Counting algebraic integers of fixed degree and bounded height

Workshop: The Geometry, Algebra and Analysis of Algebraic Numbers

October 5, 2015

Notation

Multiplicative Weil height $H : \overline{\mathbb{Q}}^n \to [1, \infty)$:

$$H(\alpha_1, \ldots, \alpha_n) = \prod_{v \in M_k} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{\frac{d_v}{m}},$$

where $m = [k : \mathbb{Q}]$.

Notation

Multiplicative Weil height $H : \overline{\mathbb{Q}}^n \to [1, \infty)$:

$$H(\alpha_1, \ldots, \alpha_n) = \prod_{v \in M_k} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{\frac{d_v}{m}},$$

where $m = [k : \mathbb{Q}]$.

Define, for a number field k,

$$k(n, e) = \left\{ \underline{\alpha} \in \overline{k}^n : [k(\underline{\alpha}) : k] = e \right\}.$$

Notation

Multiplicative Weil height $H : \overline{\mathbb{Q}}^n \to [1, \infty)$:

$$H(\alpha_1, \ldots, \alpha_n) = \prod_{v \in M_k} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{\frac{d_v}{m}},$$

where $m = [k : \mathbb{Q}]$.

Define, for a number field k,

$$k(n, e) = \left\{ \underline{\alpha} \in \overline{k}^n : [k(\underline{\alpha}) : k] = e \right\}.$$

For any $A \subseteq k(n, e)$, set

$$N(A, \mathcal{H}) = |\{\underline{\alpha} \in A : H(\underline{\alpha}) \leq \mathcal{H}\}|.$$

Asymptotics for $N(k(n,e),\mathcal{H})$

- Schanuel, '79: $N(k(n,1),\mathcal{H})$;
- Schmidt, '93: Upper and lower bounds;
- Schmidt, '95: $N(\mathbb{Q}(n,2),\mathcal{H})$;
- Gao, '95: $N(\mathbb{Q}(n,e),\mathcal{H})$, for $n > e$;
- Masser-Vaaler, '07: $N(k(1,e),\mathcal{H})$;
- Widmer, 09': $N(k(n,e),\mathcal{H})$, provided $n > 5e/2 + 5 + 2/me$.

Algebraic integers

Define

$$\mathcal{O}_k(n,e) = \left\{ \underline{\alpha} \in \mathcal{O}_k^n : [k(\underline{\alpha}) : k] = e \right\}.$$

Algebraic integers

Define

$$\mathcal{O}_k(n,e) = \left\{ \underline{\alpha} \in \mathcal{O}_k^n : [k(\underline{\alpha}) : k] = e \right\}.$$

Lang - Fundamentals of Diophantine Geometry

As $\mathcal{H} \to \infty$, we have

$$N(\mathcal{O}_k(1,1), \mathcal{H}) = \gamma \mathcal{H}^m (\log \mathcal{H})^q + O\left(\mathcal{H}^{m-1} (\log \mathcal{H})^{q-1}\right),$$

where q is the rank of $\mathcal{O}_k^\times$.

Chern-Vaaler, '01

As $\mathcal{H} \to \infty$, we have

$$N(\mathcal{O}_{\mathbb{Q}}(1,e),\mathcal{H}) = C_e \mathcal{H}^{e^2} + O\left(\mathcal{H}^{e^2-1}\right).$$

Chern-Vaaler, '01

As $\mathcal{H} \to \infty$, we have

$$N(\mathcal{O}_{\mathbb{Q}}(1,e),\mathcal{H}) = C_e \mathcal{H}^{e^2} + O\left(\mathcal{H}^{e^2-1}\right).$$

Widmer

As $\mathcal{H} \to \infty$, we have

$$N(\mathcal{O}_k(n,e),\mathcal{H}) = \sum_{i=0}^{t} D_i \mathcal{H}^{men} \left(\log \mathcal{H}^{men}\right)^i + O\left(\mathcal{H}^{men-1}(\log \mathcal{H})^t\right),$$

provided $e = 1$ or $n > e + C_{e,m}$, for some explicit $C_{e,m} \leq 7$. Here $t = e(q+1) - 1$, and the constants $D_i = D_i(k,n,e)$ are explicitly given.

Theorem (Barroero)

Let e be a positive integer, and let k be a number field of degree m over $\mathbb{Q}$. Then, as $\mathcal{H} \geq 2$ tends to infinity, we have

$$N(\mathcal{O}_k(1,e),\mathcal{H}) = C_k^{(e)}\mathcal{H}^{me^2}(\log\mathcal{H})^q + \begin{cases} O\left(\mathcal{H}^{me^2}(\log\mathcal{H})^{q-1}\right), & \text{if } q \geq 1, \\ O\left(\mathcal{H}^{e(me-1)}\mathcal{L}\right), & \text{if } q = 0, \end{cases}$$

where $\mathcal{L} = \log\mathcal{H}$ if $(m,e) = (1,2)$ and 1 otherwise. The implicit constant in the error term depends only on m and e.

We define a "generalized" Mahler measure

$$\begin{array}{rccl} M^k: & k[X] & \to & [0,\infty) \\ & f & \mapsto & \prod_{i=1}^{r+s} M(\sigma_i(f))^{\frac{d_i}{m}}. \end{array}$$

Lemma

An algebraic integer β has degree e over k and $H(\beta) \leq \mathcal{H}$ if and only if it is a root of a monic irreducible polynomial $f \in \mathcal{O}_k[X]$ of degree e with $M^k(f) \leq \mathcal{H}^e$.

Lemma

An algebraic integer β has degree e over k and $H(\beta) \leq \mathcal{H}$ if and only if it is a root of a monic irreducible polynomial $f \in \mathcal{O}_k[X]$ of degree e with $M^k(f) \leq \mathcal{H}^e$.

The number of reducible polynomial is "negligible" and we are reduced to count

$$\begin{aligned}\mathcal{M}^k(e,\mathcal{H}) &= \{f \in \mathcal{O}_k[X] : \text{monic, } \deg f = e, M^k(f) \leq \mathcal{H}\} \\ &= \{(a_1,\ldots,a_e) \in \mathcal{O}_k^e : M^k(1,a_1,\ldots,a_e) \leq \mathcal{H}\}\end{aligned}$$

Embed $\mathcal{O}_k^e$ as a lattice Λ in $\mathbb{R}^{me}$. We count points of Λ inside

$$Z(T) = \left\{ (\underline{x}_1, \ldots, \underline{x}_{r+s}) \in (\mathbb{R}^e)^r \times \left(\mathbb{R}^{2e}\right)^s : \prod_{i=1}^{r+s} M(1, \underline{x}_i)^{d_i} \leq T \right\}.$$

Embed $\mathcal{O}_k^e$ as a lattice Λ in $\mathbb{R}^{me}$. We count points of Λ inside

$$Z(T) = \left\{ (\underline{x}_1, \ldots, \underline{x}_{r+s}) \in (\mathbb{R}^e)^r \times \left(\mathbb{R}^{2e}\right)^s : \prod_{i=1}^{r+s} M(1, \underline{x}_i)^{d_i} \leq T \right\}.$$

General principle

$$|Z(T) \cap \Lambda| \sim \frac{\mathrm{Vol} Z(T)}{\det \Lambda},$$

with

$$\text{error} = O\left((\mathrm{diam} Z(T))^{me-1} \right).$$

Chern and Vaaler calculated

$$\mathrm{Vol}\left(\left\{(a_1,\dots,a_e)\in K^e : M(X^e+a_1X^{e-1}+\cdots+a_e)\le T\right\}\right),$$

for $K=\mathbb{R}$ or $\mathbb{C}$.

Chern and Vaaler calculated

$$\mathrm{Vol}\left(\left\{(a_1,\ldots,a_e)\in K^e : M(X^e+a_1X^{e-1}+\cdots+a_e)\le T\right\}\right),$$

for $K=\mathbb{R}$ or $\mathbb{C}$.
One can calculate

$$\mathrm{Vol}Z(T)=C_{e,k}\,T^e\,(\log T)^{r+s-1}+O(T^e\,(\log T)^{r+s-2}).$$

Chern and Vaaler calculated

$$\mathrm{Vol}\left(\left\{(a_1,\ldots,a_e)\in K^e : M(X^e+a_1X^{e-1}+\cdots+a_e)\le T\right\}\right),$$

for $K=\mathbb{R}$ or $\mathbb{C}$.
One can calculate

$$\mathrm{Vol}Z(T)=C_{e,k}\,T^e\,(\log T)^{r+s-1}+O(T^e\,(\log T)^{r+s-2}).$$

But $\mathrm{diam}Z(T)\sim T$, so

$$\mathrm{error}=O\left(T^{me-1}\right).$$

For $\Lambda = \mathbb{Z}^n$ one can use a result of Davenport.

For $\Lambda = \mathbb{Z}^n$ one can use a result of Davenport.

Theorem (B.-Widmer)

Let $Z \subset \mathbb{R}^{n+n'}$ be a semialgebraic family and suppose the fibers $Z_{\underline{t}}$ are bounded. Then there exists a constant $c_Z \in \mathbb{R}$, depending only on the family, such that, for every $\underline{t} \in \mathbb{R}^{n'}$,

$$\left| |Z_{\underline{t}} \cap \Lambda| - \frac{\mathrm{Vol}(Z_{\underline{t}})}{\det \Lambda} \right| \leq \sum_{j=0}^{n-1} c_Z \frac{V_j(Z_{\underline{t}})}{\lambda_1 \cdots \lambda_j},$$

where $V_j(Z_{\underline{t}})$ is the sum of the j-dimensional volumes of the orthogonal projections of $Z_{\underline{t}}$ on every j-dimensional coordinate subspace of $\mathbb{R}^n$ and $V_0(Z_{\underline{t}}) = 1$.

This is ideal for us since

$$V_j(Z(T)) = O(T^e (\log T)^{r+s-2}).$$

This is ideal for us since

$$V_j(Z(T)) = O(T^e (\log T)^{r+s-2}).$$

Moreover,

$$\det \Lambda = \left(2^{-s}\sqrt{|\Delta_k|}\right)^e \quad \text{and} \quad \lambda_1 \geq 1.$$

This is ideal for us since

$$V_j(Z(T)) = O(T^e (\log T)^{r+s-2}).$$

Moreover,

$$\det \Lambda = \left(2^{-s}\sqrt{|\Delta_k|}\right)^e \quad \text{and} \quad \lambda_1 \geq 1.$$

Therefore

$$\left| |Z(T) \cap \Lambda| - C'_{e,k} T^e (\log T)^{r+s-1} \right| \leq D(m,e) T^e (\log T)^{r+s-2}.$$