Counting Number Fields by Discriminant and Point Counting on Varieties

Eric Larson and Larry Rolen

Harvard University and Emory University

The General Problem

- Fix a transitive permutation group $G \leq S_n$ and a fixed positive integer n.

The General Problem

- Fix a transitive permutation group $G \leq S_n$ and a fixed positive integer n.
- Let $N(n, G, X) = \#\{K \ : \ [K : \mathbb{Q}] = n, \ \mathrm{Gal}(K/\mathbb{Q}) = G, \ \text{and } |D_K| \leq X\}$.

The General Problem

- Fix a transitive permutation group $G \leq S_n$ and a fixed positive integer n.
- Let $N(n, G, X) = \#\{K \ : \ [K : \mathbb{Q}] = n, \ \mathrm{Gal}(K/\mathbb{Q}) = G, \ \text{and } |D_K| \leq X\}$.

Question

What are the asymptotics of this function?

Previous Results

- When $n = 2$, this is essentially trivial.

Previous Results

- When $n = 2$, this is essentially trivial.
- By parameterizing number fields by binary cubic forms, Davenport and Heilbronn find the first order term for $n = 3$.

Previous Results

- When $n = 2$, this is essentially trivial.
- By parameterizing number fields by binary cubic forms, Davenport and Heilbronn find the first order term for $n = 3$.

Remark

This can bound average sizes of 3-parts of class numbers of quadratic fields and Selmer groups of elliptic curves.

Previous Results

- When $n = 2$, this is essentially trivial.
- By parameterizing number fields by binary cubic forms, Davenport and Heilbronn find the first order term for $n = 3$.

Remark

This can bound average sizes of 3-parts of class numbers of quadratic fields and Selmer groups of elliptic curves.

- Using "higher composition laws", Bhargava has studied the cases $G = S_4, S_5$.

Our Work

Theorem (L-R 2011)

We have

$$N(n, A_n, X) \ll_n X^{\frac{n^2-2}{4(n-1)}} \cdot \log(X)^{2n+1}.$$

Progress in the D_5 case

Theorem (L-R 2011)

To any quintic number field K with Galois group D_5, there corresponds a triple (A, B, C) with $A, B \in \mathcal{O}_{\mathbb{Q}[\sqrt{5}]}$ and $C \in \mathbb{Z}$, such that

$$\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{5}]}\left(B^2 - 4 \cdot \bar{A} \cdot A^2\right) = 5 \cdot C^2$$

and which satisfies the following under any archimedean valuation:

$$|A| \ll D_K^{\frac{1}{4}}, \quad |B| \ll D_K^{\frac{3}{8}}, \quad \text{and} \quad |C| \ll D_K^{\frac{3}{4}}.$$

Conversely, the triple (A, B, C) uniquely determines K.

Progress in the D_5 case

Theorem (L-R 2011)

To any quintic number field K with Galois group D_5, there corresponds a triple (A, B, C) with $A, B \in \mathcal{O}_{\mathbb{Q}[\sqrt{5}]}$ and $C \in \mathbb{Z}$, such that

$$\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{5}]}\left(B^2 - 4 \cdot \bar{A} \cdot A^2\right) = 5 \cdot C^2$$

and which satisfies the following under any archimedean valuation:

$$|A| \ll D_K^{\frac{1}{4}}, \quad |B| \ll D_K^{\frac{3}{8}}, \quad \text{and} \quad |C| \ll D_K^{\frac{3}{4}}.$$

Conversely, the triple (A, B, C) uniquely determines K.

Remark

We also provide numerical evidence that $N(5, D_5, X) \ll X^{\frac{2}{3}}$.

General Method of Point Counting

- If K is a primitive extension of $\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, then the characteristic polynomial for α determines K.

General Method of Point Counting

- If K is a primitive extension of $\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, then the characteristic polynomial for α determines K.
- By Minkowski theory, there is an element $\alpha \in \mathcal{O}_K$ with

$$|\alpha| \ll D_K^{\frac{1}{2(n-1)}}, \ \mathrm{Tr}(\alpha) = 0.$$

General Method of Point Counting

- If K is a primitive extension of $\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, then the characteristic polynomial for α determines K.
- By Minkowski theory, there is an element $\alpha \in \mathcal{O}_K$ with

$$|\alpha| \ll D_K^{\frac{1}{2(n-1)}}, \ \mathrm{Tr}(\alpha) = 0.$$

- Let $R = \mathbb{Z}[x_1, \ldots, x_n]^G/(s_1)$ where $s_1 = x_1 + \ldots + x_n$.

General Method of Point Counting

- If K is a primitive extension of $\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, then the characteristic polynomial for α determines K.
- By Minkowski theory, there is an element $\alpha \in \mathcal{O}_K$ with

$$|\alpha| \ll D_K^{\frac{1}{2(n-1)}}, \ \mathrm{Tr}(\alpha) = 0.$$

- Let $R = \mathbb{Z}[x_1, \ldots, x_n]^G/(s_1)$ where $s_1 = x_1 + \ldots + x_n$.
- Every pair (K, α) gives a $\mathbb{Z}$-point of $\operatorname{Spec} R$ with bounded coordinates.

The Case of D_5

- Recall that it suffices to understand bounded $\mathbb{Z}$-points of

$$\operatorname{Spec} \mathbb{Q}[x_1, x_2, x_3, x_4, x_5]^{D_5}/(x_1 + x_2 + x_3 + x_4 + x_5).$$

The Case of D_5

- Recall that it suffices to understand bounded $\mathbb{Z}$-points of

$$\operatorname{Spec} \mathbb{Q}[x_1, x_2, x_3, x_4, x_5]^{D_5}/(x_1 + x_2 + x_3 + x_4 + x_5).$$

- Let $V_j := \sum_{i=1}^{5} \zeta^{ij} x_i$.

The Case of D_5

- Recall that it suffices to understand bounded $\mathbb{Z}$-points of

$$\operatorname{Spec} \mathbb{Q}[x_1, x_2, x_3, x_4, x_5]^{D_5}/(x_1 + x_2 + x_3 + x_4 + x_5).$$

- Let $V_j := \sum_{i=1}^{5} \zeta^{ij} x_i$.
- Now define:

$$\begin{aligned} A &= V_2 \cdot V_3 \\ B &= V_1 \cdot V_2^2 + V_3^2 \cdot V_4 \\ C &= \frac{1}{\sqrt{5}} \cdot (V_1 \cdot V_2^2 - V_3^2 \cdot V_4) \cdot (V_2 \cdot V_4^2 - V_1^2 \cdot V_3). \end{aligned}$$

The Norm Equation for D_5

- The expressions A, B, and C are invariant under D_5.

The Norm Equation for D_5

- The expressions A, B, and C are invariant under D_5.
- The generators of D_5 act by $V_j \mapsto V_{5-j}$ and $V_j \mapsto \zeta^j V_j$.

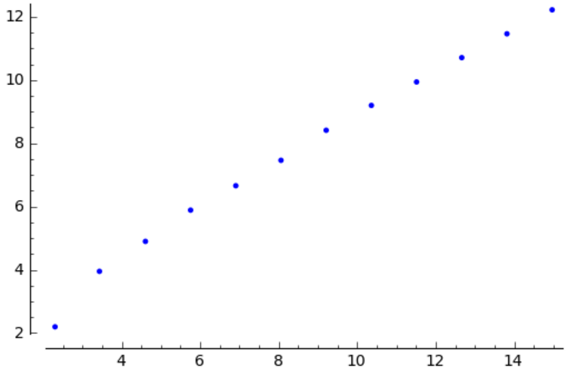
The Norm Equation for D_5

- The expressions A, B, and C are invariant under D_5.
- The generators of D_5 act by $V_j \mapsto V_{5-j}$ and $V_j \mapsto \zeta^j V_j$.
- This easily gives the norm equation in the theorem.

The Norm Equation for D_5

- The expressions A, B, and C are invariant under D_5.
- The generators of D_5 act by $V_j \mapsto V_{5-j}$ and $V_j \mapsto \zeta^j V_j$.
- This easily gives the norm equation in the theorem.
- The fact that (A, B, C) uniquely determines K can be shown using the expressions for V_i explicitly.

Numerical Data and Remarks



- This log plot and a regression analysis give strong evidence that $N(5, D_5, X) \ll X^{\frac{2}{3}}$. The data goes up to $X = 3162277$.

The Case of A_n

- The current best bounds on $N(n, A_n, X)$ follow from bounds on $N(d, X)$, the number of degree d fields with $|D_K| \leq X$.

The Case of A_n

- The current best bounds on $N(n, A_n, X)$ follow from bounds on $N(d, X)$, the number of degree d fields with $|D_K| \leq X$.
- It is a "folk" conjecture (Linnik?) that $N(d, X) \sim X$.

The Case of A_n

- The current best bounds on $N(n, A_n, X)$ follow from bounds on $N(d, X)$, the number of degree d fields with $|D_K| \leq X$.
- It is a "folk" conjecture (Linnik?) that $N(d, X) \sim X$.
- For $6 \leq n \leq 84393$, the best previous bound is due to Schmidt

$$N(n, A_n, X) \ll X^{\frac{n+2}{4}}.$$

The Case of A_n

- The current best bounds on $N(n, A_n, X)$ follow from bounds on $N(d, X)$, the number of degree d fields with $|D_K| \leq X$.
- It is a "folk" conjecture (Linnik?) that $N(d, X) \sim X$.
- For $6 \leq n \leq 84393$, the best previous bound is due to Schmidt

$$N(n, A_n, X) \ll X^{\frac{n+2}{4}}.$$

- For large n, Ellenberg and Venkatesh obtain:

The Case of A_n

- The current best bounds on $N(n, A_n, X)$ follow from bounds on $N(d, X)$, the number of degree d fields with $|D_K| \leq X$.
- It is a "folk" conjecture (Linnik?) that $N(d, X) \sim X$.
- For $6 \leq n \leq 84393$, the best previous bound is due to Schmidt

$$N(n, A_n, X) \ll X^{\frac{n+2}{4}}.$$

- For large n, Ellenberg and Venkatesh obtain:

$$N(n, A_n, X) \ll (X \cdot B_n)^{\exp(C \log \sqrt{n})}.$$

Our Result

Theorem (L-R 2011)

We have that $N(n, A_n, X) \ll X^{\frac{n^2-2}{4(n-1)}} \cdot \log(X)^{2n+1}$.

Our Result

Theorem (L-R 2011)

We have that $N(n, A_n, X) \ll X^{\frac{n^2-2}{4(n-1)}} \cdot \log(X)^{2n+1}$.

- This bound is about $X^{\frac{1}{4}}$ better than Schmidt's bound.

Our Result

Theorem (L-R 2011)

We have that $N(n, A_n, X) \ll X^{\frac{n^2-2}{4(n-1)}} \cdot \log(X)^{2n+1}$.

- This bound is about $X^{\frac{1}{4}}$ better than Schmidt's bound.
- This is the best-known bound for $6 \leq n \leq 84393$.

Our Result

Theorem (L-R 2011)

We have that $N(n, A_n, X) \ll X^{\frac{n^2-2}{4(n-1)}} \cdot \log(X)^{2n+1}$.

- This bound is about $X^{\frac{1}{4}}$ better than Schmidt's bound.
- This is the best-known bound for $6 \leq n \leq 84393$.
- By a conjecture of Malle, we expect that $N(n, A_N, X) \overset{?}{\sim} X^{\frac{1}{2}}$.

Sketch of Proof

- The ring of A_n-invariant functions is generated by the symmetric functions and the square root of the discriminant.

Sketch of Proof

- The ring of A_n-invariant functions is generated by the symmetric functions and the square root of the discriminant.
- It suffices to count $\mathbb{Z}$-points on

Sketch of Proof

- The ring of A_n-invariant functions is generated by the symmetric functions and the square root of the discriminant.
- It suffices to count $\mathbb{Z}$-points on

$$R := \mathbb{Z}[s_1, s_2, \ldots, s_n, D]/\left(D^2 = \mathrm{Disc}(t^n + s_2 t^{n-2} + \cdots \pm s_n)\right),$$

Sketch of Proof

- The ring of A_n-invariant functions is generated by the symmetric functions and the square root of the discriminant.
- It suffices to count $\mathbb{Z}$-points on

$$R := \mathbb{Z}[s_1, s_2, \ldots, s_n, D]/\big(D^2 = \mathrm{Disc}(t^n + s_2 t^{n-2} + \cdots \pm s_n)\big),$$

$$\text{with } |s_j| \ll X^{\frac{j}{2(n-1)}} \quad \text{and} \quad |D| \ll X^{\frac{n}{4}}.$$

Sketch of Proof

- The ring of A_n-invariant functions is generated by the symmetric functions and the square root of the discriminant.
- It suffices to count $\mathbb{Z}$-points on

$$R := \mathbb{Z}[s_1, s_2, \ldots, s_n, D]/\left(D^2 = \mathrm{Disc}(t^n + s_2 t^{n-2} + \cdots \pm s_n)\right),$$

$$\text{with } |s_j| \ll X^{\frac{j}{2(n-1)}} \quad \text{and} \quad |D| \ll X^{\frac{n}{4}}.$$

- The case when n is even is easier; we will use covering spaces to prove it when n is odd.

The Case when n is Even

- By fixing $s_2, s_3, \ldots, s_{n-1}$, we can view $\operatorname{Spec} R$ as a fibration of plane curves over $\mathbb{A}^{n-2}$.

The Case when n is Even

- By fixing $s_2, s_3, \ldots, s_{n-1}$, we can view $\operatorname{Spec} R$ as a fibration of plane curves over $\mathbb{A}^{n-2}$.
- Each of these curves is the zero locus of a polynomial

$$D^2 = \text{a polynomial of odd degree in } s_n.$$

The Case when n is Even

- By fixing $s_2, s_3, \ldots, s_{n-1}$, we can view $\operatorname{Spec} R$ as a fibration of plane curves over $\mathbb{A}^{n-2}$.
- Each of these curves is the zero locus of a polynomial

$$D^2 = \text{a polynomial of odd degree in } s_n.$$

- In particular, these curves are all *geometrically irreducible*.

Pila's Bound and the Proof when n is even

Theorem (Pila 1996)

Let Γ be a geometrically irreducible plane curve of degree $d \geq 2$ and let S be a square of side $N \geq 2$ in the plane with sides parallel to the coordinate axes.

Pila's Bound and the Proof when n is even

Theorem (Pila 1996)

Let Γ be a geometrically irreducible plane curve of degree $d \geq 2$ and let S be a square of side $N \geq 2$ in the plane with sides parallel to the coordinate axes.
Then the number of integral points on Γ inside S is at most

Pila's Bound and the Proof when n is even

Theorem (Pila 1996)

Let Γ be a geometrically irreducible plane curve of degree $d \geq 2$ and let S be a square of side $N \geq 2$ in the plane with sides parallel to the coordinate axes.
Then the number of integral points on Γ inside S is at most

$$(3d)^{4d+8} N^{\frac{1}{d}} (\log N)^{2d+3}.$$

Pila's Bound and the Proof when n is even

Theorem (Pila 1996)

Let Γ be a geometrically irreducible plane curve of degree $d \geq 2$ and let S be a square of side $N \geq 2$ in the plane with sides parallel to the coordinate axes.
Then the number of integral points on Γ inside S is at most

$$(3d)^{4d+8} N^{\frac{1}{d}} (\log N)^{2d+3}.$$

- This immediately implies the result when n is even.

The Case when n is Odd

- For n odd, we control when the curves are geometrically reducible.

The Case when n is Odd

- For n odd, we control when the curves are geometrically reducible.

Definition

We say two polynomials $f, g \in \mathbb{C}[z]$ are equivalent if $f(z) = g(az + b)$ for some $a \in \mathbb{C}^{\times}$ and $b \in \mathbb{C}$.

The Case when n is Odd

- For n odd, we control when the curves are geometrically reducible.

Definition

We say two polynomials $f, g \in \mathbb{C}[z]$ are equivalent if $f(z) = g(az + b)$ for some $a \in \mathbb{C}^\times$ and $b \in \mathbb{C}$.

Definition

We say that c is a critical value of a polynomial f if $c = f(d)$ for some d with $f'(d) = 0$.

Two Lemmas on Critical Values

Lemma

Fix a finite set of points $S \subset \mathbb{C}$ and an integer d. Then there are finitely many equivalence classes of polynomials of degree d whose set of critical values is contained in S.

Two Lemmas on Critical Values

Lemma

Fix a finite set of points $S \subset \mathbb{C}$ and an integer d. Then there are finitely many equivalence classes of polynomials of degree d whose set of critical values is contained in S.

Lemma

Let n be an integer. For any monic polynomial $p(z) \in \mathbb{C}[z]$ of degree $n-1$, there are only finitely many values of $(a_2, a_3, \cdots, a_{n-1}) \in \mathbb{C}^{n-2}$ such that $p(z)$ is the discriminant of the polynomial

$$q(t) = t^n + a_2 t^{n-2} + \cdots + a_{n-1} t - z.$$

Two Lemmas on Critical Values

Lemma

Fix a finite set of points $S \subset \mathbb{C}$ and an integer d. Then there are finitely many equivalence classes of polynomials of degree d whose set of critical values is contained in S.

Lemma

Let n be an integer. For any monic polynomial $p(z) \in \mathbb{C}[z]$ of degree $n-1$, there are only finitely many values of $(a_2, a_3, \cdots, a_{n-1}) \in \mathbb{C}^{n-2}$ such that $p(z)$ is the discriminant of the polynomial

$$q(t) = t^n + a_2 t^{n-2} + \cdots + a_{n-1} t - z.$$

- The proofs follow using basic theory of covering spaces.

Proof of Theorem when n is even

- Our curve is geometrically reducible iff $p(y) = \mathrm{disc}(t^n + s_2 t^{n-2} + \cdots \pm s_{n-1} t - y)$ is a perfect square.

Proof of Theorem when n is even

- Our curve is geometrically reducible iff $p(y) = \mathrm{disc}(t^n + s_2 t^{n-2} + \cdots \pm s_{n-1} t - y)$ is a perfect square.
- The coefficients of $p(y)$ are regular functions in $s_2, s_3, \ldots, s_{n-1}$ and the induced map $\mathbb{A}^{n-2} \to \mathbb{A}^{n-1}$ is a finite map by the previous lemma.

Proof of Theorem when n is even

- Our curve is geometrically reducible iff $p(y) = \mathrm{disc}(t^n + s_2 t^{n-2} + \cdots \pm s_{n-1} t - y)$ is a perfect square.
- The coefficients of $p(y)$ are regular functions in $s_2, s_3, \ldots, s_{n-1}$ and the induced map $\mathbb{A}^{n-2} \to \mathbb{A}^{n-1}$ is a finite map by the previous lemma.
- The locus of $(b_1, b_2, \ldots, b_{n-1}) \in \mathbb{A}^{n-1}$ such that $t^{n-1} + b_1 t^{n-2} + \cdots + b_{n-1}$ is a perfect square is a Zariski-closed set of dimension $\frac{n-1}{2}$.

Proof of Theorem when n is even

- Our curve is geometrically reducible iff $p(y) = \mathrm{disc}(t^n + s_2 t^{n-2} + \cdots \pm s_{n-1} t - y)$ is a perfect square.
- The coefficients of $p(y)$ are regular functions in $s_2, s_3, \ldots, s_{n-1}$ and the induced map $\mathbb{A}^{n-2} \to \mathbb{A}^{n-1}$ is a finite map by the previous lemma.
- The locus of $(b_1, b_2, \ldots, b_{n-1}) \in \mathbb{A}^{n-1}$ such that $t^{n-1} + b_1 t^{n-2} + \cdots + b_{n-1}$ is a perfect square is a Zariski-closed set of dimension $\frac{n-1}{2}$.
- The proof now follows in a similar way as when n is even.

Conclusion

Theorem (L-R 2011)

We have that $N(n, A_n, X) \ll X^{\frac{n^2-2}{4(n-1)}} \cdot \log(X)^{2n+1}$.

Conclusion

Theorem (L-R 2011)

We have that $N(n, A_n, X) \ll X^{\frac{n^2-2}{4(n-1)}} \cdot \log(X)^{2n+1}$.

Theorem

To any quintic number field K with Galois group D_5, there corresponds a triple (A, B, C) with $A, B \in \mathcal{O}_{\mathbb{Q}[\sqrt{5}]}$ and $C \in \mathbb{Z}$, such that

$$\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{5}]}\left(B^2 - 4 \cdot \bar{A} \cdot A^2\right) = 5 \cdot C^2 \tag{1}$$

and which satisfies the following under any archimedean valuation:

$$|A| \ll D_K^{\frac{1}{4}}, \quad |B| \ll D_K^{\frac{3}{8}}, \quad \text{and} \quad |C| \ll D_K^{\frac{1}{2}}. \tag{2}$$

Conversely, the triple (A, B, C) uniquely determines K.