How to Count with Topology

Jordan S. Ellenberg
University of Wisconsin-Madison

AMS-MAA Joint Mathematics Meetings
January 11, 2013

Counting squarefree integers

How many squarefree integers are there? (That is: how many integers with no square divisor other than 1?)

Counting squarefree integers

How many squarefree integers are there? (That is: how many integers with no square divisor other than 1?)

Boring answer: *infinitely many.*

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, \ldots$$

Counting squarefree integers

Better question: How many squarefree integers are there between N and $2N$? Call this function $sf(N)$.

Counting squarefree integers

Better question: How many squarefree integers are there between N and $2N$? Call this function $sf(N)$.

```
sage: len([x for x in range(1000,2000)
if Integer(x).is_squarefree()])
607
```

Counting squarefree integers

Better question: How many squarefree integers are there between N and $2N$? Call this function $sf(N)$.

$$\begin{aligned} sf(10) &= 7 \\ sf(100) &= 61 \\ sf(1000) &= 607 \\ sf(10000) &= 6077 \\ sf(100000) &= 60787 \end{aligned}$$

Counting squarefree integers

Better question: How many squarefree integers are there between N and $2N$? Call this function $sf(N)$.

$$\begin{aligned} sf(10) &= 7 \\ sf(100) &= 61 \\ sf(1000) &= 607 \\ sf(10000) &= 6077 \\ sf(100000) &= 60787 \end{aligned}$$

Looks like:

> *The probability that a random integer is squarefree is about 61%.*

Counting squarefree integers

Heuristic (can be made rigorous):
The probability that n is squarefree is the probability that it is not divisible by 4, and not divisible by 9, and not divisible by 25, and ...

$$\begin{aligned} &= (1-1/4)(1-1/9)(1-1/25)\dots \\ &= \prod_p (1-p^{-2}) = \zeta(2)^{-1} = 6/\pi^2 = 0.6079\dots \end{aligned}$$

This is an actual theorem: $\lim_{N\to\infty} N^{-1} sf(N) = \zeta(2)^{-1}$.

Indeed, $sf(N) = \zeta(2)^{-1}N + O(\sqrt{N})$.

Where's the topology?

Time-honored analogy:

- The ring $\mathbb{Z}$ of integers;
- The ring $k[t]$ of polynomials over a field (e.g. the complex numbers)

Both are *Dedekind domains* (commutative Noetherian integrally closed domains in which every nonzero prime ideal is maximal) – it turns out that many algebraic facts about $\mathbb{Z}$ are in fact general theorems about Dedekind domains.

But the theory of complex polynomials clearly encounters topology in a way that integer arithmetic (on its face) does not.

God defeats the devil

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

God defeats the devil

Theme: problems of **arithmetic statistics** over $\mathbb{Z}$ (you just missed a special session about this! But see Wei Ho's talk in the Current Events session) are analogous to problems about **topology and geometry of moduli spaces** over $\mathbb{C}[t]$.

God defeats the devil

Theme: problems of **arithmetic statistics** over $\mathbb{Z}$ (you just missed a special session about this! But see Wei Ho's talk in the Current Events session) are analogous to problems about **topology and geometry of moduli spaces** over $\mathbb{C}[t]$.

But when k is a **finite** field $\mathbb{F}_q$, **these problems retain both arithmetic aspects and geometric aspects.**

Numbers and polynomials

Z	k[t]
± 1 (units in $\mathbb{Z}$)	$k^\times$ (units in $k[t]$)
squarefree integers	squarefree polynomials
positive integers	monic polynomials
primes	monic irreducible polynomials
absolute value $n \to \lvert n \rvert$	absolute value $P \to c^{\deg P}$

Counting squarefree polynomials

Let $\mathbb{F}_q$ be a finite field of odd characteristic.

Analogue of $[N, 2N]$: the set of monic polynomials of degree n.

There are q^n of these, so think of N as q^n.

> *What is the probability that a degree-n monic polynomial over $\mathbb{F}_q$ is squarefree?*

Counting squarefree polynomials

Let $\mathbb{F}_q$ be a finite field of odd characteristic.

Analogue of $[N, 2N]$: the set of monic polynomials of degree n.

There are q^n of these, so think of N as q^n.

> *What is the probability that a degree-n monic polynomial over $\mathbb{F}_q$ is squarefree?*

Answer: $1 - 1/q$.
(this can be proved by elementary combinatorics – but see Vakil-Wood 2012 to see the motivic apotheosis of this approach!)

Counting squarefree polynomials

Why is $1 - 1/q$ "the same answer" as $6/\pi^2$?

Counting squarefree polynomials

Why is $1 - 1/q$ "the same answer" as $6/\pi^2$?

Because

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

Counting squarefree polynomials

Why is $1 - 1/q$ "the same answer" as $6/\pi^2$?

Because

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

and

$$\zeta_{\mathbb{F}_q[x]}(2)^{-1} = \prod_{P \text{ irreducible}} \left(1 - \frac{1}{q^{2deg P}}\right) = 1 - 1/q$$

Cohen-Lenstra problem

Every number field K has an *class group* $\mathrm{Cl}(K)$, a finite abelian group measuring its failure to satisfy unique factorization.
Question: What does the class group of a random number field look like?

Cohen-Lenstra problem

Every number field K has an *class group* $\mathrm{Cl}(K)$, a finite abelian group measuring its failure to satisfy unique factorization.
Question: What does the class group of a random number field look like?

d	10001	10002	10003	10005	10006
$\lvert\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))\rvert$	160	64	12	64	86
	10007	10009	10010	10011	10013
	77	96	96	24	96
	10014	10015	10018	10019	10021
	60	54	36	30	52

Cohen-Lenstra problem

Every number field K has an *class group* $\mathrm{Cl}(K)$, a finite abelian group measuring its failure to satisfy unique factorization.
Question: What does the class group of a random number field look like?

d	10001	10002	10003	10005	10006
$\lvert\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))\rvert$	160	64	12	64	86
	10007	10009	10010	10011	10013
	77	96	96	24	96
	10014	10015	10018	10019	10021
	60	54	36	30	52

We know $\lvert\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))\rvert$ is around $\sqrt{d}$ (Brauer-Siegel) and what powers of 2 divide it (genus theory.)
Other than that, is it a "random number?"

Cohen-Lenstra problem

Every number field K has an *class group* $\mathrm{Cl}(K)$, a finite abelian group measuring its failure to satisfy unique factorization.
Question: What does the class group of a random number field look like?

d	10001	10002	10003	10005	10006
$\lvert\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))\rvert$	160	64	12	64	86
	10007	10009	10010	10011	10013
	77	96	96	24	96
	10014	10015	10018	10019	10021
	60	54	36	30	52

9 out of 15 divisible by 3.
2304 out of the 6077 class numbers with d between 10000 and 20000 are divisible by 3: about 38%.

Cohen-Lenstra problem

38% – that sounds like about
$1 - (1 - 1/3)(1 - 1/9)(1 - 1/27)(1 - 1/81)\ldots!$

In fact, Cohen and Lenstra (1983) make an audacious conjecture asserting that the maximal p-torsion subgroup of the class group of a random quadratic field converges to a limiting distribution. When K is an imaginary quadratic field, Cohen and Lenstra predict:

- **a.** For all odd primes p, the probability that $|\mathrm{Cl}(K)|$ is not a multiple of p is $(1-1/p)(1-1/p^2)(1-1/p^3)\ldots$
- **b.** For all odd primes p, the number of elements of exact order p in $\mathrm{Cl}(K)$ is, on average, 1.

a is not known in any case.

b is known only for $p = 3$ (Davenport-Heilbronn.)

Now (2012) with explicit error terms! (Bhargava-Shankar-Tsimerman, Thorne-Taniguchi, Y. Zhao in the function field case)

Theorem: (Ellenberg,Venkatesh,Westerland 2009+2012) The Cohen-Lenstra conjecture is true (in the sense of **b.**, and more general averages) over $\mathbb{F}_q[x]$, for *all* odd p and for *all* finite fields $\mathbb{F}_q$ which are sufficiently large relative to p and have characteristic prime to $2p$.

EVW 09: "Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields," arXiv:0912.0325
EVW 12: "Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, II," arXiv:1212.0923

Theorem: (Ellenberg,Venkatesh,Westerland 2009+2012) The Cohen-Lenstra conjecture is true (in the sense of **b.**, and more general averages) over $\mathbb{F}_q[x]$, for *all* odd p and for *all* finite fields $\mathbb{F}_q$ which are sufficiently large relative to p and have characteristic prime to $2p$.

EVW 09: "Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields," arXiv:0912.0325
EVW 12: "Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, II," arXiv:1212.0923

(Following work of Friedman-Washington, JK Yu, Achter,...)

Typical consequence:

> *The number of nontrivial* 5*-torsion points on the Jacobian of a random hyperelliptic curve over* $\mathbb{F}_q$ *is, on average,* 1.

The other side of the bridge

Bad question: How many monic squarefree *complex* polynomials are there of degree n?

The other side of the bridge

Bad question: How many monic squarefree *complex* polynomials are there of degree n?

OK but uninteresting question: What is the probability that a random monic degree n polynomial is squarefree?
(The answer is 1; Two roots have probability 0 of coinciding!)

The other side of the bridge

Bad question: How many monic squarefree *complex* polynomials are there of degree n?

OK but uninteresting question: What is the probability that a random monic degree n polynomial is squarefree?
(The answer is 1; Two roots have probability 0 of coinciding!)

Good question: What is the *topology* (specifically: the *cohomology with rational coefficients*) of the **space** of monic squarefree polynomials of degree n?

Weil's great insight – when a space X can be defined over both $\mathbb{F}_q$ and $\mathbb{C}$ (technically – when the space can be thought of as a scheme over $\operatorname{Spec}\mathbb{Z}$) – then the behavior of the number $|X(\mathbb{F}_q)|$ "remembers" the topology of the complex manifold $X(\mathbb{C})$.

$$\{(x, y) \in C^2 : y^2 = x^6 + x + 1\}$$

describes a genus 2 surface; this places constraints on the number

$$|\{(x, y) \in \mathbb{F}_q^2 : y^2 = x^6 + x + 1\}|$$

Definition: $\mathrm{Conf}^n(\mathbb{C})$, the *degree-n configuration space of* $\mathbb{C}$, is the space of squarefree polynomials of degree n. Alternately: the space of unordered n-tuples of *distinct* complex numbers, via the bijection

$$f(T) = (T - z_1)(T - z_2)\dots(T - z_n) \mapsto \{z_1, \dots, z_n\}$$

The configuration space Conf^2 is homeomorphic to $\mathbb{C} \times (\mathbb{C} - 0)$:

$$\{z_1, z_2\} \mapsto (z_1 + z_2, (z_1 - z_2)^2)$$

and up to homotopy, Conf^2 is a circle.

The space Conf^n is n-dimensional and more and more topologically complicated as n grows; but from the point of view of rational cohomology it is beautifully simple. A theorem of Arnol'd (1969):

> *The rational cohomology of* Conf^n *is* **stable** *for* $n \geq 2$*; it always looks like that of a circle.*

It follows (after many hidden technicalities) that

> *The proportion of monic irreducible degree-n polynomials which are squarefree is* **constant** *for* $n \geq 2$*; it is always* $1 - 1/q$.

Geometric analytic number theory

- **N:** A classical problem of analytic number theory: counting problem pertaining to $\mathbb{Z}$.
- **F:** The function-field analogue of the classical problem: counting problem pertaining to $\mathbb{F}_q[T]$.
- **T:** The geometric analogue of the function field problem: topology problem, computing the cohomology of a family of *moduli spaces* over $\mathbb{C}$.

Theorems in **T** yield theorems in **F** yield conjectures (and hopefully insights) in **N**.

Wonderfully, the topological counterparts to popular conjectures in arithmetic statistics turn out to be statements of **stable cohomology**, a hugely active subfield of topology! (Notably: Madsen-Weiss proof of the Mumford conjecture)

Arithmetic problem	moduli space
Counting squarefrees	configuration space of unordered points
Cohen-Lenstra for p-torsion in class group	moduli of hyperelliptic curves with p-level structure (a kind of Hurwitz space)
Counting degree-d number fields	classical Hurwitz spaces of d-gonal curves

Arithmetic problem	moduli space
Variation of Selmer groups (Poonen-Rains, Klagsbrun-Mazur-Rubin, Bhargava-Shankar – see W Ho at 1!)	moduli spaces of elliptic surfaces
Batyrev-Manin conjecture	spaces of rational curves on Fano varieties
prime number theorem	*representation stability* for configuration space of *ordered* points (in the FI-module sense of Church,E,Farb)

Topology as conjecture machine

We don't know everything about the topological side, but we know a lot – and this gives us a principled way to make geometrically motivated conjectures in arithmetic statistics.

In this way we reproduce many existing conjectures in number theory (Cohen-Lenstra, Malle-Bhargava, Boston-Bush-Hajir...)

But sometimes the geometry doesn't agree with existing conjectures: e.g. the geometric picture suggests that when F is a field containing cube roots of unity, the average *square* of the number of 3-torsion points in the class group should be larger than the value predicted by Cohen-Lenstra-Martinet.

Topology as conjecture machine

We don't know everything about the topological side, but we know a lot – and this gives us a principled way to make geometrically motivated conjectures in arithmetic statistics.

In this way we reproduce many existing conjectures in number theory (Cohen-Lenstra, Malle-Bhargava, Boston-Bush-Hajir...)

But sometimes the geometry doesn't agree with existing conjectures: e.g. the geometric picture suggests that when F is a field containing cube roots of unity, the average *square* of the number of 3-torsion points in the class group should be larger than the value predicted by Cohen-Lenstra-Martinet.

Fortunately, this was already observed in numerical data by Malle (2010)!

Topology as conjecture machine

We don't know everything about the topological side, but we know a lot – and this gives us a principled way to make geometrically motivated conjectures in arithmetic statistics.

In this way we reproduce many existing conjectures in number theory (Cohen-Lenstra, Malle-Bhargava, Boston-Bush-Hajir...)

But sometimes the geometry doesn't agree with existing conjectures: e.g. the geometric picture suggests that when F is a field containing cube roots of unity, the average *square* of the number of 3-torsion points in the class group should be larger than the value predicted by Cohen-Lenstra-Martinet.

Fortunately, this was already observed in numerical data by Malle (2010)!

"Repaired" version of Cohen-Lenstra for fields containing pth roots of unity: Garton (2012)