Introduction to Diophantine methods *Michel Waldschmidt*
http://www.math.jussieu.fr/~miw/coursHCMUNS2007.html

Exercises

Solve as many as you can, but at least 2, of the following exercises.
Deadline: Monday, october 1, 2007, 1:30 pm. [6]

Exercise 1. Recall the geometric construction given in § 1.1 : *starting with a rectangle of sides* 1 *and* x*, split it into a maximal number of squares of sides* 1*, and if a second smaller rectangle remains repeat the construction: split it into squares as much as possible and continue if a third rectangle remains.*
a) Prove that the number of squares in this process is the sequence of integers $(a_n)_{n\geq 0}$ in the continued fraction expansion of x.
b) Start with a unit square. Put on top of it another unit square: you get a rectangle with sides 1 and 2. Next put on the right a square of sides 2, which produces a rectangle with sides 2 and 3. Continue the process as follows: when you reach a rectangle of small side a and large side b, complete it with a square of sides b, so that you get a rectangle with sides b and $a+b$.
Which is the sequence of sides of the rectangles you obtain with this process?
Generalizing this idea, deduce a geometrical construction of the rational number having continued fraction expansion

$$[a_0; a_1, \ldots, a_k].$$

Exercise 2. Let $b \geq 2$ be an integer. Show that a real number x is rational if and only if the sequence $(d_n)_{n\geq 1}$ of digits of x in the expansion in basis b

$$x = [x] + d_1 b^{-1} + d_2 b^{-2} + \cdots + d_n b^{-n} + \cdots \qquad (0 \leq d_n < b)$$

is ultimately periodic (see § 1.1).
Deduce another proof of Lemma 1.17 in § 1.3.5.

Exercise 3. Let $b \geq 2$ be an integer. Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers and $(u_n)_{n\geq 0}$ an increasing sequence of positive numbers. Assume there exists $c > 0$ such that, for all sufficiently large n,

$$u_n - u_{n-1} \geq cn.$$

Show that the number

$$\vartheta = \sum_{n\geq 0} a_n b^{-u_n}$$

is irrational if and only if the set $\{n \geq 0\,;\; a_n \neq 0\}$ is infinite.
Compare with Lemma 1.17 in § 1.3.5.

[6]Updated: February 20, 2008

Exercise 4. Recall the proof, given in in § 1.1 of the irrationality of the square root of an integer n, assuming n is not the square of an integer: *by contradiction, assume $\sqrt{n}$ is rational and write $\sqrt{n} = a/b$ as an irreducible fraction; notice that b is the least positive integer such that $b\sqrt{n}$ is an integer; denote by m the integral part of $\sqrt{n}$ and consider the number $b' = (\sqrt{n} - m)b$. Since $0 < b' < b$ and $b'\sqrt{n}$ is an integer, we get a contradiction.*

Extend this proof to a proof of the irrationality of $\sqrt[k]{n}$, when n and k are positive integers and n is not the k-th power of an integer.

Exercise 5. Let α be a complex number. Show that the following properties are equivalent.
(i) The number α is algebraic.
(ii) The numbers $1, \alpha, \alpha^2, \ldots$ are linearly dependent over $\mathbb{Q}$.
(iii) The $\mathbb{Q}$-vector subspace of $\mathbb{C}$ spanned by the numbers $1, \alpha, \alpha^2, \ldots$ has finite dimension.
(iv) There exists an integer $N \geq 1$ such that the $\mathbb{Q}$-vector subspace of $\mathbb{C}$ spanned by the N numbers $1, \alpha, \alpha^2, \ldots, \alpha^{N-1}$ has dimension $< N$.
(v) There exists positive integers $n_1 < n_2 < \ldots < n_k$ such that $\alpha^{n_1}, \ldots, \alpha^{n_k}$ are linearly dependent over $\mathbb{Q}$.

Exercise 6. Recall the definition of the Smarandache function given in § 1.2.7 Prove that for any $p/q \in \mathbb{Q}$ with $q \geq 2$,

$$\left| e - \frac{p}{q} \right| > \frac{1}{(S(q)+1)!} \cdot$$

Exercise 7. Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers.
a) Prove that the following conditions are equivalent:
(i) The number

$$\vartheta_1 = \sum_{n\geq 0} \frac{a_n}{n!}$$

is rational.
(ii) There exists $N_0 > 0$ such that $a_n = 0$ for all $n \geq N_0$.
b) Prove that these properties are also equivalent to
(iii) The number

$$\vartheta_2 = \sum_{n\geq 0} \frac{a_n 2^n}{n!}$$

is rational.

Exercise 8. Complete the proof of (iii)⇒(iv) in Lemma 1.6.

Exercise 9. Extend the irrationality criterion Lemma 1.6 by replacing $\mathbb{Q}$ by $\mathbb{Q}(i)$.

Exercise 10. Check that any solution (m, m_1, m_2) of Markoff's equation (1.15) is in Markoff's tree.
`(See § 1.4.1 ).`

Exercise 11. a) Check that Liouville's inequality in Lemma 2.12 holds with d the degree of the minimal polynomial of α and c given by

$$c = \frac{1}{1 + \max\limits_{|t-\alpha|\le 1} |P'(t)|}.$$

where $P \in \mathbb{Z}[X]$ is the minimal polynomial of α.
b) Check also that the same estimate is true with again d the degree of the minimal polynomial P of α and c given by

$$c = \frac{1}{a_0 \prod\limits_{i=2}^{d} (|\alpha_j - \alpha| + 1)},$$

where a_0 is the leading coefficient and $\alpha_1, \ldots, \alpha_d$ the roots of P with $\alpha_1 = \alpha$:

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_d).$$

Exercise 12. Let m and n be positive integers and ϑ_{ij} $(1 \le i \le n,\ 1 \le j \le m$ be mn real numbers. Let $Q \ge 1$ be a positive integer. Show that there exists rational integers $q_1, \ldots, q_m,\ p_1, \ldots, p_n$ with

$$1 \le \max\{|q_1|,\ \ldots,\ |q_m|\} < Q^{n/m}$$

and

$$\max_{1\le i\le n} |\vartheta_{i1} q_1 + \cdots + \vartheta_{im} q_m - p_i| \le \frac{1}{Q}.$$

Deduce that if $\vartheta_1, \ldots, \vartheta_m$ are real numbers and H a positive integer, then there exists a tuple $(a_0, a_1, \ldots, a_m)$ of rational integers such that

$$0 < \max_{1\le i\le m} |a_i| \le H \quad \text{and} \quad |a_0 + a_1\vartheta_1 + \cdots + a_m\vartheta_m| \le H^{-m}.$$

Exercise 13. Let $f_1, \ldots, f_m$ be analytic functions of one complex variable near the origin. Let $d_0, d_1, \ldots, d_m$ be non-negative integers. Set

$$M = d_0 + d_1 + \cdots + d_m + m.$$

a) Show that there exists a tuple $(A_0, \ldots, A_m)$ of polynomials in $\mathbb{C}[X]$, not all of which are zero, where A_i has degree $\le d_i$, such that the function

$$A_0 + A_1 f_1 + \cdots + A_m f_m$$

has a zero at the origin of multiplicity $\ge M$.
`(This is Exercise 9 .)`
b) Give an explicit solution (A_0, A_1) in the case $m = 1$ and $f_1(z) = e^z$.

Exercise 14. Prove the implication (i)⇒(ii) in lemma 2.2 in the special cases $m = 1$, $m = 2$ and $m = 3$.

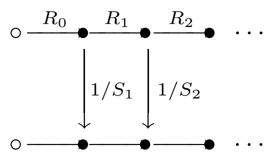
Exercise 15. a) Let b be a positive integer. Give the continued fraction expansion of the number

$$\frac{-b+\sqrt{b^2-4}}{2}.$$

b) Let a and b be two positive integers. Write a degree 2 polynomial with integer coefficients having a root at the real number whose continued fraction expansion is

$$[0;\overline{a,b}].$$

Exercise 16. Check that the resistance of the following network for the circuit



R_i: resistances in series

$1/S_j$: resistances in parallele

is given by the continued fraction

$$[R_0; S_1, R_1, S_2, R_2 \ldots]$$

(See § 2.2.2).

Exercise 17. Using Hermite's method as explained in § 2.1, prove that for any non-zero $r \in \mathbb{Q}(i)$, the number e^r is transcendental.

Exercise 18. Let $(v_n)_{n\geq 1}$ be a sequence of positive integers. Check that the following properties are equivalent.
(i) $\lim_{n\to\infty} v_n = +\infty$.
(ii) For any integer $k \geq 1$, the set of $n \geq 1$ such that $v_n = k$ is finite.
Remark. This question is related with Pillai's Conjecture.

Exercise 19. Prove that the following conditions are equivalent.
(i) There exists $c_1 > 0$ such that, for any pair (a, b) of integers satisfying $a \geq 3$ and $b \geq 2$,

$$|e^b - a| \geq a^{-c_1}.$$

(ii) There exists $c_2 > 0$ such that, for any pair (a, b) of integers satisfying $a \geq 3$ and $b \geq 2$,

$$|e^b - a| \geq e^{-c_2 b}.$$

(vii) There exists $c_3 > 0$ such that, for any pair (a, b) of integers satisfying $a \geq 3$ and $b \geq 2$,

$$|b - \log a| \geq a^{-c_3}.$$

(viii) There exists $c_4 > 0$ such that, for any pair (a, b) of integers satisfying $a \geq 3$ and $b \geq 2$,

$$|b - \log a| \geq e^{-c_4 b}.$$

Exercise 20. Let m be a positive integer and $\epsilon > 0$ a real number. Show that there exists $q_0 > 0$ such that, for any $q \geq q_0$ and for any tuple $(q, p_1, \dots, p_m)$ of rational integers with $q > q_0$,

$$\max_{1 \leq \mu \leq m} \left| e^{\mu} - \frac{p_\mu}{q} \right| \geq \frac{1}{q^{1+(1/m)+\epsilon}}.$$

Is it possible to improve the exponent by replacing $1 + (1/m)$ with a smaller number?

`Hint.` Consider Hermite's proof of the transcendence of e (§ 2.1.3), especially Proposition 2.10. First check (for instance using Cauchy's formulae)

$$\max_{0 \leq j \leq m} \frac{1}{k!} |D^k f_j(\mu)| \leq c_1^n,$$

where c_1 is a positive real number which does not depend on n. Next, check that the numbers p_j and $q_{\mu j}$ satisfy

$$\max\{q_j, |p_{\mu j}|\} \leq (n!)^m c_2^m$$

for $1 \leq \mu \leq m$ and $0 \leq j \leq n$, where again $c_2 > 0$ does not depend on n. Then repeat the proof of Hermite in § 2.1 with n satisfying

$$(n!)^m c_3^{-2mn} \leq q < \big((n+1)!\big)^m c_3^{-2m(n+1)},$$

where $c_3 > 0$ is a suitable constant independent on n. One does not need to compute c_1, c_2 and c_3 in terms of m, one only needs to show their existence so that the proof yields the desired estimate.