Counting arithmetic objects

Jordan Ellenberg

21 Jan 2005

By an *arithmetic counting problem* we mean: count objects over a ring R (or scheme S) which become isomorphic over the algebraic closure of the fraction field of R (or geometric generic point of S.) For instance:

- How many degree-3 extensions of K are there with discriminant at most X? (all are isomorphic to $\bar{K}^3$ over $\bar{K}$)

- How many ideal classes are there in R? (All are isomorphic over the fraction field.)

- How many isomorphism classes of nondegenerate quadratic forms of rank n are there over $\mathbb{Z}$? (All are isomorphic over $\bar{\mathbb{Q}}$.)

Main ideas:

- Relation between arithmetic counting problems and geometric problems (rational points on varieties)

- Analogies between counting problems over number fields and counting problems over function fields.

Counting extensions of global fields

- K a global field (number field or function field of curve $C/\mathbb{F}_q$.)

- L/K a degree-n extension with discriminant $\mathcal{D}$:

  - (number field case) $\mathcal{D}$ is an ideal of $\mathcal{O}_K$, whose norm is $N \in \mathbb{Z}$;

  - (function field case) $\mathcal{D}$ is a divisor (ramification divisor) on C of degree b, whose norm is q^b. In this case, L is the function field of a degree n cover $\pi : X \to C$, and $2g(X) - 2 = 2g(C) - 2 + b$ by Riemann-Hurwitz (assuming char $K > n$).

- $N_{K,n}(B)$: number of extensions of K of degree n with discriminant of norm at most B. (Implicit theorem statement: there are *finitely* many such (Hermite)

- If $G \subset S_n$, can restrict to L/K whose splitting field has Galois group G, and consider $N_{K,G}(B)$: number of extensions of K with Galois group G whose discriminant has norm at most B.

Question: Asymptotic behavior of $N_{K,G}(B)$?

Example: $G = \mathbb{Z}/2\mathbb{Z}, K = \mathbb{Q}$

- $L = \mathbb{Q}(\sqrt{d})$, d a squarefree integer; $\mathcal{D}$ is $|d|$ (if d is 1 mod 4) or $4|d|$ (if d is $2, 3$ mod 4). Conclude

$$N_{\mathbb{Q},\mathbb{Z}/2\mathbb{Z}}(B) \sim \zeta(2)^{-1}B$$

Example: $G = \mathbb{Z}/2\mathbb{Z}, K = \mathbb{F}_q(t)$

- $L = K(\sqrt{f})$ where f is a squarefree polynomial; $X \leq q^{2g+2}$ implies $\deg f \leq 2g + 2$. Probability a polynomial is squarefree is the probability that discriminant is 0, which should be $1/q$, number of polynomials of degree at most q^{2g+2} up to $(\mathbb{F}_q^*)^2$ is about $2q^{2g+2}(1 - q^{-1})^{-1}$, so and so one expects

$$N_{K,\mathbb{Z}/2\mathbb{Z}}(q^{2g+2}) \sim 2q^{2g+2}$$

and one can check this is right.

So in both cases, $N_{K,2}(B) \sim C_K B$.

What's known, I:

- $N_{K,2}(B) \sim C_K B$ for all global fields K;

- $N_{\mathbb{Q},3}(B) \sim \zeta(3)^{-1} B$ (Davenport-Heilbronn, 1971)

- $N_{K,3}(B) \sim \zeta_K(3)^{-1} B$ for all global fields (Datskovsky-Wright, 1988) (slightly imprecise)

- $N_{\mathbb{Q},4}(B) \sim \frac{5}{24} \prod_p (1 + p^{-2} - p^{-3} - p^{-4}) B$ (Bhargava, 2005)

- $N_{\mathbb{Q},5}(B) \sim c_5 B$ (Bhargava, to appear)

- $N_{\mathbb{Q},(\mathbb{Z}/2\mathbb{Z})^r} \sim cB(\log B)^{2^r - 2}$ (exercise!)

- and more ...

Malle's conjecture

- Let K a global field, $G \subset S_n$ a group, $n <$ char K.

- *Index* of a permutation in S_n is n - number of orbits; e.g. index of 3-cycle (123) is 2, index of transposition (12) is 1.

- Two combinatorial invariants:

  - $1/a(G) =$ minimal index of any element of G

  - $b(K, G) =$ number of conjugacy classes in G with index $1/a(G)$, up to action of cyclotomic character of G_K (depends only on group of roots of unity in K)

Conjecture:

$$N_{K,G}(B) \sim c(K, G) B^{a(G)} (\log B)^{b(K,G)-1}.$$

Malle and Batyrev-Manin

- **M:** K a global field, $G \subset S_n$.

- **BM:** K a global field, X/K a projective variety.

- **M:** Counting fields by *discriminant*

- **BM:** Counting rational points by *height*

- **M:** $N_{K,G}(B) \sim c(K,G)B^{a(G)}(\log B)^{b(K,G)-1}$

- **BM:** $N_{K,X}(B) \sim c(K,X)B^{a(X)}(\log B)^{b(K,X)-1}$

- **M:** a, b combinatorial invariants of G

- **BM:** a, b geometric invariants of X

Malle and Baytrev-Manin

- **M:** $\exists K$ s.t. $b(K', G) = b(K, G)$ for all K' containing K

- **BM:** same

- **M:** No prediction for $c(K, G)$ in general (but see Bhargava via Belabas's Asterisque for conjectured $c(K, S_n)$)

- **BM:** Prediction for $c(K, X)$ (Peyre)

- **M:** Counterexample (Klüners, 2004) where $N_{Q,G}(B)$ has too high a power of $\log B$

- **BM:** Counterexample (Batyrev-Tschinkel, 1996) where $N_{K,X}(B)$ has too high a power of $\log B$

What's known, II: Malle's conjecture

In addition to results above, one knows Malle conjecture

- Holds for G abelian (Wright, 1989)

- Holds for $G = D_4$ (Cohen-Diaz-Olivier, 2002)

- Holds up to B^ϵ for all nilpotent groups embedded in S_n via regular permutation representation (Klüners-Malle, 2004)

Some questions:

- Why the formal similarity between Batyrev-Manin and Malle?

  - Can think of G-extensions of K as maps from $\operatorname{Spec} K$ to the stack BG.

  - Notion of *height* for rational points of BG? (Will have to involve *vector bundles*, not just line bundles.)

Some questions:

- Write $\mathbf{N}(\mathcal{D}_{L/K})$ for norm of discriminant of L/K. Under what circumstances does the "zeta function"

$$f(s) = \sum_{L/K} \mathbf{N}(\mathcal{D}_{L/K})^{-s}$$

have good analytic properties? (Probably not always.) In any event, the location and order of the rightmost pole of $f(s)$ governs the asymptotics of $N_{K,G}(B)$.

- What is the secondary main term, if any, of $N_{K,G}(B)$? **Conjecture** (Roberts, 1999, following Shintani)

$$N_{\mathbb{Q},S_3}(B) =$$
$$\zeta(3)^{-1} + \frac{12(\sqrt{3}+1)\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}B^{5/6} + o(B^{5/6}).$$

Techniques:

- Bhargava makes masterful use of *integral orbits*. His work is extremely concrete but I shall present it in a vague and imprecise way to emphasize connection with techniques in rational points.

- Idea (described vaguely) Suppose X is a variety with a transitive action of G, and H is the stabilizer of a point $x_0 \in X(\mathbb{Z})$. Let x be another point of $X(\mathbb{Z})$. Then $P_{x_0,x}$, the subscheme of G sending x_0 to x, is isomorphic to H if $x \in G(\mathbb{Z})x_0$. So $P_{x_0,x}$ is isomorphic to H over $\bar{\mathbb{Q}}$; it is an H-torsor; one can rephrase many arithmetic counting problems as "count H-torsors."

- **Example:** X is the space of binary cubic forms of discriminant d (a hypersurface in $\mathbb{A}^3$) and $G = \mathsf{SL}_2$. Then H is a form of $\mathbb{Z}/3\mathbb{Z}$ and the $G(\mathbb{Z})$ orbits on $X(\mathbb{Z})$ are in bijection with cubic rings of discriminant d (Delone-Fadeev). This allows counting of cubic fields as in Davenport-Heilbronn. (Note that a cubic form $ax^3 + bx^2y + cxy^2 + dy^3$ naturally yields a cubic field; the field over which the linear factors are defined.)

- **Compare** with method of "the universal torsor" in which one counts points on X by counting points on Y, where $Y \to X$ is a vector bundle and Y is sufficiently simple (e.g. open subscheme of affine space) that counting on $Y(\mathbb{Z})$ is tractable.

- In the present context we have

$$
\begin{array}{ccc}
G & \longrightarrow & \mathsf{Spec}\,\mathbb{Z} \\
\downarrow & & \downarrow \\
X & \longrightarrow & BH
\end{array}
$$

where the left-hand map sends g to gx_0; X is a G-bundle (not necessarily a vector bundle) over BH. Often X is sufficiently simple (e.g. affine space) that counting points on $X(\mathbb{Z})$ is easy.

- Also, compare (E,Venkatesh, to appear) in which one gets upper bounds for $N_{\mathbb{Q},n}(B)$ by means of the map

$$\mathbb{A}^{rn}/S_n \to BS_n$$

which is a vector bundle. This yields $N_{\mathbb{Q},n}(B) \ll_\epsilon B^{n^\epsilon}$. (Method of Hermite is the case $r = 1$.)

A heuristic Suppose K is the function field of $C/\mathbb{F}_q$. Then we have a bijection, more or less, between

- G-extensions L/K of discriminant q^b;

- covers $\pi : C' \to C$ with Galois group G and ramification degree b, where C' is a connected curve;

- $\mathcal{H}_b(\mathbb{F}_q)$, where $\mathcal{H}_b$ is a *Hurwitz space*.

E.G.: When $G = \mathbb{Z}/2\mathbb{Z}$ and $C = \mathbb{P}^1$, the Hurwitz space parametrizing double covers with ramification degree b is just the moduli space of hyperelliptic curves of genus $b/2 - 1$.

A heuristic

- **False Hypothesis A**: If X is an irreducible d-dimensional variety over $\mathbb{F}_q$, then $|X(\mathbb{F}_q)| = q^d$.

- If we accept **A**, computing $|\mathcal{H}_b(\mathbb{F}_q)|$ is reduced to computing the dimension and number of irreducible components of $\mathcal{H}_b$, a purely combinatorial problem.

- **Fact** (E.-Venkatesh, 2005) Under **A**, Malle's conjecture holds for K and arbitrary G of order prime to q, as long as *only geometrically connected C' are counted.*

- Sometimes the non-geometrically connected covers dominate; this is exactly parallel with Klüners' counterexample and should point the way towards a revised conjecture.

- Batyrev used a heuristic of this kind to motivate Batyrev-Manin.

Stable cohomology

- To believe Malle (or Batyrev-Manin) over $K = \mathbb{F}_q(C)$ is to believe that certain sequences of spaces $\mathcal{H}_1, \mathcal{H}_2, \ldots$ (Hurwitz spaces or spaces of maps from C to X) satisfy for some function f

$$\lim_{i \to \infty} |\mathcal{H}_i(\mathbb{F}_q)| q^{-f(i)} = c \neq 0$$

- This is certainly possible:

  - $|\mathbb{P}^i(\mathbb{F}_q)| q^{-i} \to (1 - q^{-1})^{-1}$

  - If $\mathcal{H}_i$ is the space of smooth degree-i curves in $\mathbb{P}^2$, then

$$\begin{aligned} |\mathcal{H}_i(\mathbb{F}_q)| q^{-\dim \mathcal{H}_i} &\to (1 - q^{-1})^{-1} \zeta_{\mathbb{P}^2}(3)^{-1} \\ &= (1 - q^{-2})(1 - q^{-3}) \end{aligned}$$

  by (Poonen, 2004).

Stable cohomology

- Why would the limit $|\mathcal{H}_i(\mathbb{F}_q)|q^{-i}$ exist? Maybe because $\mathcal{H}_i$ has *stable cohomology*, i.e.

$$H^j(\mathcal{H}_i, \mathbb{Z}_\ell) = H^j(\mathcal{H}_{i+1}, \mathbb{Z}_\ell)$$

  for $i \gg j$.

- True for $\mathcal{H}_i$ the space of hyperelliptic curves (stable cohomology of Artin's braid group)

- True for $\mathcal{H}_i$ the space of maps from $\mathbb{P}^1$ to X of degree i, where X is projective space (Segal), Grassmannian (Kirwan), toric variety (Guest).... compare with list of varieties where Batyrev-Manin is known.

- For $\mathcal{H}_i$ the space of degree 3 covers of $\mathbb{P}^1$ with i branch points?