EXAMPLE SHEET 4 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 Questions 2 and 4, by Monday 20 January at 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.

1. The goal of this question is to prove a special case of Theorem 47 with an effective constant following an argument of Runge.

Let $d \in \mathbf{Z}_{\geq 3}$, and let $F \in \mathbf{Z}[X, Y]$ be a homogeneous polynomial of degree d without repeated factors, which is *reducible* in $\mathbf{Z}[X, Y]$. Let $G \in \mathbf{Z}[X, Y]$ be a polynomial of degree at most $d - 1$. Suppose that $P = F - G$ is irreducible in $\mathbf{Z}[X, Y]$, and for simplicity $Y \nmid F$.

In what follows you may use without proof the following statement. With

$$F(X, Y) = (X - \alpha_1 Y) \cdots (X - \alpha_d Y)$$

there is some number $R \in \mathbf{R}_{>0}$ and for each $j = 1, \ldots, d$, there is a series

$$\varphi_j(Y) = \alpha_j Y + \beta_{j,0} + \beta_{j,1} Y^{-1} + \ldots$$

such that the following holds. We have $\beta_{j,n} \in \mathbf{Q}(\alpha_j)$ for all $j = 1, \ldots, d$ and $n \in \mathbf{Z}_{\geq 0}$. The series φ_j converges for $Y \in \mathbf{C}$, $|Y| > R$. Furthermore, for all $x, y \in \mathbf{C}$ with $|y| > R$ and $P(x, y) = 0$, we have $x = \varphi_j(y)$ for some j. (That is, $(\varphi_j(y), y)$ for $j = 1, \ldots, d$ are parametrizations of the complex solutions of $P(x, y) = 0$ for large $|y|$.)

(a) Prove that for each $j = 1, \ldots, d$, there is a polynomial $Q(X, Y) \in \mathbf{Z}[X, Y]$ of degree at most $[\mathbf{Q}(\alpha_j) : \mathbf{Q}]$ in the X variable such that

$$Q_j(\varphi_j(Y), Y) = \gamma_{j,1} Y^{-1} + \gamma_{j,2} Y^{-2} + \ldots$$

for some $\gamma_{j,n} \in \mathbf{C}$.

(b) Prove that for all $x, y \in \mathbf{Z}$ with $|y| > R$ and $P(x, y) = 0$, we have $Q_j(x, y) = 0$ for some $j = 1, \ldots, d$.

(c) Prove that for all $x, y \in \mathbf{Z}$ with $P(x, y) = 0$, we have $|x| + |y| < C$ for some effective constant depending only on P.

Comment: The fact that

$$X = \alpha_j Y + \beta_{j,0} + \beta_{j,1} Y^{-1} + \ldots + \beta_{j,n} Y^{-n} + O(Y^{-n-1})$$

for large solutions of $P(X,Y)=0$ for some j and $\beta_{j,k} \in \mathbf{Q}(\alpha_j)$, where n can be taken arbitrarily large may be proved following the proof of Lemma 49. This weaker fact is, in fact, enough to solve the question. The convergence of the resulting series requires another proof. One way to do this is contained in Lemmata 4.4 and 4.5 in the book of Masser (reference [9] in the notes.)

Hint: (a) Write up the conditions to be satisfied as a system of linear equations for the coefficients of the polynomial Q_j. If the degree in Y is large enough, you should have more variables than linear constraints over $\mathbf{Q}$. (b) Prove that $Q_j(x,y)$ is an integer with absolute value less than 1. (c) You need to show that P and Q_j have no common factors. Use the irreducibility of P and what you know about the degrees in X.

2. In this question, you may use the following version of the subspace theorem.

Theorem. *Let K be a number field and let $n \geq 2$. Let $S \subset M_K$ be finite containing all the infinite places. For each $v \in S$, let $L_1^{(v)}, \ldots, L_n^{(v)}$ be linearly independent linear forms in n variables with algebraic coefficients. Fix an extension of $|\cdot|_v$ to a number field that contains all the coefficients of the linear forms for each $v \in S$. Then for all $\varepsilon > 0$, the solutions $(x_1, \ldots, x_n) \in \mathcal{O}_K^n$ of*

$$\prod_{v \in S} \prod_{j=1}^{n} |L_j^{(v)}(x_1, \ldots, x_n)|_v^{d_v} \leq H(x_1, \ldots, x_n)^{-\varepsilon}$$

are contained in a finite union of proper subspaces of K^n.

Here $H(x_1, \ldots, x_n)^{[K:\mathbf{Q}]} = \prod_{v \in M_K} \max(|x_1|_v, \ldots, |x_n|_v)^{d_v}$, but it could also be replaced by $\max(H(x_1), \ldots, H(x_n))$ if you prefer that.

(a) Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be non-zero algebraic numbers, and let K be a number field. Prove that there is a finite set $A \subset \mathcal{O}_K^\times$ depending only on $\alpha_1, \ldots, \alpha_n$ and K such that all solutions $(x_1, \ldots, x_n) \in (\mathcal{O}_K^\times)^n$ of the generalized unit equation

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = 0$$

satisfies that $x_i/x_j \in A$ for some $i \neq j$.

(b) In the setting of the previous part, prove that there is a finite set $A \subset \mathcal{O}_K^\times$ depending only on $\alpha_1, \ldots, \alpha_n$ and K such that for all solutions $(x_1, \ldots, x_n) \in (\mathcal{O}_K^\times)^n$ of the above equation, the index set $\{1, \ldots, n\}$ may be partitioned as $I_1 \cup \cdots \cup I_k$ such that $x_i/x_j \in A$ whenever $i, j \in I_l$ for some $l = 1, \ldots, k$ and

$$\sum_{j \in I_l} \alpha_j x_j = 0$$

for all $l = 1, \ldots, k$.

Hint: For (a) use an argument similar to the proof of Proposition 57 from the lectures but use the above form of the subspace theorem with the set of infinite places as S. For (b) use (a) to show that $\alpha_j = \beta\alpha_i$ for some $\beta \in A$ and some $i \neq j$. Then use this to eliminate α_j and reduce to an equation in $n-1$ variables.

3. Fix some $n \in \mathbf{Z}_{>1}$ and consider the vector space

$$V = \mathbf{Q}^{n^2}/\{(y, \ldots, y) : y \in \mathbf{Q}\}.$$

If $a, b \in \mathbf{Z}_{>1}$, write $e_1(a,b), \ldots, e_{n^2}(a,b)$ for an enumeration of the numbers $a^i b^j$ for $i, j = 0, \ldots, n-1$. (The enumeration is independent of a, b.)

Let $d = \gcd(a-1, b-1)$, and let $\Lambda_1, \ldots, \Lambda_{n^2-1}$ be a basis of V^* and let $v \in \{2, 3, \infty\}$. Prove that there are infinitely many choices for multiplicatively independent $a, b \in \{2^i 3^j : i, j \in \mathbf{Z}_{\geq 1}\}$ such that

$$\prod_{j=1}^{n^2-1} |\Lambda_j(e_1/d, \ldots, e_{n^2}/d)|_v > c|a|_v^{n^2(n-1)/2-n+1}|b|_v^{n^2(n-1)/2-n+1}$$

if $v = 2$ or 3 and

$$\prod_{j=1}^{n^2-1} |\Lambda_j(e_1/d, \ldots, e_{n^2}/d)|_v > c|a|_v^{n^2(n-1)/2}|b|_v^{n^2(n-1)/2}d^{-n^2+1}$$

if $v = \infty$. Here c is a constant that depends only on the functionals and v.

Conclude that the choice of the forms used in the proof of Theorem 56 is optimal up to a multiplicative constant.

Hint: Observe that you may write each Λ_j in the form $a_1 Y_1 + \ldots + a_{n^2} Y_{n^2}$, where $a_1, \ldots, a_{n^2} \in \mathbf{Q}$ are some numbers depending on j such that $a_1 + \ldots + a_{n^2} = 0$, and $Y_1, \ldots, Y_{n^2}$ are the coordinates on $\mathbf{Q}^{n^2}$. Choose a and b in such a way that $|e_1|_v, \ldots, |e_{n^2}|_v$ are distinct and far apart from one another depending on the size of the coefficients of the Λ_j in the above representation.

4. Let K be a number field. Prove that there is an effective constant depending only on K such that any solution $\alpha, \beta \in \mathcal{O}_K^\times$ of

$$\alpha + \beta = 1$$

satisfies $H(\alpha), H(\beta) \leq C$.

Hint: Pick a fundamental system of units $u_1, \ldots, u_r \in \mathcal{O}_K^\times$. Prove that for all $n_1, \ldots, n_r$, there is at least one place $v \in M_{K,\infty}$ such that

$$|u_1^{n_1} \cdots u_r^{n_r}|_v > (1+c)^{\max(|n_1|, \ldots, |n_r|)}$$

for some $c > 0$ depending only on K and the choice of $u_1, \ldots, u_r$. Use the logarithmic embedding to do this and that a vector cannot be almost orthogonal to all the coordinate axes.

Write α and β as products of roots of unity and powers of the fundamental units. Prove that if $\alpha + \beta = 1$, then $|\alpha/\beta + 1|_v$ is exponentially small in the exponents that appear in the representation of α and β for a suitable v.

Use the embedding into $\mathbf{C}$ associated to v and lower bounds for linear forms in logarithms.

5. Let $m \in \mathbf{Z}_{\geq 1}$ and let $\alpha_1, \ldots, \alpha_m \in \overline{\mathbf{Q}}_{\neq 0}$ be such that α_i/α_j is not a root of unity for any $1 \leq i \neq j \leq m$. Let $P_1, \ldots, P_m \in \overline{\mathbf{Q}}[X]$ be non-zero polynomials. Use the version of the subspace theorem in Question 2 to prove that there are finitely many $n \in \mathbf{Z}$ such that

$$P_1(n)\alpha_1^n + \ldots + P_m(n)\alpha_m^n = 0.$$

Hint: It is enough to prove the finiteness for $n \in \mathbf{Z}_{\geq 0}$. Show that you may assume without loss of generality that all α_j and the coefficients of all P_j are algebraic integers. Let K be a number field containing all the α_j and all the coefficients. Let $S \subset M_K$ be finite such that $|\alpha_j|_v = 1$ for all j and all $v \notin S$. Use the subspace theorem on the space

$$V = \{(x_1, \ldots, x_m) \in K^m : x_1 + \ldots + x_m = 0\}$$

and for the places S. Choose the functionals from among $\{X_1, \ldots, X_m\}$ for each $v \in S$. Prove that there is $v \in S$ such that $|\alpha_1|_v, \ldots, |\alpha_m|_v$ are not all equal.

6. In the setting of the previous question, assume that $|\alpha_1| > |\alpha_j|$ for all $j \geq 3$, but we permit $|\alpha_1| = |\alpha_2|$. (We fix an embedding into $\mathbf{C}$.) Use lower bounds for linear forms in logarithms to prove that there is an effective constant C depending only on $\alpha_1, \ldots, \alpha_m$ and $P_1, \ldots, P_m$ such that

$$P_1(n)\alpha_1^n + \ldots + P_m(n)\alpha_m^n \neq 0.$$

for all $|n| > C$.

Hint: Let K be as in the previous hint. If $m = 2$, show that there is a $v \in M_K$ such that $|\alpha_1|_v \neq |\alpha_2|_v$ and finish using just this without linear forms in logarithms.

If $m > 2$ and $|\alpha_1| = |\alpha_2|$, then show that

$$-\frac{P_1(n)}{P_2(n)}\Big(\frac{\alpha_1}{\alpha_2}\Big)^n$$

is very close to 1 for those n with $P_1(n)\alpha_1^n + \ldots + P_m(n)\alpha_m^n = 0$ and use lower bounds for linear forms in logarithms.

Use the $m = 2$ case to deal with the potential vanishing of your linear form in logarithms.

7. Let $x \in (0,1)$ be a number with base 10 digit expansion $0.x_1x_2x_3\ldots$. We say that the expansion has long repetitions if there is some $\varepsilon > 0$ and infinitely many $n \in \mathbf{Z}_{>0}$ such that $x_1x_2\ldots x_n$ contains two identical substrings of length $\lceil \varepsilon n \rceil$. That is to say, there are $1 \le k < m \le n-l+1$ and $l = \lceil \varepsilon n \rceil$ such that $\alpha_{k+j} = \alpha_{m+j}$ for $j = 0, \ldots, l-1$.

(a) Suppose that $x \in (0,1)$ has long repetitions in its base 10 digit expansion. Prove that there is $\varepsilon > 0$ and infinitely many $n \in \mathbf{Z}_{>0}$ such that there are integers $0 \le k \ne m \le n$ and $A \in \mathbf{Z}$ with
$$|10^m x - 10^k x - A| \le 10^{-\varepsilon n}.$$

(b) Use the p-adic subspace theorem (E.g. Theorem 59 should suffice) to show that if $x \in (0,1)$ has long repetition in its base 10 digit expansion, then x is either rational or transcendental.

Comment: This is a result of Adamczewski, Bugeaud and Luca.

Hint: (a): With k, m as in the definition of long repetitions, show that $10^{k-1}x$ and $10^{m-1}x$ are close to each other in $\mathbf{R}/\mathbf{Z}$. (b): Use $S = \{2, 5, \infty\}$. Suppose x is algebraic. Use the coordinate functions as your linear forms together with $xX_1 - xX_2 - X_3$ for $v = \infty$ and evaluate them at the point $(10^m, 10^k, A)$. Prove that if a proper linear subspace contains infinitely many solutions of the inequality in your application of the subspace theorem then it is given by the equation $xX_1 - xX_2 - X_3 = 0$. Conclude that x is rational.