Diophantine Approximation

§0 Intro

e? π? $\mathbb{C}$ $\sum \frac{1}{10^{n!}}$?

transcendental

$\overline{\mathbb{Q}}$ = algebraic numbers

$\mathbb{Q}$ = rational numbers.

Q1. How can we show a number is transcendental? — Roth's Thm — Apply

Arithmetic geometry

(Siegel) $y^2 = f(x)$ has finitely many sol'ns in $\mathbb{Z}$.

(Faltings) C/K of genus ≥ 2 has finitely many sol'ns in K

Q2. How can we show a Diophantine equation has finitely many solutions?

Idea: A number "way too close" to a ~~rational number~~ algebraic number is ~~irrational~~ transcendental

approximate efficiently w/ rational number of small denominator.

formalize

Def. Let $\alpha \in \mathbb{R}$. Approximation exponent

$$\tau(\alpha) = \inf\left\{\tau : \left|\frac{p}{q} - \alpha\right| < \frac{1}{q^\tau} \text{ has fin. sol'ns}\right\}$$

can't approx. α within ε with denom $\leq \varepsilon^{1/\tau}$.

Dirichlet's Thm (1842)

$\forall \alpha \in \mathbb{R}$, $\exists \infty$ many $\frac{p}{q} \in \mathbb{Q}$,

$\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{q^2}$ $\rightsquigarrow \tau(\alpha) \geq 2$.

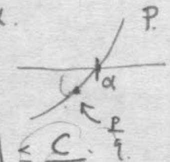
~~Liouville's Thm (1844)~~ Roth 1955 For $\alpha \in \overline{\mathbb{Q}}$, $d = [\mathbb{Q}(\alpha):\mathbb{Q}]$, $\varepsilon > 0$

$\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{q^{d+\varepsilon}}$ ($q^{2+\varepsilon}$) has fin solns $\rightsquigarrow \tau(\alpha) \leq d$ (2).

Pf. of Liouville BWOC $\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{q^{d+\varepsilon}}$

1. Construct polynomial P, $P(\alpha) = 0$.
2. Show that $P(\frac{p}{q})$ really small $\overset{\text{FPoNT}}{\Rightarrow} = 0$.
3. Show that $P(\frac{p}{q}) \neq 0$.

1. P = min poly of α.
2. $P(\frac{p}{q}) = \frac{k}{q^d}$



$\left|P(\frac{p}{q})\right| \leq \left|P'(x)(\frac{p}{q} - \alpha)\right| \leq \frac{C}{q^{d+\varepsilon}}$.

$\rightsquigarrow P(\frac{p}{q}) = 0$.

3. P has no rat. root.

Pf. $\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{q^{\tau+\varepsilon}}$

1. Construct P w/ small coeff vanishes to high ord @ α
2. Show that $P(\frac{p}{q})$ really small $\overset{\text{FPoNT}}{\Rightarrow} = 0$

   $\text{ord}_{\frac{p}{q}} P = j \Rightarrow j \geq \bullet$
3. P has coeff $\Rightarrow$ P can't vanish to high order at $\frac{p}{q}$

1. $\deg P = r$, $(x-\alpha)^{r_1} \| P$.
2. $P(\frac{p}{q}) = \frac{k}{q^r}$

   $\left|P(\frac{p}{q})\right| \leq C\left|\frac{p}{q} - \alpha\right|^{r_1} \leq \frac{C}{q^{r_1(\tau+\varepsilon)}}$

   $r \approx r_1 \tau$, $\tau \approx \frac{r}{r_1}$
3. $(qX - p)^j \mid P$

   $|P| \geq \max(|p|, |q|)^j = H(\frac{p}{q})^j$

   $j \leq \frac{\ln |P|}{\ln H(\frac{p}{q})}$

Generalize to alg. #s.

Def. $K/\mathbb{Q}$. Height $p: [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$

$$H_K(p) := \prod_{v \in V_K} \max(\|x_i\|_v)$$

$\alpha \in K$, $H_K(\alpha) := H_K([1:\alpha])$

Ex. $H_{\mathbb{Q}}(\frac{p}{q}) = \max(|p|, |q|)$

- finite # of elements of K w/ height $\leq C$
- measures arithmetic/geometric complexity of numbers

Roth's Thm' For $\alpha \in \overline{\mathbb{Q}}$, $\beta \in K/\mathbb{Q}$, $\varepsilon > 0$

$$\prod_{v \in V_K} \min(\|\beta - \alpha\|_v, 1) \leq \frac{1}{H_K(\beta)^{2+\varepsilon}}$$

has fin. solns.

Roth's Thm'' .... $\xi_v : S \to [0,1]$ $\sum_v \xi_v = 1$

$$\prod_{v \in S} \cdots \leq \frac{1}{H_K(\beta)^{\xi_v(2+\delta)}}$$

has fin. solns

§1 Construction of Auxiliary Poly

Soln. Construct multivariable P.

Construct small poly vanishing to high order

$\leftrightarrow$ Find a small integer solution to sys. eq.

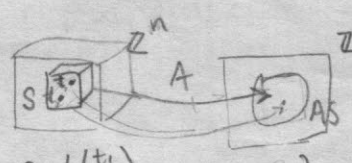
Siegel's Lemma $|A| = \max |a_{ij}|$

$A \in M_{m \times n}(\mathbb{Q})$ (K), $m < n$

$At = 0$ has soln t, $|t| \leq (n \cdot |A|)^{\frac{m}{n-m}}$ ($\frac{dm}{n-dm}$, $H(A)$)

$(t \in \mathbb{Z}^n)$

Pf.



$S = \left\{\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} : t_i \in [0, M]\right\}$

$At_1 = At_2 \Rightarrow A(\underbrace{t_1 - t_2}_{t}) = 0$

Take $M = (n \cdot |A|)^{\frac{m}{n-m}}$

Def. Index of $P(x_1, \ldots x_m)$

$$\text{Ind}_{(\beta_1, \ldots \beta_m, r_1, \ldots r_m)} P = \min\left\{\sum_j \frac{i_j}{r_j} \,\middle|\, \partial_{i_1 \ldots i_m} P \neq 0\right\}$$

Want P s.t. $\text{Ind}_{(\alpha, r_1, \ldots r_m)} P \approx \frac{m}{2} \cdot (\alpha, \ldots \alpha)$

Prop. $\varepsilon > 0$, given r_i, $\exists P \in \mathbb{Z}[x_1, \ldots x_m]$ s.t. $r_i = \deg_{x_i} P$, $r = \sum r_i$, $\partial_i = \frac{\partial^{i_j}}{\partial x_{i_1} \cdots}$, $i_1! \cdots i_m!$

- (P vanishes to high order @ α) $\text{Ind}_\alpha P \geq \frac{m}{2}(1 - \varepsilon)$
- (P has small coeff.) $|P| \leq B(\alpha)^r$

Pf. $R = \prod(r_i + 1)$ $P = \sum P_{i_1 \ldots i_m} X^{i_1} \cdots X^{i_m}$, $0 \leq i_j \leq r_j + 1$

- For large m, $L_{\frac{m}{2}(1-\varepsilon)} := \{(i_1, \ldots i_m) : i_j \in [0, r_j], \sum \frac{i_j}{r_j} < \frac{m}{2}(1-\varepsilon)\}$ has card. $\varepsilon' R$ $\varepsilon' \to 0$ (probab.)
- $\forall i \in L_{\frac{m}{2}(1-\varepsilon)}$, $\partial_i P = 0$

  Sys. of $\varepsilon' R$ eq'ns, $d\varepsilon' R < R$

  Apply S.L. to get bd on $|P|$.

§2 Index @ α is large

Prop Suppose $0 < \delta < 1$ $\delta \to \varepsilon$

- β_i good approx to α
- $H_K(\beta_h)^{r_h}$ are close to g.
- $H_K(\beta_h) \geq C(\alpha, \delta)$

$\Rightarrow \text{Ind} P \geq \varepsilon m$

Pf Liouville's ineq

$\beta \in \overline{\mathbb{Q}}$, $\beta = 0$ or $\prod_{v \in S} \min(\|\beta\|_v, 1) \geq \frac{1}{H_K(\beta)}$

- $\prod_{v \in S} \|\partial_j P(\beta)\|_v \leq F_1(d, H_K(P), H_K(\beta_i), r)$

  $\geq \frac{1}{H_K(\partial_j(P(\beta)))} \geq F_2(H_K(\beta_i), H_K(P), d)$

  j small — coeff P small

*

Ex. e is irrational.

$$\frac{p}{q} = e = \sum_{n=0}^{\infty} \frac{1}{n!} = \boxed{\sum_{n=0}^{N} \frac{1}{n!}} + \sum_{N+1}^{\infty} \frac{1}{n!}$$

$$\frac{k}{qN!} = \left| \frac{p}{q} - \sum_{0}^{N} \frac{1}{n!} \right| = \sum_{N+1}^{\infty} \frac{1}{n!} \le \frac{2}{(N+1)!}$$

$$0 < k \le q \cdot \frac{2}{N+1} < 1$$

FPONT $((0,1) \cap \mathbb{Z} = \phi)$ ↯.

§3 Index @ α is small

Prop: $f_1, \dots f_r \in \bar{\mathbb{Q}}[X_1, \dots X_m]$.

$f = \prod f_i$, $d_i = \deg_X f$.

$$\sum_{i=1}^{r} h(f_i) = h(f) + O(1) \quad \hookrightarrow \le \dots + \sum d_i$$'s

(Gelfand's).

Need to reduce # variables.

Def. Gererализed Wronskian det. of $\phi_1, \dots \phi_k$ is

$\det((\Delta_i \phi_j)_{i,j})$, $\operatorname{ord}(\Delta_i) \le i-1$, $\Delta_i = \partial_{i_1, \dots i_m}$.

Fact $\phi_1, \dots \phi_k$ lin ind/k $\Leftrightarrow$ $\exists$(gen. Wr. of ϕ_i) $\neq 0$

Roth's Lemma. $\eta > 0$.

- (r_i decrease rapidly enough)
$$\frac{r_{n+1}}{r_n} \le \eta^{2^{m-1}}$$
- ($H(\beta_i)$'s increase rapidly enough)
$$\eta^{2^{m-1}} \min_n (r_n H(\beta_n)) \ge 1 \ln H(\beta) + 2m\eta$$

$\Rightarrow \operatorname{Ind}_{(\beta, r)} P \le 2m\eta$.

Pf. $P = \sum_{j=1}^{k} \underbrace{\phi_j(X_1, \dots X_{m-1})}_{\text{lin indep.}} \psi_j(X_m)$

$W(X_1, \dots, X_m) = V(X_1, \dots X_{m-1}) \cdot U(X_m)$

$\partial_m^0 P, \dots \partial_m^{k-1} P$ ↖ $\phi_1, \dots \phi_k$ ↖ $\psi_1, \dots \psi_k$.

$$\frac{k(\operatorname{Ind} P)^2}{2m} \le \operatorname{Ind} W \le \operatorname{Ind} V + \operatorname{Ind} U \simeq (m\eta)^2$$

§4 Applications

Thm (Unit equation) $K/\mathbb{Q}$ $S \subset V_K$

$\mathcal{O}_S$:= S-integers

$U + V = 1$ finitely solns in U_S.

Pf. $\left| \frac{U}{V} - 1 \right|_w = \frac{1}{|V|_w}$

$aX^m + bY^m = 1$

$$\prod_{j=1}^{m} \left(\frac{X}{Y} - \frac{\xi_j}{m} \alpha \right) = \frac{X^m}{Y^m} + \frac{b}{a} = \frac{1}{aY^m}$$

$$\left\| \frac{X}{Y} - \xi_m^i \alpha \right\|_w C_1^{m-1} \le \frac{1}{\|aY^m\|_w}$$

$$\|Y\|_w \ge \left(\prod_{v \in S/V_K} \|Y\|_v \right)^{\frac{1}{s}} = H_K(Y)^{\frac{1}{s}} \ge C_2 H_K\left(\frac{X}{Y}\right)^{\frac{1}{s}}.$$

$$\left\| \frac{X}{Y} - \xi_m^i \right\|_w \le \frac{C_3}{H_K\left(\frac{X}{Y}\right)^{m/s}} \quad m = 2s+1$$

Q.E.D. U_S / U_S^m is finite

$U = aX^m$

$V = bY^m$

Pigeonhole (a,b)

$\|Y\|_w$ max

Thm. (Siegel)

$Y^2 = f(X)$ has fin soln $X, Y \in \mathcal{O}_S$

≥ 3 dist. roots in $\bar{K}$

Pf $Y^2 = a(X-\alpha_1) \cdots (X-\alpha_n)$

① $X - \alpha_i = U_i z_i^2 = v_i^2 z_i^2 = w_i^2$

② $(X-\alpha_i) - (X-\alpha_j) = \alpha_j - \alpha_i$ units

$(w_i - w_j)(w_i + w_j)$

Q.E.D. (Siegel's unit eq)

$$\begin{cases} \frac{w_1 - w_3}{w_1 - w_3} + \frac{w_2 - w_3}{w_1 - w_3} = 1 \\ \frac{w_1 + w_2}{w_1 - w_3} + \frac{-w_2 - w_3}{w_1 - w_3} = 1 \end{cases}$$

Extend K so

- f splits
- $u_i = v_i^2$

Extend S so.

- $a \in U_S$, $\alpha_i \in \mathcal{O}_S$
- $\alpha_i - \alpha_j \in U_S$, $i \neq j$
- $\mathcal{O}_S$ is PID. UFD (class grp finite)