a family of hypersurface sections in X, namely $\{\lambda_1 f - \lambda_0 g = 0\} \cap X$ for $(\lambda_0 : \lambda_1) \in \mathbb{P}^1$. Ideally, questions about X can then be reduced to questions about these hypersurface sections, which are of lower dimension.

Unfortunately, even if X is smooth and the rational map is chosen generically, some of the hypersurface sections may fail to be smooth. The best one can reasonably expect is that there will be at most finitely many singular fibers, and each such fiber has the simplest kind of singularity. More precisely, $(f : g) \colon X \dashrightarrow \mathbb{P}^1$ defines a Lefschetz pencil if all of the following hold (after base extension to an algebraically closed field):

(1) The axis $f = g = 0$ intersects X transversely.
(2) All but finitely many hypersurface sections in the family are smooth.
(3) Each non-smooth hypersurface section has only one singularity, and that singularity is an ordinary double point.

Over an infinite field k, a dimension-counting argument proves the existence of Lefschetz pencils for any smooth $X \subseteq \mathbb{P}^n$: see [Kat73]. This was famously used by P. Deligne to prove the Riemann hypothesis for varieties over finite fields [Del74, Del80]: for his application, he had the freedom to enlarge the ground field if necessary, so he needed only the existence of Lefschetz pencils over an algebraic closure of a finite field.

In any case, the question remained as to whether Lefschetz pencils over k existed for varieties over k in the case where k is finite. Nguyen [Ngu05] proved such an existence result using the closed point sieve. Again, because the conditions in the definition of Lefschetz pencil are not all local, he had to sieve over pairs of closed points.

11. The Bertini irreducibility theorem

The Bertini irreducibility theorem over a field k states that if X is a geometrically irreducible subscheme $X \subseteq \mathbb{P}^n$ over k and $\dim X \geq 2$, then for a sufficiently general hyperplane $H \subset \mathbb{P}^n$, the intersection $H \cap X$ is geometrically irreducible too. But again, "sufficiently general" means inside a Zariski dense open subset U of the dual projective space, so the statement is vacuous if k is finite. Therefore it is natural again to intersect X with hypersurfaces H of degree d, and to study the density of good hypersurfaces H as $d \to \infty$.

Geometric irreducibility is not a property that can be tested analytically locally, so the closed point sieve cannot be used directly to attack this problem. Nevertheless, the following has been proved [CP13, Theorem 1.2]:

Theorem 11.1. *Let X be a geometrically irreducible subscheme of $\mathbb{P}^n_{\mathbb{F}_q}$. If $\dim X \geq 2$, then the density of f such that $\{f = 0\} \cap X$ is geometrically irreducible is 1.*

12. Questions

(1) There seems to be a general principle that if an existence result about polynomials or n-tuples of polynomials over an infinite field can be proved by dimension counting, then a corresponding result over finite fields can be proved by the closed point sieve. Can this principle be formalized and proved?
(2) The closed point sieve we have discussed is the geometric analogue of the simplest kind of sieve appearing in analytic number theory. Are there also geometric analogues of more sophisticated sieves like the *large sieve*, and do these have applications?
(3) What other theorems currently require the hypothesis "Assume that k is an infinite field"? Hopefully the closed point sieve could be used to eliminate the hypothesis in many of these.

Part 2. Selmer group heuristics

13. Selmer groups

We will work over $\mathbb{Q}$. (We could work over other number fields, or even global fields, but the main ideas are the same, with some extra technicalities or restrictions when considering p-power Selmer groups in characteristic p.) Let $G := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. For each place v of $\mathbb{Q}$, let $\mathbb{Q}_v$ be the completion (either $\mathbb{R}$ or $\mathbb{Q}_p$ for some prime p). For finite v, let $\mathbb{Z}_v$ be the valuation ring of $\mathbb{Q}_v$. The adele ring of $\mathbb{Q}$ is the restricted direct product

$$\mathbf{A} := \prod_v{}' (\mathbb{Q}_v, \mathbb{Z}_v) := \left\{ (a_v) \in \prod_v \mathbb{Q}_v : a_v \in \mathbb{Z}_v \text{ for all but finitely many } v \right\}.$$

Let E be an elliptic curve over $\mathbb{Q}$. The only known proof (up to minor variations) of Mordell's theorem that $E(\mathbb{Q})$ is finitely generated first shows that $E(\mathbb{Q})/nE(\mathbb{Q})$ is finite for some $n \geq 2$.

How is the latter done? Identify E with the G-module $E(\overline{\mathbb{Q}})$, and define $E[n]$ as the kernel in the exact sequence

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

of G-modules. The "take G-invariants" functor is only left exact, but the left exact sequence can be continued by using (profinite) group cohomology:

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

Here $\mathrm{H}^1(\mathbb{Q}, E) := \mathrm{H}^1(G, E(\overline{\mathbb{Q}}))$ and so on.[1] The long exact sequence can be contracted to

$$0 \longrightarrow \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \longrightarrow \mathrm{H}^1(\mathbb{Q}, E[n]) \longrightarrow \mathrm{H}^1(\mathbb{Q}, E). \tag{1}$$

Unfortunately $\mathrm{H}^1(\mathbb{Q}, E[n])$ is infinite, so the finiteness of $E(\mathbb{Q})/nE(\mathbb{Q})$ is not immediate. To prove the finiteness, we will constrain the image of $\dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} \to \mathrm{H}^1(\mathbb{Q}, E[n])$ by local conditions.

The sequence (1) maps to the analogous sequence over $\mathbb{Q}_v$ for each v, and we may take a product to obtain a diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} & \longrightarrow & \mathrm{H}^1(\mathbb{Q}, E[n]) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}, E) \\ & & \downarrow & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ 0 & \longrightarrow & \displaystyle\prod_v \frac{E(\mathbb{Q}_v)}{nE(\mathbb{Q}_v)} & \xrightarrow{\alpha} & \displaystyle\prod_v \mathrm{H}^1(\mathbb{Q}_v, E[n]) & \longrightarrow & \displaystyle\prod_v \mathrm{H}^1(\mathbb{Q}_v, E) \end{array} \tag{2}$$

with exact rows. Choose a model $\mathcal{E}$ of E over $\mathbb{Z}[1/N]$ for some $N \geq 1$. Then for finite $v \nmid N$, the sequence (1) has an analogue also over $\mathbb{Z}_v$. Replacing the direct products in the diagram (2) by restricted direct products yields a new diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} & \longrightarrow & \mathrm{H}^1(\mathbb{Q}, E[n]) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}, E) \\ & & \downarrow & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ 0 & \longrightarrow & \dfrac{E(\mathbf{A})}{nE(\mathbf{A})} & \xrightarrow{\alpha} & \mathrm{H}^1(\mathbf{A}, E[n]) & \longrightarrow & \mathrm{H}^1(\mathbf{A}, E), \end{array} \tag{3}$$

[1] This notation is reasonable since this is what one gets by taking cohomology of the sheaf represented by E on $(\operatorname{Spec} \mathbb{Q})_{\mathrm{et}}$.

in which the groups in the second row are *defined* as the restricted direct products. The maps α, β, γ are the same as before; only their codomains have shrunk.[2]

For an element $\xi \in \mathrm{H}^1(\mathbb{Q}, E[n])$ to be in the image of $\dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})}$, it is necessary that its localization in $\mathrm{H}^1(\mathbf{A}, E[n])$ be in the image of α. The set of ξ satisfying this necessary condition is called the n-Selmer group:

$$\mathrm{Sel}_n E := \beta^{-1}(\operatorname{im}\alpha) \subseteq \mathrm{H}^1(\mathbb{Q}, E[n]).$$

(Warning: $\mathrm{Sel}_n E$ is *not* the subgroup of locally trivial elements of $\mathrm{H}^1(\mathbb{Q}, E[n])$.) The group $\mathrm{Sel}_n E$ is an upper bound for the image of $\dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})}$. Using finiteness theorems of algebraic number theory (finiteness of the class group, and the finite generation of the unit group), one shows that $\mathrm{Sel}_n E$ is finite, and computable in principle.

Also define the Shafarevich–Tate group

$$Ш = Ш(E) := \ker\gamma.$$

14. Distribution questions

Let $\mathscr{E}$ be the set of all elliptic curves over $\mathbb{Q}$, ordered by "height" defined in some way (e.g., the height of E could be defined as the minimum value of $\max(|A|^3, |B|^2)$ over all Weierstrass models $y^2 = x^3 + Ax + B$ for E with $A, B \in \mathbb{Z}$). Let $\mathscr{E}_{<X} := \{E \in \mathscr{E} : h(E) < X\}$. An event is a subset S of $\mathscr{E}$, and its "probability" (or density) is

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

if the limit exists.

We are interested in the distribution of the rank of $E(\mathbb{Q})$, the group $\mathrm{Sel}_n E$, and the group $Ш(E)$, as E varies. For instance, given a prime p, we can ask, for each $s \in \mathbb{Z}_{\geq 0}$, what is $\mathrm{Prob}(\dim \mathrm{Sel}_p E = s)$? We will motivate a conjecture that $\mathrm{Sel}_p E$ behaves like the intersection of two maximal isotropic subspaces in a hyperbolic quadratic space of large dimension (we will explain below what all this means).

15. Maximal isotropic subspaces

Equip the vector space $V := \mathbb{F}_p^{2n}$ with the quadratic form

$$Q(x_1, \ldots, x_n, y_1, \ldots, y_n) := x_1y_1 + \cdots + x_ny_n.$$

[2]Suppose that $p \nmid N$. The valuative criterion for properness gives $\mathcal{E}(\mathbb{Z}_p) = E(\mathbb{Q}_p)$. Any torsor T of $\mathcal{E}_{\mathbb{Z}_p}$ is smooth over $\mathbb{Z}_p$; the special fiber $T_{\mathbb{F}_p}$ has an $\mathbb{F}_p$-point by Lang's theorem on the triviality of torsors under a connected algebraic group over a finite field; this $\mathbb{F}_p$-point lifts to a $\mathbb{Z}_p$-point, by Hensel's lemma, so T is trivial. Thus $\dfrac{E(\mathbf{A})}{nE(\mathbf{A})} = \prod_v \dfrac{E(\mathbb{Q}_v)}{nE(\mathbb{Q}_v)}$ and $\mathrm{H}^1(\mathbf{A}, E) = \bigoplus_v \mathrm{H}^1(\mathbb{Q}_v, E)$.

Any quadratic space isomorphic to this one is called a hyperbolic quadratic space. Associated to Q is the symmetric bilinear pairing $\langle\ ,\ \rangle\colon V \times V \to \mathbb{F}_p$ defined by

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

Given a subspace $Z \leq V$, define

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

Call Z isotropic if $Q|_Z = 0$. Call Z maximal isotropic if $Q|_Z = 0$ and $Z = Z^\perp$; every such Z has dimension n, half that of V. For example, $\{(x_1, \ldots, x_n, 0, \ldots, 0) : x_1, \ldots, x_n \in \mathbb{F}_p\}$ is a maximal isotropic subspace. Let $\mathrm{OGr}_n(\mathbb{F}_p)$ be the set of all maximal isotropic Z in V. (If $\mathrm{Gr}_{n,m}$ denotes the usual Grassmannian parametrizing n-dimensional subspaces of a given m-dimensional space, then $\mathrm{OGr}_n(\mathbb{F}_p) \subseteq \mathrm{Gr}_{n,2n}(\mathbb{F}_p)$; the O is for orthogonal.)

Choose $Z, W \in \mathrm{OGr}_n(\mathbb{F}_p)$ uniformly at random, and examine the distribution of $\dim(Z \cap W) \in \mathbb{Z}_{\geq 0}$. One can show that this distribution converges to a discrete probability distribution on $\mathbb{Z}_{\geq 0}$ as $n \to \infty$. (Recall that $2n$ was $\dim V$.)

Conjecture 15.1 ([PR12, Conjecture 1.1(a)])**.** The distribution of $\mathrm{Sel}_p E$ for $E \in \mathscr{E}$ matches the limiting distribution above. That is, for each $s \in \mathbb{Z}_{\geq 0}$,

$$\mathrm{Prob}(\dim \mathrm{Sel}_p E = s) = \lim_{n\to\infty} \mathrm{Prob}(\dim(Z \cap W) = s).$$

Remark 15.2. Conjecture 15.1 was inspired by a result of Heath-Brown. Define $s(E) := \dim_{\mathbb{F}_2} \mathrm{Sel}_2 E - \dim_{\mathbb{F}_2} E[2](\mathbb{Q})$. Heath-Brown [HB93, HB94] proved that as E varies over quadratic twists of $y^2 = x^3 - x$ over $\mathbb{Q}$,

$$\mathrm{Prob}(s(E) = s) = \prod_{j\geq 0}(1 + 2^{-j})^{-1} \prod_{j=1}^{s} \frac{2}{2^j - 1}.$$

The authors of [PR12] intuited that there should be not be so many distributions on nonnegative integers arising naturally as the dimension of a random $\mathbb{F}_2$-vector space. After trying various linear algebra constructions, they found the one above that produced the same distribution.

16. Evidence in the arithmetic of elliptic curves

But *why* should $\mathrm{Sel}_p E$ behave like the intersection of random maximal isotropic subspaces? It turns out that $\mathrm{Sel}_p E$ actually *is* an intersection of maximal isotropic subspaces, in an *infinite-dimensional* quadratic space! The goal of this section is to explain this.

For simplicity, we will assume that p is odd, so that quadratic forms correspond bijectively to symmetric bilinear forms. (We already showed how to pass from Q to $\langle\ ,\ \rangle$. To go back, define $Q(v) := \frac{1}{2}\langle v, v\rangle$.)

16.1. **Elliptic curves over local fields.** Let $\mathbb{Q}_v$ be a completion of $\mathbb{Q}$. Let $G_v := \mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v)$. Let $\mathbb{G}_m$ be the multiplicative group over $\mathbb{Q}_v$; the corresponding G_v-module is $\overline{\mathbb{Q}}_v^\times$. Then $\mathrm{H}^2(\mathbb{Q}_v, \mathbb{G}_m)$ is the Brauer group of $\mathbb{Q}_v$, which injects into $\mathbb{R}/\mathbb{Z}$. (In fact, the Brauer group is $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if $v = \infty$, and $\mathbb{Q}/\mathbb{Z}$ if v is finite.)

Let E be an elliptic curve over $\mathbb{Q}_v$. Let $V_v := \mathrm{H}^1(\mathbb{Q}_v, E[p])$, which is a finite-dimensional $\mathbb{F}_p$-vector space. The Weil pairing

$$e\colon E[p] \times E[p] \to \mathbb{G}_m$$

induces a cup product pairing

$$\langle\ ,\ \rangle_v\colon V_v \times V_v \xrightarrow{\cup} \mathrm{H}^2(\mathbb{Q}_v, E[p] \otimes E[p]) \xrightarrow{e} \mathrm{H}^2(\mathbb{Q}_v, \mathbb{G}_m) \hookrightarrow \mathbb{R}/\mathbb{Z}.$$

The map $\cup$ is alternating ($\alpha \cup \beta = -\beta \cup \alpha$), but so is e, so $\langle\ ,\ \rangle$ is a *symmetric* bilinear pairing. Let $q_v\colon V_v \to \mathbb{R}/\mathbb{Z}$ be the associated quadratic form.

Let W_v be the image of $\dfrac{E(\mathbb{Q}_v)}{pE(\mathbb{Q}_v)} \hookrightarrow \mathrm{H}^1(\mathbb{Q}_v, E[p]) = V_v$. It turns out that W_v coincides with $\mathrm{H}^1(\mathbb{Z}_v, \mathcal{E}[p])$ if $\mathcal{E}$ is a smooth model over $\mathbb{Z}_v$ and $v \nmid p$. Also, W_v is maximal isotropic because of Tate local duality, and the analogous facts hold even if $p = 2$: see [O'N02, Proposition 2.3]. The existence of a maximal isotropic subspace implies that (V_v, q_v) is a *hyperbolic* quadratic space.

16.2. **Elliptic curves over a global field.** Now suppose that E is an elliptic curve over $\mathbb{Q}$. For every place v of $\mathbb{Q}$, form $V_v := \mathrm{H}^1(\mathbb{Q}_v, E[p])$ as above. Let $V := \prod_v (V_v, W_v) \simeq \mathrm{H}^1(\mathbf{A}, E[p])$. Then $Q := \sum_v q_v\colon V \to \mathbb{R}/\mathbb{Z}$ is well-defined.

Recall from (3) the maps

$$\begin{array}{ccc} & & \mathrm{H}^1(\mathbb{Q}, E[p]) \\ & & \Big\downarrow{\scriptstyle \beta} \\ \dfrac{E(\mathbf{A})}{pE(\mathbf{A})} & \xrightarrow{\alpha} & \mathrm{H}^1(\mathbf{A}, E[p]) = V. \end{array}$$

Theorem 16.1.

(a) $\mathrm{im}(\alpha)$ *and* $\mathrm{im}(\beta)$ *are maximal isotropic.*
(b) β *is injective.*
(c) $\mathrm{im}(\alpha) \cap \mathrm{im}(\beta) = \beta(\mathrm{Sel}_p E) \simeq \mathrm{Sel}_p E$.

Sketch of proof. Here we will only list the ingredients of the proof.

(a) The space $\mathrm{im}(\alpha)$ is $\prod_v W_v$, so it is maximal isotropic. That $\mathrm{im}(\beta)$ is isotropic is a consequence of global duality, specifically the exactness in the middle of the 9-term Poitou–Tate exact sequence. (If $p = 2$, one uses also the reciprocity law for the Brauer group.)

(b) Injectivity of β follows from the Chebotarev density theorem and the fact that the Sylow p-subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ is cyclic! (The injectivity is delicate: it can fail if p is replaced by a power of p, or if E is replaced by a higher-dimensional abelian variety.)
(c) The first equality is the definition of Sel_p. The second equality is the injectivity of β. □

17. The p^∞-Selmer group

From (3) one can extract a short exact sequence

$$0 \longrightarrow \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \longrightarrow \mathrm{Sel}_n E \longrightarrow Ш[n] \longrightarrow 0.$$

Setting $n = p^e$ and taking the direct limit over e yields a short exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty} E \longrightarrow Ш[p^\infty] \longrightarrow 0 \tag{Seq_E}$$

in which each term is a $\mathbb{Z}_p$-module of the form $\left(\frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)^s \oplus F$ for some $s \in \mathbb{Z}_{\geq 0}$ and finite abelian p-group F. Knowing the distribution of (Seq_E) among isomorphism types of short exact sequences of $\mathbb{Z}_p$-modules would be much better than knowing just the distribution of $\dim \mathrm{Sel}_p$, because (Seq_E) contains information also about the rank of $E(\mathbb{Q})$ and about Ш.

18. The orthogonal Grassmannian

In Section 15, we defined $\mathrm{OGr}_n(\mathbb{F}_p) \subseteq \mathrm{Gr}_{n,2n}(\mathbb{F}_p)$ using the standard hyperbolic quadratic form Q.

Now replace $\mathbb{F}_p$ by an arbitrary commutative ring A. For any $n \leq m$, the Grassmannian $\mathrm{Gr}_{n,m}$ is a smooth projective scheme over $\mathbb{Z}$ such that

$$\mathrm{Gr}_{n,m}(A) = \{\text{locally free rank } n \text{ } A\text{-submodules } Z \leq A^m : Z \text{ is a direct summand}\}$$

functorially in A, so define

$$\mathrm{OGr}_n(A) := \{Z \in \mathrm{Gr}_{n,2n}(A) : Q|_Z = 0\}.$$

It turns out that OGr_n is a smooth projective scheme over $\mathbb{Z}$ with two connected components [SGA 7_{II}, XII, Proposition 2.8]. A classical fact, valid over any field k, states that $Z, Z' \in \mathrm{OGr}_n(k)$ lie in the same component if and only if $\dim(Z \cap Z') \equiv n \pmod 2$.

By smoothness, the fibers of $\mathrm{OGr}_n(\mathbb{Z}/p^{e+1}\mathbb{Z}) \to \mathrm{OGr}_n(\mathbb{Z}/p^e\mathbb{Z})$ have constant size, so the uniform probability measures on these finite sets induce a probability measure on the inverse limit

$$\mathrm{OGr}_n(\mathbb{Z}_p) = \varprojlim_e \mathrm{OGr}_n(\mathbb{Z}/p^e\mathbb{Z}).$$

19. Model

Let $V := \mathbb{Z}_p^{2n}$. There is no interesting information in the choice of *one* element of $\mathrm{OGr}_n(\mathbb{Z}_p)$, since it turns out that the orthogonal group $\mathrm{O}_{2n}(\mathbb{Z}_p)$ of Q acts transitively on $\mathrm{OGr}_n(\mathbb{Z}_p)$. Therefore we choose *two*. One of them might as well be $W := \mathbb{Z}_p^n \times \{0\}$; the other one, Z, we sample at random from $\mathrm{OGr}_n(\mathbb{Z}_p)$. Form the random short exact sequence

$$0 \longrightarrow \underbrace{(Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}}_{R} \longrightarrow \underbrace{\left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)}_{S} \longrightarrow T \longrightarrow 0$$

which defines R and S as shown, and then $T := S/R$.

Theorem 19.1 ([BKL+13, Theorem 1.2])**.** *The limit as $n \to \infty$ of the distribution of $0 \to R \to S \to T \to 0$ exists.*

Conjecture 19.2 ([BKL+13, Conjecture 1.3])**.** The limit distribution equals the distribution of Seq_E for $E \in \mathscr{E}$.

Loosely speaking, the conjecture is that R models the rank (or rational points), S models the Selmer group, and T models the Tate–Shafarevich group.

20. Consequences of the conjecture

20.1. **Consequences for rank.** Let $Z_{\mathbb{Q}_p} := Z \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and so on. We have

$$(Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} = \left(\frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)^r$$

where

$$r := \dim_{\mathbb{Q}_p}(Z_{\mathbb{Q}_p} \cap W_{\mathbb{Q}_p}) \approx \begin{cases} 0, & \text{for } Z \text{ in one component of } \mathrm{OGr}_n, \\ 1, & \text{for } Z \text{ in the other component of } \mathrm{OGr}_n, \end{cases}$$

where $\approx$ means "equal for Z outside a lower-dimensional locus". (The set of $\mathbb{Z}_p$-points of a lower-dimensional locus has measure 0.)

Corollary 20.1. *Conjecture 19.2 implies that* 50% *of elliptic curves have rank* 0 *and* 50% *of elliptic curves have rank* 1.

20.2. **Consequences for Sel_{p^e}.** Fix a prime p. By the Hilbert irreducibility theorem, $E[p](\mathbb{Q}) = 0$ for 100% of elliptic curves E. In this case, one can show that $\mathrm{Sel}_{p^e} E = (\mathrm{Sel}_{p^\infty} E)\,[p^e]$.

Corollary 20.2. *Conjecture 19.2 implies that the distribution of $\mathrm{Sel}_{p^e} E$ for $E \in \mathscr{E}$ is the limit as $n \to \infty$ of the distribution of $Z \cap W$ for random $Z, W \in \mathrm{OGr}_n(\mathbb{Z}/p^e\mathbb{Z})$.*

In particular, Conjecture 19.2 is compatible with Conjecture 15.1. Corollary 20.2 is compatible also with the theorems of Bhargava and Shankar [BS13a, BS13b, BS13c, BS13d] on the average size of $\mathrm{Sel}_{p^e} E$ for $p^e \leq 5$.

20.3. **Consequences for Ш.** In the model, elementary group theory shows that R is always the maximal divisible subgroup of S, and T is always finite.

Corollary 20.3. *Conjecture 19.2 implies that* $Ш[p^\infty]$ *is finite for* 100% *of elliptic curves.*

When speaking of Shafarevich–Tate groups, it is natural to condition on the rank of $E(\mathbb{Q})$. There are *three* descriptions of a distribution supported on the set of finite abelian p-groups $\mathcal{G}$, each conjectured to be the distribution of $Ш[p^\infty]$ as E varies over elliptic curves of rank r!

1. Delaunay [Del01, Del07, DJ13], in analogy with the Cohen–Lenstra heuristics for class groups [CL84], proposed the distribution in which $\mathcal{G}$ occurs with probability
$$\frac{\#\mathcal{G}^{1-r}}{\#\operatorname{Aut}(\mathcal{G}, [\ ,\ ])} \prod_{i=r+1}^{\infty} \left(1 - p^{1-2i}\right),$$
where $[\ ,\ ] := \mathcal{G} \times \mathcal{G} \to \mathbb{Q}_p/\mathbb{Z}_p$ denotes any nondegenerate alternating pairing (if no such $[\ ,\ ]$ exists, the probability should be 0).
2. The paper [BKL+13] proposes the limit as $n \to \infty$ of the distribution of
$$\operatorname{coker}(A\colon \mathbb{Z}_p^{2n+r} \to \mathbb{Z}_p^{2n+r})_{\mathrm{tors}}$$
for a random $A \in \mathrm{M}_{2n+r}(\mathbb{Z}_p)$ such that $A^T = -A$ and $\operatorname{rank} A = 2n$. This is analogous to the Friedman–Washington interpretation [FW89] of the Cohen–Lenstra heuristics for class groups.
3. Conjecture 19.2 suggests the limit as $n \to \infty$ of the distribution of the group T in the model, when Z is sampled from the locus in $\mathrm{OGr}_n(\mathbb{Z}_p)$ where $\operatorname{rank}(Z \cap W) = r$. (Strictly speaking, this sampling makes sense only for $r = 0, 1$, the problem being that the locus has measure 0 if $r \geq 2$. But there is a natural variant of Conjecture 19.2 involving a probability measure supported on that locus for each $r \geq 2$.)

Happily, the three distributions coincide for each $r \geq 0$ [BKL+13, Theorems 1.6 and 1.10].

References

[BKL+13] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra jr., Bjorn Poonen, and Eric Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, August 6, 2013. Preprint, `arXiv:1304.3971v2`. ↑(document), 19.1, 19.2, 2, 20.3

[BS13a] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, December 23, 2013. Preprint, `arXiv:1006.1002v3`, to appear in *Annals of Math.* ↑20.2

[BS13b] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0, December 24, 2013. Preprint, `arXiv:1007.0052v2`. ↑20.2

[BS13c] ———, *The average number of elements in the 4-Selmer groups of elliptic curves is 7*, December 27, 2013. Preprint, `arXiv:1312.7333v1`. ↑20.2

[BS13d] ———, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, December 30, 2013. Preprint, `arXiv:1312.7859v1`. ↑20.2

[CP13] François Charles and Bjorn Poonen, *Bertini irreducibility theorems over finite fields*, November 27, 2013. Preprint, available at `http://www-math.mit.edu/~poonen/papers/bertini_irred.pdf`. ↑11

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, DOI 10.1007/BFb0099440. MR756082 (85j:11144) ↑1

[Del01] Christophe Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196. MR1837670 (2003a:11065) ↑1

[Del07] ———, *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 323–340. MR2322355 (2008i:11089) ↑1

[DJ13] Christophe Delaunay and Frédéric Jouhet, *p^ℓ-torsion points in finite abelian groups and combinatorial identities*, March 31, 2013. Preprint, `arXiv:1208.6397v2`. ↑1

[Del74] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307 (French). MR0340258 (49 #5013) ↑10

[Del80] ———, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252 (French). MR601520 (83c:14017) ↑10

[Dwo60] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. MR0140494 (25 #3914) ↑5

[EW12] Daniel Erman and Melanie Matchett Wood, *Semiample Bertini theorems over finite fields*, September 24, 2012. Preprint, `arXiv:1209.5266v1`. ↑8

[FW89] Eduardo Friedman and Lawrence C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239. MR1024565 (91e:11138) ↑2

[Gab01] O. Gabber, *On space filling curves and Albanese varieties*, Geom. Funct. Anal. **11** (2001), no. 6, 1192–1200. MR1878318 (2003g:14034) ↑7

[Gra98] Andrew Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices **19** (1998), 991–1009. MR1654759 (99j:11104) ↑3, 8

[HB93] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), no. 1, 171–195, DOI 10.1007/BF01231285. MR1193603 (93j:11038) ↑15.2

[HB94] ———, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370, DOI 10.1007/BF01231536. With an appendix by P. Monsky. MR1292115 (95h:11064) ↑15.2

[Hoo67] C. Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21–26. MR0214556 (35 #5405) ↑3

[Kat73] Nicholas M. Katz, *Pinceaux de Lefschetz: théorème d'existence*, Groupes de monodromie en géométrie algébrique. II, Springer-Verlag, Berlin. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II); Dirigé par P. Deligne et N. Katz, Lecture Notes in Mathematics, Vol. 340, Exposé XVII, 1973, pp. 212–253. ↑10

[Kat99] ———, *Space filling curves over finite fields*, Math. Res. Lett. **6** (1999), no. 5-6, 613–624. MR1739219 (2001e:11067) ↑7

[LLR05] Qing Liu, Dino Lorenzini, and Michel Raynaud, *On the Brauer group of a surface*, Invent. Math. **159** (2005), no. 3, 673–676. MR2125738 ↑7

[Ngu05] Nghi Huu Nguyen, *Whitney theorems and Lefschetz pencils over finite fields*, May 2005. Ph.D. thesis, University of California at Berkeley. ↑9, 10

[O'N02] Catherine O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory **95** (2002), no. 2, 329–339, DOI 10.1016/S0022-314X(01)92770-2. Erratum in *J. Number Theory* **109** (2004), no. 2, 390. MR1924106 (2003f:11079) ↑16.1

[Poo03] Bjorn Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J. **118** (2003), no. 2, 353–373. MR1980998 (2004d:11094) ↑8

[Poo04] ———, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127. MR2144974 (2006a:14035) ↑(document), 8

[Poo07] ———, *Sieve methods for varieties over finite fields and arithmetic schemes*, J. Théor. Nombres Bordeaux **19** (2007), no. 1, 221–229 (English, with English and French summaries). MR2332063 (2008d:11061) ↑(document)

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269, DOI 10.1090/S0894-0347-2011-00710-8. MR2833483 ↑(document), 15.1, 15.2

[SGA 7_{II}] *Groupes de monodromie en géométrie algébrique. II*, Lecture Notes in Mathematics, Vol. 340, Springer-Verlag, Berlin, 1973 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II); Dirigé par P. Deligne et N. Katz. MR0354657 (50 #7135) ↑18

[Wei49] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR0029393 (10,592e) ↑5

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/