Diophantine inequalities for the Weil height

1241, January 9, 2018

The Weil height:

The Weil height $h(\alpha)$ can be defined on algebraic numbers $\alpha \neq 0$ in two ways. Assume that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, and let

$$m_\alpha(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d$$

be the minimal polynomial for α in $\mathbb{Z}[x]$. Then

$$h(\alpha) = d^{-1} \int_0^1 \log\left| m_\alpha\left(e^{2\pi i t}\right)\right| \, dt.$$

Alternatively, let k be a number field containing α, and for each place v of k let $| \ |_v$ be a normalized absolute value on k. Then we have

$$0 = \sum_v \log |\alpha|_v,$$

and

$$h(\alpha) = \sum_v \log^+ |\alpha|_v = \tfrac{1}{2} \sum_v \left|\log |\alpha|_v\right|.$$

An important early result:

Theorem 1. (Northcott, 1949) *For positive* d *and* T*, the set of algebraic numbers*

$$\{\alpha \in \overline{\mathbb{Q}} : [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d \text{ and } h(\alpha) \leq T\}$$

is finite.

A more recent result:

Theorem 2. (V., M. Widmer, 2011) *Let* k *be a number field of degree* d *and discriminant* Δ_k*. If* k *has a real embedding, then there exists* $\alpha \neq 0$ *in* k *such that* $k = \mathbb{Q}(\alpha)$*, and*

$$h(\alpha) \leq \frac{\log |\Delta_k|}{2d}.$$

If k is totally complex a similar bound holds provided the Dedekind zeta-function $\zeta_l(s)$ satisfies GRH, where l is the Galois closure of k.

Units: let k be an algebraic number field, O_k the ring of algebraic integers in k,

$$O_k^\times = \text{ multiplicative group of units in } O_k,$$

and

$$\begin{aligned}\text{Tor}\left(O_k^\times\right) &= \text{ torsion subgroup of } O_k^\times \\ &= \text{ roots of unity in } O_k^\times \\ &= \text{ a finite, cyclic group.}\end{aligned}$$

Dirichlet's unit theorem: there exists a finite collection of multiplicatively independent units $\eta_1, \eta_2, \ldots, \eta_r$, and a generator ζ of $\text{Tor}\left(O_k^\times\right)$, so that every unit α has a unique representation as

$$\alpha = \zeta^m \eta_1^{n_1} \eta_2^{n_2} \cdots \eta_r^{n_r},$$

where m, and $n_1, n_2, \ldots, n_r$, are integers. Here

$$r = \text{rank}\left(O_k^\times\right).$$

Minkowski units: we now assume that $k/\mathbb{Q}$ is a *Galois* extension of degree d. Then the Galois group

$$G = \text{Aut}(k/\mathbb{Q})$$

has order d, and G acts on $O_k^\times$. If $\alpha \neq 1$ belongs to $O_k^\times$, then

$$\{\sigma(\alpha) : \sigma \in G\} \subseteq O_k^\times.$$

Minkowski proved: if $k/\mathbb{Q}$ is a Galois extension and $O_k^\times$ has positive rank r, then there exists a unit α in $O_k^\times$ such that the subgroup

$$\langle \sigma(\alpha) : \sigma \in G \rangle \subseteq O_k^\times$$

generated by the conjugates of α has the maximum possible rank r. We call a unit α with this property a *Minkowski unit*.

Theorem 3 (S. Akhtari-V.). *Let* $\eta_1, \eta_2, \ldots, \eta_r$*, be multiplicatively independent elements in* $O_k^\times$*, where* $r = \text{rank}\Big(O_k^\times\Big)$*. Let*

$$\mathfrak{A} = \langle \eta_1, \eta_2, \ldots, \eta_r \rangle \subseteq O_k^\times$$

be the subgroup they generate. Then there exists a Minkowski unit β *in* $\mathfrak{A}$ *such that*

$$h(\beta) \le 2\Big(h(\eta_1) + h(\eta_2) + \cdots + h(\eta_r)\Big).$$

Moreover, if

$$\mathfrak{B} = \langle \sigma(\beta) : \sigma \in G \rangle,$$

is the subgroup of $O_k^\times$ *generated by the conjugates of* β*, then*

$$\text{Reg}(k)[O_k^\times : \mathfrak{B}] \le \Big([k : \mathbb{Q}]h(\beta)\Big)^r,$$

where $\text{Reg}(k)$ *is the regulator of* k*.*

The following simple result about real matrices is a key lemma:

Lemma 1. *Let $A = (a_{mn})$ be a real, nonsingular, $N \times N$ matrix. Then there exists a point*

$$\boldsymbol{\xi} = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_N \end{pmatrix}$$

in $\mathbb{Z}^N$, such that

$$0 < \sum_{n=1}^{N} a_{mn}\xi_n \leq \sum_{n=1}^{N} |a_{mn}|$$

for each $m = 1, 2, \ldots, N$.

Full modules and norm forms: Let l/k be an extension of degree e, and $\omega_1, \omega_2, \ldots, \omega_e$, a basis for l/k. We use the basis to define a full O_k-module

$$\mathfrak{M} = \Big\{\omega_1\nu_1 + \omega_2\nu_2 + \cdots + \omega_e\nu_e : \nu_i \in O_k\Big\}$$

generated by the basis $\omega_1, \omega_2, \ldots, \omega_e$. If

$$\boldsymbol{\nu} = (\nu_i)$$

belongs to $(O_k)^e$, then

$$\boldsymbol{\nu} \mapsto \mathrm{Norm}_{l/k}(\mu),$$

where

$$\mu = \omega_1\nu_1 + \omega_2\nu_2 + \cdots + \omega_e\nu_e$$

belongs to $\mathfrak{M}$, is the associated norm form. For each $\beta \neq 0$ in k, we wish to describe

$$\Big\{\mu \in \mathfrak{M} : \mathrm{Norm}_{l/k}(\mu) \in \mathrm{Tor}\Big(O_k^{\times}\Big)\beta\Big\}.$$

There is a natural equivalence relation in $\mathfrak{M}$ such that solution set is either empty, or it is a disjoint union of finitely many equivalence classes.

The *coefficient ring* associated to $\mathfrak{M}$ is

$$O_{\mathfrak{M}} = \Big\{\alpha \in l : \alpha\mathfrak{M} \subseteq \mathfrak{M}\Big\}.$$

The coefficient ring $O_{\mathfrak{M}}$ is an order in l, so

$$O_{\mathfrak{M}} \subseteq O_l.$$

The group of units in $O_{\mathfrak{M}}^{\times}$ is

$$O_{\mathfrak{M}}^{\times} = \Big\{\alpha \in l : \alpha\mathfrak{M} = \mathfrak{M}\Big\},$$

and by the extension of Dirichlet's unit theorem to orders

$$\text{rank}\Big(O_{\mathfrak{M}}^{\times}\Big) = \text{rank}\Big(O_l^{\times}\Big) = r(l).$$

Hence the group $O_{\mathfrak{M}}^{\times}$ acts on the module $\mathfrak{M}$ by multiplication. Let

$$\mathcal{E}_{l/k}(\mathfrak{M}) = \Big\{\alpha \in O_{\mathfrak{M}}^{\times} : \text{Norm}_{l/k}(\alpha) \in \text{Tor}\Big(O_k^{\times}\Big)\Big\}$$

be the subgroup of *relative units* in the coefficient ring $O_{\mathfrak{M}}$. The subgroup $\mathcal{E}_{l/k}(\mathfrak{M})$ has rank

$$r(l/k) = r(l) - r(k).$$

Now suppose that $\beta \neq 0$ belongs to O_k, and μ in $\mathfrak{M}$ satisfies

$$\text{Norm}_{l/k}(\mu) = \zeta\beta, \quad \text{where } \zeta \in \text{Tor}\Big(O_k^{\times}\Big).$$

If γ belongs to the group $\mathcal{E}_{l/k}(\mathfrak{M})$, then $\gamma\mu$ belongs to $\mathfrak{M}$, and

$$\text{Norm}_{l/k}(\gamma\mu) = \zeta'\beta, \quad \text{where } \zeta' \in \text{Tor}\Big(O_k^{\times}\Big).$$

We say that two nonzero elements μ_1 and μ_2 in $\mathfrak{M}$ are *equivalent* if there exists an element γ in the group $\mathcal{E}_{l/k}(\mathfrak{M})$ such that $\gamma\mu_1 = \mu_2$. For $\beta \neq 0$ in O_k, the set

$$\Big\{\mu \in \mathfrak{M} : \text{Norm}_{l/k}(\mu) \in \text{Tor}\Big(O_k^{\times}\Big)\beta\Big\}.$$

is a disjoint union of finitely many equivalence classes. A finiteness result of this sort also follows from Northcott's theorem and the following inequality.

Theorem 4 (S. Akhtari-V.). *Let $\mathfrak{M} \subseteq O_l$ be a full O_k-module, and assume that the rank $r(l/k)$ of the group $\mathcal{E}_{l/k}(\mathfrak{M})$ of relative units is positive. Let*

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r(l/k)},$$

be multiplicatively independent units in the subgroup $\mathcal{E}_{l/k}(\mathfrak{M})$. Assume that $\beta \neq 0$ is a point in O_k, and $\mu \neq 0$ is a point in $\mathfrak{M}$, such that

$$\mathrm{Norm}_{l/k}(\mu) = \zeta\beta, \quad \textit{where } \zeta \in \mathrm{Tor}\Big(O_k^{\times}\Big).$$

Then there exists an element γ in $\mathcal{E}_{l/k}(\mathfrak{M})$, such that $\gamma\mu$ belongs to $\mathfrak{M}$,

$$\mathrm{Norm}_{l/k}(\gamma\mu) = \zeta'\beta, \quad \textit{where } \zeta' \in \mathrm{Tor}\Big(O_k^{\times}\Big),$$

and

$$h(\gamma\mu) \leq \tfrac{1}{2} \sum_{j=1}^{r(l/k)} h(\varepsilon_j) + [l:k]^{-1} h(\beta).$$

Relative Minkowski units: Assume that both $l/\mathbb{Q}$ and $k/\mathbb{Q}$ are Galois. An element $\gamma \neq 1$ in $E_{l/k}$ is a *relative Minkowski unit* if the group

$$\langle \tau(\gamma) : \tau \in \mathrm{Aut}(l/k) \rangle$$

generated by the conjugates of γ over the field k has maximum rank in $E_{l/k}$. These exist.

Theorem 5 (S. Akhtari-V.). *Let* $\eta_1, \eta_2, \ldots, \eta_{r(l)}$, *be a basis for* $O_l^\times$.

(i) If $l/\mathbb{Q}$ is totally real, there exists a relative Minkowski unit γ in $E_{l/k}$ such that

$$h(\gamma) \leq 4[l : k] \sum_{j=1}^{r(l)} h(\eta_j).$$

(i) If $l/\mathbb{Q}$ is totally complex, there exists a relative Minkowski unit γ in $E_{l/k}$ such that

$$h(\gamma) \leq 8[l : k] \sum_{j=1}^{r(l)} h(\eta_j).$$