

①

# DIOPHANTINE APPROXIMATION 23-1-2018

① a) Since  $\deg \beta$  has degree  $d$ , there are no  $a_0, a_1, \dots, a_d \in \mathbb{Q}$ , not all zero, with  $a_0 + a_1 \beta + a_2 \beta^2 + \dots + a_d \beta^d = 0$ , i.e., if  $\beta, \beta^2, \dots, \beta^d$  are linearly independent over  $\mathbb{Q}$ . So  $\log \alpha, \beta \log \alpha, \dots, \beta^d \log \alpha$  are linearly independent over  $\mathbb{Q}$ . Hence by Schanuel's conjecture,

$$\text{trdeg}(\log \alpha, \beta, \beta^2, \dots, \beta^d) = \text{trdeg}(\log \alpha, \beta \log \alpha, \dots, \beta^d \log \alpha) \geq d.$$

So  $\log \alpha, \beta, \beta^2, \dots, \beta^d$  are algebraically independent. In particular,  $\alpha, \beta, \beta^2, \dots, \beta^d$  are algebraically independent.

There are integers  $a_0, a_1, \dots, a_d$ , with  $a_d \neq 0$ , such that  $a_0 + a_1 \beta + a_2 \beta^2 + \dots + a_d \beta^d = 0$ . Multiplying with  $\log \alpha$ , and exponentiating, gives  $(\alpha^{a_0} (\beta^{\log \alpha})^{a_1} \cdots (\beta^d)^{a_d})^d = 1$ . Choose a positive integer  $m$  such that  $m+a_i > 0$ ,  $m+a_d \geq 0$ . Then we see that  $(\alpha^m, \alpha^{\log \alpha}, \alpha^{\log \alpha})$  is a zero of the polynomial  $P(X_1, X_d) = X_d^m - \alpha^{a_0} X_1^{m+a_1} \cdots X_d^{m+a_d}$ . Hence they are algebraically dependent.

b) We have  $\text{trdeg}(e, \pi, e^\pi, e^{\pi i}, e^{\pi i \alpha}) = \text{trdeg}(1, \pi, \pi i, \pi i \alpha, e, e^\pi, e^{\pi i}, e^{\pi i \alpha}) \geq 4$ , i.e.,  $e, \pi, e^\pi, e^{\pi i}, e^{\pi i \alpha}$  are algebraically independent, provided that  $1, \pi, \pi i, \pi i \alpha$  are linearly independent over  $\mathbb{Q}$ . To prove this, let  $a, b, c, d$  be rationals with  $a+b\pi+c\pi i+d\pi i \alpha=0$ . Then  $a+(b+c i+d \alpha)\pi=0$ . Since  $\pi$  is transcendental, we have  $b+c i+d \alpha=0$ , hence  $a=0$ . Since  $\alpha \notin \mathbb{Q}(\pi)$  we have  $d=0$ . Since  $i \notin \mathbb{Q}$  we have  $c=0$ . Hence  $b=0$ .

(2)

a) We proceed by induction on  $r$ . First let  $r=1$ . Let  $q \in C$  and  $x_1 \in \mathbb{R}$  with  $|x_1| \leq 1$ . Put  $t := \frac{x_1+1}{2}$ . Then  $t \in C$ . Since  $C$  is a c.s.c.b., we have  $q, -q \in C$ , and so  $tq + (1-t)(-q) = x_1 q \in C$ . Now let  $r \geq 2$  and assume the assertion is true for fewer than  $r$  points. Let  $x_1, x_{r-1}, x_r \in \mathbb{R}$  with  $|x_1| + \dots + |x_r| \leq 1$ . Let  $\lambda := |x_1| + |x_r|$ , assume w.l.o.g.  $\lambda > 0$  (which we may since  $0 \in C$ ), put  $x_i' = |x_i|/\lambda$ , and let  $b_i = \pm q_i$  with the same sign as  $x_i$ . Then  $x_1 b_1 + \dots + x_r b_r = \lambda(x_1 b_1 + x_r b_r)$ , where  $b_1, \dots, b_r \in C$ ,  $y_i \geq 0$ ,  $y_1 + \dots + y_r = 1$ . Assume  $y = y_1 + \dots + y_r > 0$  otherwise  $x_1 = \dots = x_r = 0$ ,  $x_i q_i \in C$  as we have seen above. By the induction hypothesis,  $c := (y_1/\mu)b_1 + \dots + (y_r/\mu)b_r \in C$ , and by the convexity of  $C$ ,  $\mu c + (1-\mu)b_r = y_1 b_1 + \dots + y_r b_r \in C$ . From the case  $r=1$ , we then infer that  $x_1 b_1 + x_r b_r \in C$ .

b) Let  $C$  be a c.s.c.b. in  $\mathbb{R}^n$  and  $L$  a lattice in  $\mathbb{R}^n$ . Then the successive minima  $\lambda_1, \dots, \lambda_n$  of  $C$  with respect to  $L$  are defined as follows:  $\lambda_i$  is the minimum of all  $\lambda > 0$  such that  $\lambda C \cap L$  contains at least  $i$  linearly independent points. Now Minkowski's theorem asserts that  $\frac{2^n}{n!} \frac{d(L)}{\text{vol}(C)} \leq \lambda_1 \dots \lambda_n \leq \frac{2^n}{n!} \frac{d(L)}{\text{vol}(C)^2}$ , where  $d(L)$  is the determinant of  $L$ .

c) We have  $\lambda_i^{-1} v_i \in C$  for  $i=1, \dots, n$ , so  $D := \left\{ \sum_{i=1}^n x_i (\lambda_i^{-1} v_i) : \sum_i |x_i| \leq 1 \right\}$  is c.s.c.  $D$  is the image of  $\mathbb{Q}_n$  under the linear map  $\varphi: (x_1, \dots, x_n) \in \mathbb{R}^n \mapsto \sum_{i=1}^n x_i (\lambda_i^{-1} v_i)$  which has determinant  $\det(v_1, \dots, v_n)/(\lambda_1 \dots \lambda_n) = \frac{d(n)}{\lambda_1 \dots \lambda_n}$ . So  $\text{vol}(D) = \frac{d(n)}{\lambda_1 \dots \lambda_n} \text{vol}(\mathbb{Q}_n)$ . Combining this with Minkowski's theorem, we get

$$\frac{d(n)}{\lambda_1 \dots \lambda_n} \frac{2^n}{n!} = \text{vol}(D) \leq \text{vol}(C) \leq \frac{d(L)}{d(L)} \cdot 2^n. \text{ Hence } (M:L) \leq \frac{d(n)}{d(L)} \leq \frac{n!}{d(L)}$$

(3)

Many students had the following much easier solution, which I had overlooked. Let  $\mu_1, \dots, \mu_n$  be the successive minima of  $C$  with respect to  $M$ . Since MSL we have  $\mu_i \geq \lambda_i$  for  $i = 1, \dots, n$ . On the other hand we have linearly independent points  $v_1, v_2, \dots, v_n \in C \cap \mathbb{Z}^n$  with  $v_i \in M$ . Hence  $\mu_i \leq \lambda_i$  for  $i = 1, \dots, n$ . So

$$\frac{z^n}{n!} \frac{d(M)}{\text{vol}(C)} \leq \mu_1 \cdots \mu_n \leq \lambda_1 \cdots \lambda_n \leq z^n \frac{d(M)}{\text{vol}(C)},$$

$$\text{hence } (\text{vol}(M))^{-\frac{1}{n}} \leq \frac{d(M)}{\text{vol}(C)} \leq n!$$

(3) a) We first determine  $\gamma, \bar{\gamma}$  from  $u_0 = \gamma + \bar{\gamma}, u_1 = \gamma z + \bar{\gamma} \bar{z}$ . This gives  $\gamma = \frac{u_0 - u_1}{z - \bar{z}}, \bar{\gamma} = \frac{u_0 - u_1}{z - \bar{z}}$ . Since  $z \notin \mathbb{R}$  we have  $\gamma, \bar{\gamma} \neq 0$ .

We prove by induction on  $n$  that  $u_n = \gamma z^n + \bar{\gamma} \bar{z}^n$  for  $n \geq 0$ . For  $n=0, 1$  we are done. Suppose  $n \geq 2$ , and  $u_k = \gamma z^k + \bar{\gamma} \bar{z}^k$  for all  $k < n$ . Since  $z^2 + \bar{z}^2 = B > 0, z^2 - \bar{z}^2 = D > 0$  we have  $\gamma^2 = A\gamma + B, \bar{\gamma}^2 = A\bar{\gamma} + B$ . Hence

$$\begin{aligned} u_{n+2} &= Au_{n+1} + Bu_{n+2} = A(\gamma z^{n+1} + \bar{\gamma} \bar{z}^{n+1}) + B(\gamma z^{n+2} + \bar{\gamma} \bar{z}^{n+2}) \\ &= \gamma z^{n+2}(A + B) + \bar{\gamma} \bar{z}^{n+2}(A + B) = \gamma z^{n+2} + \bar{\gamma} \bar{z}^{n+2}. \end{aligned}$$

b) Suppose  $u_n = \gamma z^n + \bar{\gamma} \bar{z}^n \neq 0$ . Then by Baker's Theorem,

$$|u_n| = |\gamma z^n| \cdot \left|1 + \frac{\bar{\gamma} \bar{z}^n}{\gamma z^n}\right| = |\gamma z^n| \cdot \left|1 - \left(-\frac{\bar{\gamma}}{\gamma}\right)\left(\frac{\bar{z}}{z}\right)^n\right| \geq |\gamma z^n| / (eB),$$

where  $B$  and  $|z|$ , and  $C$  is effectively computable in terms of  $A, B, \gamma, \bar{\gamma}$ . So

$$(*) |u_n| \geq |\gamma|^n \cdot (1/e^C)^n = |\gamma|^n / e^{nC}, \text{ with } C, C.$$

Effectively computable in terms of  $A, B, \gamma, \bar{\gamma}$ .

(4)

Now suppose  $\alpha = 0$ . Then  $\left(\frac{\beta}{\alpha}\right)^n = -\frac{\delta}{\gamma}$ . This can be satisfied by at most one value of  $n$  for if there were two such values,  $n_1$  and  $n_2$ , say, then it would follow  $\left(\frac{\beta}{\alpha}\right)^{n_1+n_2} = 1$ , hence  $n_1 = n_2$  since  $\frac{\beta}{\alpha}$  is not a root of unity. Let  $\eta \in \mathbb{Q}$ , if  $\left(\frac{\beta}{\alpha}\right)^n = -\frac{\delta}{\gamma}$  is unsolvable, and the unique solutions of  $\left(\frac{\beta}{\alpha}\right)^n = -\frac{\delta}{\gamma}$  otherwise. Then  $\eta_\beta$  is effectively computable in terms of  $\alpha, \beta, \gamma, \delta$  hence in terms of  $A, B, y_1, y_2$  and  $u_n$  for  $n > n_1$ . So (4) holds for  $n > n_1$ .

(4) a) Let  $L_i = x_1 X + \dots + x_n X^i$  ( $i \in \mathbb{N}_0, n$ ) be linearly independent linear forms (over  $\mathbb{Q}$ ) with coefficients  $x_j \in \mathbb{Q}$ , and let  $C > 0$ . Then the ~~ininitely~~<sup>set of</sup> solutions of

$$|L_1(x) - L_n(x)| \leq C \|x\|^{-\delta} \quad \text{in } x \in \mathbb{Z}^n$$

is contained in a finite union  $T_1 \cup \dots \cup T_r$  of proper linear subspaces of  $\mathbb{Q}^n$ . Here  $\|x\| = \max(|x_1|, \dots, |x_n|)$ . For  $x \in (x_1, x_2) \in \mathbb{Z}^2$

b) Consider  $(+) \quad 0 < |(\alpha x_1 + \beta x_2)(\delta x_1 + \gamma x_2)| \leq C \|x\|^{-\delta} \quad \text{in } x = (x_1, x_2) \in \mathbb{Z}^2$

where  $\alpha, \beta, \gamma, \delta \neq 0$ . By a), the solutions of (+) lie in a union  $T_1 \cup \dots \cup T_r$  of one-dimensional linear subspaces of  $\mathbb{Q}^2$ , so we have to prove that each of these subspaces contains only finitely many solutions of (+). Let  $T_j = \{ \lambda x_j, \lambda \in \mathbb{Q} \}$ ,  $x_1 + \lambda x_2 = l_1(x)$ ,  $x_1 + \delta x_2 = l_2(x)$ . Then for a solution  $\lambda x_j \in \mathbb{Z}^2$  of (+) we have

$$0 < |\lambda|^2 \cdot |l_1(x_j)l_2(x_j)| \leq C |\lambda|^{-\delta} \cdot \|x_j\|^{-\delta},$$

$$\text{hence } |\lambda|^{2\delta} \leq C (\|x_j\|^{-\delta} |l_1(x_j)l_2(x_j)|)^{-1} = D.$$

So  $|\lambda x_j| \leq D^{\frac{1}{2\delta}} \cdot \|x_j\| = E$ . There are only finitely many  $x \in \mathbb{Z}^2$

(5)

with  $\|x\| \leq R$ , so  $T$  contains indeed only finitely many solutions of (+)

$$c) \text{ Consider } (+) \quad 0 < \underbrace{[(\alpha_1 x_1 + \dots + \alpha_n x_n)(\beta_1 x_1 + \dots + \beta_n x_n)]}_{\text{if } x = (x_1, \dots, x_n) \in \mathbb{Z}^n} \stackrel{\text{and}}{\in} C \|x\|$$

By assumption, the numbers  $\alpha_i - q_j \beta_i$  ( $1 \leq i, j \leq n$ ) are linearly independent over  $\mathbb{Q}$ . We prove by induction on  $n$  that (+) has only finitely many solutions. For  $n=2$  we are done by b). Let  $n \geq 3$ . The linear forms  $L_1, L_2, X_1, \dots, X_{n-2}$  have determinant

$$\begin{vmatrix} \alpha_1 - q_1 \beta_1 & \dots & \alpha_1 - q_n \beta_1 \\ \vdots & \ddots & \vdots \\ \alpha_n - q_1 \beta_n & \dots & \alpha_n - q_n \beta_n \end{vmatrix} = \pm \alpha_{1,n} \neq 0, \text{ hence are linearly independent.}$$

If  $x \in \mathbb{Z}^n$  is a solution of (+) then

$$|L_1(x)L_2(x)x_1 \dots x_{n-2}| \in C \|x\|^2 \stackrel{\text{and}}{\in} C \|x\|$$

By a) No solutions of (+) lie in a finite union  $T_1 \cup \dots \cup T_l$  of proper linear subspaces of  $\mathbb{Q}^n$ . We have to prove that each of these spaces  $T$  contains only finitely many solutions.

Suppose without loss of generality that  $T$  is given by  $q_1 x_1 + \dots + q_m x_m = 0$ , with  $q_m \neq 0$ . If every  $x \in T$  satisfies  $x_n = b_1 x_1 + \dots + b_m x_m$ , with  $b_i = -q_i/q_m$  for  $i = 1, \dots, m$  the solutions of (+) in  $T$  satisfy

$$(++) \quad 0 < |(\alpha_1 + q_1 \beta_1)x_1 + \dots + (\alpha_m + q_m \beta_m)x_m| \cdot |(\beta_1 + q_1 \beta_m)x_1 + \dots + (\beta_m + q_m \beta_m)x_m| \stackrel{\text{and}}{\in} C \|x\|^2 \stackrel{\text{and}}{\in} C \|x\| \text{ where } x' = (x_1, \dots, x_m)$$

The determinants  $\alpha'_i = (\alpha_i + q_i \beta_m)(\beta_i + q_i \beta_m) - (\alpha_i + q_i \beta_m)(\beta_i + q_i \beta_m)$  ( $1 \leq i \leq m-1$ ) are linearly independent over  $\mathbb{Q}$ . Indeed, we have  $\alpha'_1 = \alpha_1 - q_1 \beta_1 \alpha'_m + q_1 \beta_1 \alpha'_m$ . Assume that there are rationals  $c_j$  such that  $\sum_{j=1}^m \sum_{i=1}^{m-1} c_j \alpha'_j = 0$ . Then

(6)

$$\sum_{i=1}^m \sum_{j=1}^m c_{ij} (\alpha_j - \alpha_i \alpha_{jn} + \alpha_i \alpha_{in}) = 0,$$

$$\sum_{i=1}^m \sum_{j=1}^m c_{ij} \alpha_{ij} - \sum_{i=1}^m \left( \sum_{j=1}^m c_{ij} \alpha_j \right) \alpha_{jn} + \sum_{i=1}^m \left( \sum_{j=1}^m c_{ij} \alpha_j \right) \alpha_{in} = 0,$$

implying  $c_{ij} = 0$  for  $i \neq j, n$  since the  $\alpha_{ij}$  are linearly independent over  $\mathbb{Q}$ .

We can now apply the induction hypothesis to (++) and conclude that (++) has only finitely many solutions. Consequently, (+) has only finitely many solutions in  $T$ .