# EXAMPLE SHEET 2 FOR DIOPHANTINE ANALYSIS, MICHAELMAS 2024

PÉTER VARJÚ

About this example sheet:

- Please send comments and corrections to pv270@dpmms.cam.ac.uk.
- Please submit your solutions of Problems 3 *or* 4 and 9, by Monday 11 November, 13:00.
- The purpose of this example sheet is to complement the material of the lectures. The level of difficulty of the problems varies considerably (in a non-monotone fashion), and they are not intended to be mock exam questions.
- The solutions went under minimal proof reading only, so they are error prone. Please handle with care, and corrections sent by email are very much appreciated.

**1.** Fix some numbers $H, D \in \mathbf{Z}_{>0}$. Prove that the number of algebraic numbers $\alpha$ with $H(\alpha) \leq H$ and $\deg(\alpha) \leq D$ is at most $3^{D+1}D(2H)^{D(D+1)}$.

*Hint:* Use Mahler measure to bound the coefficients of the minimal polynomial of $\alpha$.

*Solution:* For $\alpha$ with $H(\alpha) \leq H$ and $\deg(\alpha) \leq D$, we have

$$H(f_\alpha) \leq 2^D M(f_\alpha) \leq (2H(\alpha))^D.$$

The number of polynomials of degree $\leq D$ with coefficients $\leq (2H)^D$ is at most

$$(2(2H)^D + 1)^{D+1} \leq 3^{D+1}(2H)^{D(D+1)}.$$

Each has at most $D$ roots.

**2.** Prove that for every $D \in \mathbf{Z}_{>0}$, there is a constant $c = c(D)$ such that for all $H \in \mathbf{Z}_{>0}$, the number of algebraic numbers with $H(\alpha) \leq H$ and $\deg(\alpha) = D$ is at least $cH^{D(D+1)}$.

*Hint:* Use Eisenstein's criterion to construct many irreducible polynomials.

*Solution:* Consider polynomials of degree $D$ with coefficients between $1, \dots, \lfloor (H^D)/(D+1) \rfloor$ that are 2-Eisenstein, that is, the leading coefficient is odd, the rest are even, but the constant coefficient is not divisible by 4. If $H$ is large enough so that $\frac{H^D}{D+1} \geq 2$, then the number of such polynomials is at least

$$\Big(\frac{H^D}{5(D+1)}\Big)^{D+1}.$$

A positive proportion of these have coprime coefficients. Indeed, just considering two of the coefficients, less than $4/p^{-2}$ proportion of the polynomials have coefficients all divisible by $p$. (One needs to check that in the arithmetic progressions where the coefficients are chosen from, not more than a $2/p$ proportion is divisible by $p$ even if $p$ is large. This requires some thinking.) When $p = 2$, none of the polynomials are divisible by 2 because of the Eisenstein condition. It turns out that

$$\sum_{p\geq 3 \text{ prime}} \frac{4}{p^2} < 1,$$

so a positive proportion of the polynomials indeed have coprime coefficients. In fact, for the proof it would be enough that the above some is convergent if we restrict the coefficients in suitable arithmetic progressions that rule out small primes.

Therefore, we have at least $cH^{D(D+1)}$ polynomials with coprime coefficients of size at most $(H^D)/(D+1)$ that are irreducible, where $c > 0$ is a constant depending only on $D$. The roots of all these polynomials are distinct and their height is at most

$$\Big((D+1)\frac{H^D}{D+1}\Big)^{1/D} = H.$$

**3.** Fix some $H \in \mathbf{R}_{>0}$ and $d \in \mathbf{Z}_{>0}$. Let $\alpha$ be an algebraic number of degree at most $d$ with

$$H(\alpha) \leq H^{1/|\{\beta\in\overline{\mathbf{Q}}:\deg(\beta)\leq d, H(\beta)\leq H\}|}.$$

Prove that $\alpha$ is a root of unity or $\alpha = 0$.

Choose some value of $H$ and combine with Question 1 to get an explicit $H_0(d) > 1$ such that for a non-zero algebraic number $\alpha$ of degree $d$, $H(\alpha) < H_0(d)$ implies that $\alpha$ is a root of unity.

*Hint:* Consider the numbers $1, \alpha, \alpha^2, \dots, \alpha^N$ with $N = |\{\beta \in \overline{\mathbf{Q}} : \deg(\beta) \leq d, H(\beta) \leq H\}|$.

*Solution:* Let

$$N = |\{\beta \in \overline{\mathbf{Q}} : \deg(\beta) \leq D, H(\beta) \leq H\}|.$$

Let $\alpha$ be such that $\deg(\alpha) \leq D$ and $H(\alpha) \leq H^{1/N}$. Then

$$H(\alpha^k) = H(\alpha)^k \leq H(\alpha)^N \leq H.$$

Therefore, by the box principle, there are $k \neq l \in \{0, \dots, N\}$ such that $\alpha^k = \alpha^l$. Then $\alpha^{k-l} = 1$, so $\alpha$ is a root of unity. Taking e.g. $H = 2$ and using the bound from Question 1, we get that

$$H(\alpha) \leq 2^{1/12^{D(D+1)}}$$

implies that $\alpha$ is a root of unity. It is possible to improve on the value of the constant 12 by a more careful calculation or a better choice of $H$.

**4.** Let $\alpha$ be an algebraic number of degree $d$ and let $D \geq d$ a rational integer. Use Siegel's lemma to find a number $A$ such that a polynomial $P$ with $\deg P \leq D$, $H(P) \leq A$ and $P(\alpha) = 0$ exists. (Try to make $A$ as small as you can.) Use this to improve on the $H_0(d)$ you got in Question 3.

*Solution:* Let $\alpha$ be an algebraic number of degree at most $d$ and of height at most $H$. We use Siegel's lemma for the linear form

$$L = X_D\alpha^D + \ldots + X_1\alpha + X_0.$$

It follows directly from the definition that

$$H(L) = H(\alpha)^D \leq H^D.$$

The lemma gives integers $a_0, \ldots, a_D$ not all 0 such that

$$\max_j |a_j| \leq ((D+1)H^D)^{\frac{d}{D+1-d}} =: A.$$

and

$$a_d\alpha^D + \ldots + a_1\alpha + a_0 = 0.$$

It follows that the number of algebraic numbers of height at most $H$ of degree at most $d$ is at most

$$D(A+1)^D \leq (4A)^D \leq (2DH^D)^{2d}4^D$$

provided $D + 1 - d > D/2$, which we assume from now on.

It follows from the result of Question 3 that

$$H(\alpha) \leq H_0(d) := H^{1/(2DH^D)^{2d}4^D}$$

implies that $\alpha$ is a root of unity with any choice of $H$ and $D$. Setting $H$ such that $\log H = 1/D$, we get

$$H_0(d) \geq \exp((D(2eD)^{2d}4^D)^{-1}).$$

Taking $D = d\log d$, we get

$$H_0(d) \geq \exp(C_1^{-d\log d}) \geq 1 + C_2^{-d\log d}$$

with appropriate constants $C_1, C_2$.

*Remark:* Lehmer's conjecture predicts that one may take $H_0(d) = 1 + c/d$ for some $c > 0$. The best currently known bound is due to Dobrowolski, which is $H_0(d) = 1 + c(\log\log d)^3/d(\log d)^3$.

*Hint:* Taking $H = 2^{1/D}$ for the parameter in Question 3 and $D = 2d$ you should get that $H_0(d) = 1 + d^{-Cd}$ for an absolute constant $C$.

**5.** Let $P, Q \in \mathbf{Z}[X]$ with $Q|P$. Prove that

$$H(Q) \leq 2^{\deg Q}(\deg(P) + 1)H(P).$$

*Hint:* Prove that $M(P_1P_2) = M(P_1)M(P_2)$ for two polynomials $P_1, P_2 \in \mathbf{C}[X]$.

*Solution:* We show that $M(P_1P_2) = M(P_1)M(P_2)$ for any two polynomials $P_1, P_2$. Indeed, let $P_1(X) = a_{d_1}\prod_{j=1}^{d_1}(x-\alpha_j)$ and $P_2(X) = b_{d_2}\prod_{j=1}^{d_2}(x-\beta_j)$. Then

$$P_1(X)P_2(X) = a_{d_1}b_{d_2}\prod_{j=1}^{d_1}(x-\alpha_j)\prod_{j=1}^{d_2}(x-\beta_j),$$

and

$$M(P_1P_2) = |a_{d_1}b_{d_2}|\prod_{j=1}^{d_1}\max(1,|\alpha_j|)\prod_{j=1}^{d_2}\max(1,|\beta_j|) = M(P_1)M(P_2).$$

Now suppose $P = QR$ in $\mathbf{Z}[X]$. Then

$$H(Q) \le 2^{\deg Q}M(Q) = 2^{\deg Q}\frac{M(P)}{M(R)} \le 2^{\deg Q}M(P) \le 2^{\deg Q}(1+\deg P)H(P).$$

**6.** Let $a \in \mathbf{Z}_{\ge 3}$, and $d \in \mathbf{Z}_{\ge 2}$. Prove that the polynomial $X^d - aX^{d-1} + 1$ is irreducible, and it has exactly one root with absolute value greater than 1. Write $\alpha$ for this root. Prove that $a-1 < \alpha < a$, $|\alpha| = M(\alpha)$ and $|\alpha^{-1}| = M(\alpha^{-1})^{-1}$. Conclude the equality in Liouville's inequality is possible for any degree.

*Remark:* Real algebraic integers that are greater than 1 and all of whose Galois conjugates have modulus strictly less than 1 are called Pisot or PV numbers. They have many interesting properties.

*Hint:* Rouché's theorem can be used to locate the zeros of the polynomial. You may also find it helpful to consider the polynomial $1 - aX + X^d$. In proving irreducibility, you may consider weather it is possible for an algebraic integer to have all its Galois conjugates have modulus strictly less than 1.

*Solution:* The polynomial $X^d - aX^{d-1} + 1$ has the same number of complex roots with absolute value at least 1 as the polynomial $X^d - aX + 1$ has with absolute value at most 1. By Rouche's theorem, this has the same number of roots with absolute value at most 1 as $-aX+1$, that is 1, because $|-aX+1| > |X^d|$ for all $X$ with $|X| = 1$. Now

$$X^d - aX + 1|_{X=a} = 1 > 0$$

and

$$X^d - aX^{d-1} + 1|_{X=a-1} = (a-1)^d - a(a-1)^{d-1} + 1 = -(a-1)^{d-1} + 1 < 0$$

so there must be a root between $a$ and $a-1$, and we call this $\alpha$.

If $X^d - aX^{d-1} + 1$ was reducible, then at least one of its factors would have all its roots with absolute value less than 1, and their product would be the constant coefficient of the factor, a non-zero integer. This is not possible. By the definition of Mahler measure, $M(\alpha) = \alpha$. Hence $M(\alpha^{-1}) = M(\alpha) = \alpha$. It follows that $|\alpha| = M(\alpha)$

and $|\alpha^{-1}|^{-1} = M(\alpha^{-1})$, so equality is possible in the Liouville bound on both sides.

**7.**

(a) Let $\alpha$ be an algebraic number of degree $d$, and $p, q \in \mathbf{Z}$ with $q \neq 0$. Give an upper bound for $H(\alpha - p/q)$ and use this via Liouville's inequality to give a lower bound on $|\alpha - p/q|$.

(b) Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbf{Q}}_{\neq 0}$ and $b_1, \ldots, b_n \in \mathbf{Z}$. Give an upper bound for $H(\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1)$ and use this to show

$$|b_1 \log(\alpha_1) + \ldots + b_n \log(\alpha_n)| \geq \exp(-(D+1)\log 2 - (\log H(\alpha_1) + \ldots \log H(\alpha_n))DB),$$

where $D$ is the degree of the number field $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ and $B = \max(|b_1|, \ldots, |b_n|)$.

*Solution:* Part (a). We have

$$H(\alpha - p/q) \leq 2H(\alpha)H(p/q) = 2H(\alpha)\max(|p|, |q|).$$

Now the Liouville bound gives

$$|\alpha - p/q| \geq H(\alpha - p/q)^{-d} \geq (2H(\alpha)\max(|p|, |q|))^{-d}.$$

Part (b). By Proposition 28,

$$H(\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1) \leq 2(H(\alpha_1) \cdots H(\alpha_n))^B.$$

Using the Liouville bound, we have

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq H(\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1)^{-D} \geq \exp(-D\log 2 - (\log H(\alpha_1) + \ldots + \log H(\alpha_n))DB).$$

Then $|\log x| \geq |1 - x|/2$ gives

$$|b_1 \log(\alpha_1) + \ldots + b_n \log(\alpha_n)| \geq (1/2)\exp(-D\log 2 - (\log H(\alpha_1) + \ldots \log H(\alpha_n))DB),$$

which is equivalent to the claimed bound.

**8.**

(a) Let $K$ be a number field, and let $\alpha \in K$. Consider the number

$$\beta = \alpha^5 + (1 - \alpha)^5 - 1.$$

Prove that

$$|\beta|_v \leq 3\max(1, |\alpha|_v)^5 \max(1, |1 - \alpha|_v)^5$$

for all $v \in M_K$.

(b) Show that $\beta = 5P(\alpha)$ for some $P \in \mathbf{Z}[X]$ of degree 4. Use this to prove

$$|\beta|_v \leq |5|_v \max(1, |\alpha|_v)^4 \leq |5|_v \max(1, |\alpha|_v)^5 \max(1, |1 - \alpha|_v)^5$$

for all $v \in M_{K,f}$.

(c) Show that

$$H(\alpha)H(1-\alpha) \geq \left(\frac{5}{3}\right)^{1/5}$$

or $\alpha \in \{0, 1, (1 \pm \sqrt{-3})/2\}$.

*Hint:* Use the product formula for $\beta$.

*Solution:* Part (a). We have

$$|\beta|_v = |\alpha^5 + (1-\alpha)^5 - 1|_v \leq |\alpha|_v^5 + |1-\alpha|_v^5 + |1|_v.$$

Each of the three terms are not large than $\max(1, |\alpha|_v)^5 \max(1, |1-\alpha|_v)^5$, and the claimed bound follows.

Part (b). We have

$$\beta = \alpha^5 + (1-\alpha)^5 - 1 = -5\alpha + 10\alpha^2 - 10\alpha^3 + 5\alpha^4 = 5(-\alpha + 2\alpha^2 - 2\alpha^3 + \alpha^4).$$

Therefore,

$$|\beta|_v = |5|_v \max(1, |\alpha|_v)^4 \leq |5|_v \max(1, |\alpha|_v)^5 \max(1, |1-\alpha|_v)^5$$

for all $v \in M_{K,f}$.

Part (c). If $\beta \neq 0$, we apply the product formula for $\beta$ and get

$$\begin{aligned} 1 &= \prod_{v \in M_K} |\beta|_v^{d_v} \\ &\leq \prod_{v \in M_{K,\infty}} |3|_v^{d_v} \prod_{v \in M_{K,f}} |5|_v^{d_v} \prod_{v \in M_K} \max(1, |\alpha|_v)^{5d_v} \max(1, |1-\alpha|_v)^{5d_v} \\ &= \frac{3^{[K:\mathbf{Q}]}}{5^{[K:\mathbf{Q}]}} H(\alpha)^{5[K:\mathbf{Q}]} H(1-\alpha)^{5[K:\mathbf{Q}]}. \end{aligned}$$

The claim follows by dividing by $(3/5)^{[K:\mathbf{Q}]}$ and then taking order $5[K:\mathbf{Q}]$ roots.

It remains to analyse $\beta = 0$. To this end, we use

$$\beta = 5(-\alpha + 2\alpha^2 - 2\alpha^3 + \alpha^4) = 5\alpha(\alpha-1)(\alpha^2 - \alpha + 1).$$

Then $\beta = 0$ implies that $\alpha \in \{0, 1, (1 \pm \sqrt{-3})/2\}$.

**9.** Prove that for all real irrational algebraic $\alpha$ and $\varepsilon > 0$, there is an effective constant $C = C(\alpha, \varepsilon)$ such that the number of pairs of integers $p, q \in \mathbf{Z}$ with $q \neq 0$, $\gcd(p, q) = 1$ such that

$$|\alpha - p/q| < C^{-1} q^{-\sqrt{2d}-\varepsilon}$$

is at most $C$.

*Hint:* First convince yourself that the proof given in the lectures implies the existence of an effective constant $C_1 = C_1(\alpha, \varepsilon)$ such that the existence of some $p_1, q_1 \in \mathbf{Z}$ with $q_1 \neq 0$ and $|\alpha - p_1/q_1| < C_1^{-1} q_1^{-\sqrt{2d}-\varepsilon}$ implies that $|\alpha - p/q| > C_1^{-1} q^{-\sqrt{2d}-\varepsilon}$ for all $p, q \in \mathbf{Z}$ with $q > q_1^{C_1}$. Estimate the number of good rational approximations with denominators between $q_1$ and $q_1^C$ using the inequality $|p_1/q_1 - p/q| \geq 1/q_1 q$.

*Solution:* Following the proof of Theorem 30 given in the lectures we may find an effective constant $C_1 = C_1(\alpha, \varepsilon)$ such that if there

are $p_1/q_1, \widetilde{p}/\widetilde{q}$ such that $|\alpha - p_1/q_1| < q_1^{-\sqrt{2d}-\varepsilon}$, $|\alpha - \widetilde{p}/\widetilde{q}| < \widetilde{q}^{-\sqrt{2d}-\varepsilon}$, $\log q_1 > C_1$ and $\log \widetilde{q} > C_1 \log q_1$, then the argument for the proof of Theorem 30 yields a contradiction. (Take $C_1$ to be $C\varepsilon_0^{-1}$ in equation (23) in the notes. One needs to check the proof carefully to see that this is true.)

Now we need to show that the number of $p/q$ with $C_1 \log q_1 > \log q > \log q_1$ and

$$|\alpha - p/q| < q^{-\sqrt{2d}-\varepsilon}$$

may be bounded by an effective constant $C_2$ independent of $q_1$. If we show this then there can be at most $e^{C_1} + 1 + C_2$ exceptionally good rational approximation to $\alpha$. There are at most $e^{C_1}$ with $\log q \le C_1$, then the smallest one with $\log q > C_1$, which plays the role of $q_1$ and $C_2$ with $C_1 \log q_1 > \log q > \log q_1$. There can be no more, because if there was, we could take that as $\widetilde{p}/\widetilde{q}$.

Now let $p_2/q_2, p_3/q_3, \ldots \in \mathbf{Q}$ be all the rational approximation of $\alpha$ such that $|\alpha - p_i/q_i| < q_i^{-\sqrt{2d}}$ and $q_1 < q_2 < q_3 < \ldots$. (We dropped the $\varepsilon$ in the exponent, because we do not need it. All we need for the argument is that the exponent is $> 2$.) Then

$$|p_i/q_i - p_{i+1}/q_{i+1}| \le |\alpha - p_i/q_i| + |\alpha - p_{i+1}/q_{i+1}| \le 2q_i^{-\sqrt{2d}}.$$

On the other hand

$$|p_i/q_i - p_{i+1}/q_{i+1}| = \frac{|p_i q_{i+1} - p_{i+1} q_i|}{q_i q_{i+1}} \ge 1/q_i q_{i+1}.$$

Comparing the upper and lower bounds, we get

$$q_i^{\sqrt{2d}-1} \le 2q_{i+1}.$$

For any $t < \sqrt{2d} - 1$, we have

$$\log q_{i+1} \ge t \log q_i$$

provided $q_i$ is sufficiently large depending on this $t$ and $d$, which we assume, as we may. Iterating this, we get $\log q_i \ge t^{i-1} \log q_1$. Hence we have the claim with $C_2 \le \log C_1 / \log t$.

**10.** The following statement in known as Dyson's lemma.

**Lemma.** *Let $m \in \mathbf{Z}_{\ge 1}$, and let $x_1, \ldots, x_m \in \mathbf{C}$ and $y_1, \ldots, y_m \in \mathbf{C}$ be two sets of distinct numbers. Let $t_1, \ldots, t_m \in [0, 1]$. Let $P \in \mathbf{C}[X_1, X_2]$ be a non-zero polynomial of degree at most $n_1$ in $X_1$ and $n_2$ in $X_2$. Suppose*

$$I_P(x_j, y_j; n_1^{-1}, n_2^{-1}) \ge t_j$$

*for $j = 1, \ldots, m$. Then*

$$\sum_{j=1}^{m} \frac{t_j^2}{2} \le 1 + \max\Big(\frac{m-2}{2}, 0\Big) \frac{n_2}{n_1}.$$

For a slightly more general version of the above lemma, see [Bombieri, Acta Math. **148** (1982)].

Give a proof of Dyson's Diophantine exponent $\sqrt{2d}+\varepsilon$ (Theorem 29) using Dyson's lemma instead of the non-vanishing result in Section 3.3.

*Hint:* Use that $I_P(\alpha_j,\alpha_j;w_1,w_2)=I_P(\alpha,\alpha;w_1,w_2)$ for any Galois conjugate $\alpha_j$ of $\alpha$ when $P\in\mathbf{Z}[X_1,X_2]$.

*Solution:* Let $\alpha$, $\varepsilon$ and $p_1/q_1$, $p_2/q_2$ be as in the proof of Dyson's Diophantine exponent. For the argument to work, we need an auxiliary polynomial $\widetilde{P}\in\mathbf{Z}[X_1,X_2]$ of degree at most $n_1$ in $X_1$ and $n_2$ in $X_2$ and of height at most $C^{n_1+n_2}$ such that

$$I_{\widetilde{P}}(\alpha,\alpha;\log q_1,\log q_2)\geq\frac{n_1\log q_1+n_2\log q_2}{\sqrt{2d}+\varepsilon/5}$$

and

$$\widetilde{P}(p_1/q_1,p_2/q_2)\neq 0.$$

Here $C$ is a constant that depends only on $\alpha$ and $\varepsilon$, and $n_1$ and $n_2$ are large integers such that $n_1\log q_1$ is very close to $n_2\log q_2$.

Fix some $\widetilde{\varepsilon}>0$, which will be chosen in terms of $\varepsilon$ later. Applying Siegel's lemma in the same way as in the lectures, we find a polynomial $P\in\mathbf{Z}[X_1,X_2]$ with height at most $C^{n_1+n_2}$ and

$$I_P(\alpha,\alpha;\log q_1,\log q_2)\geq\frac{n_1\log q_1+n_2\log q_2}{\sqrt{2d}+\widetilde{\varepsilon}}$$

If $n_1\log q_1$ and $n_2\log q_2$ are close enough, then this implies

$$I_P(\alpha,\alpha;n_1^{-1},n_2^{-1})\geq\frac{2}{\sqrt{2d}+2\widetilde{\varepsilon}}.$$

We also have

$$I_P(\alpha_i,\alpha_i;n_1^{-1},n_2^{-1})\geq\frac{2}{\sqrt{2d}+2\widetilde{\varepsilon}}$$

for all Galois conjugates $\alpha_1,\dots,\alpha_d$ of $\alpha$, and define

$$I_P(p_1/q_1,p_2/q_2;n_1^{-1},n_2^{-1})=:\kappa.$$

We apply Dyson's lemma for $P$, $m=d+1$ and the points

$$(\alpha_1,\alpha_1),\dots,(\alpha_d,\alpha_d),(p_1/q_1,p_2/q_2)$$

in the role of $(x_j,y_j)$. We get

$$d\Big(\frac{2}{\sqrt{2d}+2\widetilde{\varepsilon}}\Big)^2\cdot\frac{1}{2}+\kappa^2/2\leq 1+\frac{d-1}{2}\frac{n_2}{n_1}.$$

There is an appropriate constant $C_2=C_2(d)$ such that

$$\Big(\frac{2}{\sqrt{2d}+2\widetilde{\varepsilon}}\Big)^2\geq\frac{4}{2d}-C_2\widetilde{\varepsilon}$$

provided $\widetilde{\varepsilon} < 1$, which we assume. All in all, we get

$$1 - C_2 d\widetilde{\varepsilon}/2 + \kappa^2/2 \leq 1 + \frac{d-1}{2}\frac{n_2}{n_1}$$

Since $n_1 \log q_1$ is close to $n_2 \log q_2$ we may force $n_2/n_1$ to be arbitrarily small if we force $\log q_2$ to be much larger than $\log q_1$. We can force

$$\frac{d-1}{2}\frac{n_2}{n_1} \leq \widetilde{\varepsilon},$$

and hence get

$$\kappa \leq C_3 \widetilde{\varepsilon}^{1/2}$$

for some $C_3 = C_3(d)$.

Taking an appropriate partial derivative of $P$ as $\widetilde{P}$, we get

$$I_{\widetilde{P}}(\alpha, \alpha; n_1^{-1}, n_2^{-1}) \geq \frac{2}{\sqrt{2d} + 2\widetilde{\varepsilon}} - \kappa.$$

and

$$\widetilde{P}(p_1/q_1, p_2/q_2) \neq 0.$$

If we make $\widetilde{\varepsilon}$ sufficiently small in terms of $\varepsilon$ and $d$ we have

$$\frac{2}{\sqrt{2d} + 2\widetilde{\varepsilon}} - \kappa \geq \frac{2}{\sqrt{2d} + \varepsilon/10}.$$

Now using again that $n_1 \log q_1$ is close to $n_2 \log q_2$, we get

$$I_{\widetilde{P}}(\alpha, \alpha; \log q_1, \log q_2) \geq \frac{n_1 \log q_1 + n_2 \log q_2}{\sqrt{2d} + \varepsilon/5},$$

and the proof can be completed as in the lectures.

**11.** Fix some numbers $\varepsilon, C > 0$. Suppose that $\varepsilon$ is smaller than a suitable absolute constant (e.g. $\varepsilon \leq 1/6$ would do). Show that there are $n_1, n_2 \in \mathbf{Z}_{\geq 1}$, $p_1/q_1, p_2/q_2 \in \mathbf{Q}$ and a polynomial $0 \neq P \in \mathbf{Z}[X_1, X_2]$ of degree at most $n_1$ in $X_1$ and $n_2$ in $X_2$ such that the following holds.

$$\exp(n_1 + n_2) \leq q_j^{n_j/C},$$
$$H(P) \leq q_j^{n_j/C}$$

for $j = 1, 2$,

$$I_P(p_1/q_1, p_2/q_2; \log q_1, \log q_2) \geq \varepsilon(n_1 \log q_1 + n_2 \log q_2)$$

and

$$\log q_2 \geq (10\varepsilon)^{-1} \log q_1.$$

It is useful to consider $P$ of the form $(F(X_1) - G(X_1)X_2)^n$ and evaluate it at $(X_1, X_2) = (p_1/q_1, p_2/q_2)$ with $p_2/q_2 = F(p_1/q_1)/G(p_1/q_1)$ for some choice of $p_1/q_1$.

Compare this with the non-vanishing result in Section 3.3.

*Solution:* Fix two polynomials $F, G \in \mathbf{Z}[X_1]$ of degree $d$ for some $d \in \mathbf{Z}_{\geq 1}$ to be specified later. Write

$$h = \max(H(F), H(G)).$$

We consider $P = (F(X_1) - G(X_1)X_2)^n$ for a fixed large $n \in \mathbf{Z}_{\geq 1}$.

The degree of $P$ in $X_1$ is $n_1 = dn$ and its degree in $X_2$ is $n_2 = n$. Using the inequalities $\mathcal{L}(P_1P_2) \leq \mathcal{L}(P_1)\mathcal{L}(P_2)$ and $H(Q) \leq \mathcal{L}(Q) \leq (\deg(Q) + 1)H(Q)$, we get

$$H(P) \leq (2d + 2)^n h^n.$$

Now fix an interval $K \subset \mathbf{R}$ where neither $F$ nor $G$ vanishes so there is a constant $C_0$ such that

$$C_0^{-1} \leq |F(x)|, |G(x)| \leq C_0$$

for $x \in K$.

Now we choose $p_1/q_1 \in K \cap \mathbf{Q}$ in such a way that $p_2 := q_1^d F(p_1/q_1)$ and $q_2 := q_1^d G(p_1/q_1)$ are coprime integers. The simplest way to guarantee this is by choosing $G(X_1) = X_1^d$ and choosing $F$ to have constant coefficient 1. Then $q_1^d G(p_1/q_1) = p_1^d$, on the other hand all but the constant term in $q_1^d F(p_1/q_1)$ is divisible by $p_1$. Then $C_0^{-1} q_1^d \leq q_2 \leq C_0 q_1^d$. In particular, if $q_1$ is chosen large enough, then $q_2 > q_1$.

Observe that all partial derivatives of $P$ of order less than $n$ is divisible by $F(X_1) - G(X_1)X_2$, hence all of these partial derivatives vanish at $(p_1/q_1, p_2/q_2)$. Therefore

$$I_P(p_1/q_1, p_2/q_2; \log q_1, \log q_2) \geq n \log q_1 \geq \frac{1}{3d}(n_1 \log q_1 + n_2 \log q_2).$$

provided $q_1$ is sufficiently large so that

$$n_2 \log q_2 = (n_1/d) \log q_2 \leq n_1(\log q_1 + \log C_0) \leq 2n_1 \log q_1.$$

In addition, again if $q_1$ is large enough then

$$\log q_2 \geq d \log q_1 - \log C_0 \geq d/2 \log q_1.$$

Therefore, the final two conditions asked in the question are satisfied provided we set $d$ such that $d/2 \geq (10\varepsilon)^{-1}$ and $\varepsilon \leq 1/3d$, that is if

$$(5\varepsilon)^{-1} \leq d \leq (3\varepsilon)^{-1}.$$

This is always possible to do provided $\varepsilon \leq 1/6$.

Finally, if we set $q_1$ large enough depending on $d$, $h$ and $C$, then the first two conditions will also hold.