UNIVERSITY OF NATURAL SCIENCES HO CHI MINH City
http://www.hcmuns.edu.vn/

Introduction to Diophantine methods: irrationality and transcendence

Michel Waldschmidt,
Professeur, Université P. et M. Curie (Paris VI)
http://www.math.jussieu.fr/~miw/coursHCMUNS2007.html

Examen – December 15, 2007
3 hours

We denote by $e^z = \sum_{n\geq 0} z^n/n!$ the exponential function ($z \in \mathbb{C}$) and by $\log x$ the Neperian logarithm of a positive real number x, so that

$$e^{\log x} = x \text{ for } x > 0 \quad \text{and} \quad \log e^t = t \text{ for } t \in \mathbb{R}.$$

Exercise 1. a) Prove that

$$\frac{\log 2}{\log 3}$$

is irrational.
b) Deduce that one at least of the two numbers $\log 2$, $\log 3$ is irrational.
c) Do you know whether both are irrational?

Exercise 2. For each of the following statements, say whether it is true or not, and explain your answer.
(i) If $x \in \mathbb{R}$ is irrational, then x^2 is irrational.
(ii) If $x \in \mathbb{R}$ is irrational, then $\sqrt{x}$ is irrational.
(iii) If x and y in $\mathbb{R}$ are irrational, then $x + y$ is irrational.
(iv) If x and y in $\mathbb{R}$ are irrational, then xy is irrational.
(v) If $x \in \mathbb{R}$ is irrational, then e^x is irrational.
(vi) If $x > 0$ is irrational, then $\log x$ is irrational.

Exercise 3. a) Let $f(X,Y) = aX^2 + bXY + cY^2 \in \mathbb{R}[X,Y]$ be a homogeneous quadratic polynomial with real coefficients and with positive discriminant

$$\Delta = b^2 - 4ac > 0.$$

Let $\epsilon > 0$. Show that there exists $(x,y) \in \mathbb{Z}^2$ with $(x,y) \neq (0,0)$ such that

$$|f(x,y)| \leq \sqrt{\Delta/5} + \epsilon.$$

`Hint:` *you may use a Theorem of Hurwitz.*
b) Let Δ be a positive real number. Give an example of a homogeneous quadratic polynomial f having discriminant Δ such that

$$\min\bigl\{|f(x,y)|\ ;\ (x,y) \in \mathbb{Z}\times\mathbb{Z},\ (x,y) \neq (0,0)\bigr\} = \sqrt{\Delta/5}.$$

c) Give an example of a homogeneous quadratic polynomial f having positive discriminant such that

$$\min\bigl\{|f(x,y)|\ ;\ (x,y)\in\mathbb{Z}\times\mathbb{Z},\ (x,y)\neq(0,0)\bigr\}=0.$$

Exercise 4. Let α be a complex number. Show that the following properties are equivalent.
(i) The number α is root of a polynomial of degree ≤ 2 with coefficients in $\mathbb{Q}(i)$
(ii) The $\mathbb{Q}(i)$–vector space spanned by 1, α, α^2, $\alpha^3\dots$ has dimension ≤ 2.
(iii) For any integer $m\ge 1$, the number α^m is root of a polynomial of degree ≤ 2 with coefficients in $\mathbb{Q}(i)$.

Exercise 5. a) Using Fourier's proof of the irrationality of e and Liouville's proof that e and e^2 are not quadratic numbers, show that e^{2i} is not root of a polynomial of degree ≤ 2 with coefficients in $\mathbb{Q}(i)$.
b) Deduce that for any integer $m\ge 1$, the number $e^{2i/m}$ is not root of a polynomial of degree ≤ 2 with coefficients in $\mathbb{Q}(i)$.
c) Show that for any integer $m\ge 1$, the numbers $\bigl(\cos(1/m)\bigr)^2$, $\bigl(\sin(1/m)\bigr)^2$, $\cos(1/m)\sin(1/m)$, $\cos(2/m)$, $\sin(2/m)$ are irrational.

Exercise 6. Show that a real number x is irrational if and only if 0 is an accumulation point of

$$\bigl\{a+bx\ ;\ (a,b)\in\mathbb{Z}^2\bigr\}\subset\mathbb{R}.$$

Examen – December 15, 2007
Solutions

Solution exercise 1.
a) If a and b are two positive rational integers, then 2^b is even and 3^a is odd, therefore $2^b \neq 3^a$, hence $\log 2/\log 3 \neq a/b$.
b) The quotient of two rational numbers is a rational number.
c) By the Theorem of Hermite and Lindemann each of the numbers $\log 2$, $\log 3$ is transcendental, hence irrational.

Solution exercise 2.
(i) No: take for instance $x = \sqrt{2}$.
(ii) Yes: the square of a rational number a/b is a rational number a^2/b^2. Hence if $\sqrt{x}$ is rational then x is rational.
(iii) No: take any irrational number x, any rational number r and set $y = r - x$.
(iv) No: take any irrational number x, any rational number r and set $y = r/x$.
(v) No: we have seen in exercise 1 that one at least of $x_1 = \log 2$, $x_2 = \log 3$ is irrational, while $e^{x_1} = 2$, $e^{x_2} = 3$ are rational.
(vi) No: take for instance $x = e$, which is irrational, while $\log e = 1$ is rational.

Solution exercise 3.
a) Let θ and θ' be the roots of the polynomial $aX^2 + bX + c$. By Hurwitz's Theorem for any $\epsilon > 0$ there exists x and y in $\mathbb{Z}$ with $y^2 \geq |a|/5\epsilon$ and

$$\left|\theta - \frac{x}{y}\right| < \frac{1}{\sqrt{5}y^2}\cdot$$

Write

$$f(x,y) = a(x - \theta y)(x - \theta' y)$$

and use the estimates

$$|x - \theta y| \leq \frac{1}{\sqrt{5}y} \quad \text{and} \quad |x - \theta' y| \leq y|\theta - \theta'| + |x - \theta y| \leq y|\theta - \theta'| + \frac{1}{\sqrt{5}y}\cdot$$

Since $|a(\theta - \theta')| = \sqrt{\Delta}$ we deduce

$$|f(x,y)| \leq |a| \cdot \frac{1}{\sqrt{5}y}\left(y|\theta - \theta'| + \frac{1}{\sqrt{5}y}\right) \leq \sqrt{\frac{\Delta}{5}} + \frac{|a|}{5y^2} \leq \sqrt{\frac{\Delta}{5}} + \epsilon.$$

b) The sequence of Fibonacci numbers $(F_n)_{n\geq 0}$ satisfies

$$F_n^2 - F_nF_{n-1} - F_{n-1}^2 = (-1)^{n-1} \quad \text{for } n \geq 1.$$

Define

$$f(X,Y) = \sqrt{\frac{\Delta}{5}}(X^2 - XY - Y^2).$$

Then f has discriminant Δ and $|f(F_n, F_{n-1})| = \sqrt{\Delta/5}$. On the other hand for any $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ the number $x^2 - xy - y^2$ is a non–zero rational integer, hence has absolute value ≥ 1. Therefore

$$\min\bigl\{|f(x, y)|\ ;\ (x, y) \in \mathbb{Z} \times \mathbb{Z},\ (x, y) \neq (0, 0)\bigr\} = \sqrt{\Delta/5}.$$

c) Let θ be a real number such that for any $\epsilon > 0$ there exists $p/q \in \mathbb{Q}$ with

$$0 < \left|\theta - \frac{p}{q}\right| \leq \frac{\epsilon}{q^2}.$$

For instance a Liouville number satisfies this property (and much more!). Then the polynomial $f(X, Y) = Y(X - \theta Y)$ satisfies

$$\min\bigl\{|f(x, y)|\ ;\ (x, y) \in \mathbb{Z} \times \mathbb{Z},\ (x, y) \neq (0, 0)\bigr\} = 0.$$

Solution exercise 4.
The implication (iii) $\Rightarrow$ (i) is trivial: take $m = 1$.

Proof of (i) $\Rightarrow$ (ii). If α is root of a polynomial of degree ≤ 2 with coefficients in $\mathbb{Q}(i)$, then there exist a and b in $\mathbb{Q}(i)$ such that $\alpha^2 = a\alpha + b$. By induction for each integer $m \geq 1$ we can write $\alpha^m = a_m\alpha + b_m$ with a_m and b_m in $\mathbb{Q}(i)$. Hence the $\mathbb{Q}(i)$–vector space spanned by 1, α, α^2, $\alpha^3 \ldots$ is also spanned by 1, α, hence has dimension ≤ 2.

Proof of (ii) $\Rightarrow$ (iii). If the $\mathbb{Q}(i)$–vector space spanned by 1, α, α^2, $\alpha^3 \ldots$ has dimension ≤ 2, then the three numbers 1, α^m, α^{2m} are linearly dependent over $\mathbb{Q}(i)$.

Solution exercise 5
a) Assume a, b and c are elements in $\mathbb{Z}[i]$ such that e^{2i} is a root of the polynomial $aX^2 + bX + c$. Write

$$ae^{2i} + b + ce^{-2i} = 0,$$

replace e^{2i} and e^{-2i} by the Taylor expansion of the exponential function, truncate at a rank N and multiply by $N!/2^{N-1}$:

$$\frac{N!}{2^{N-1}}b + \sum_{n=0}^{N} \frac{N!2^n}{n!2^{N-1}}\bigl(ai^n + c(-i)^n\bigr) = A_N + B_N + C_N \qquad (1)$$

where

$$A_N = \frac{4}{N+1}\bigl(ai^{N+1} + c(-i)^{N+1}\bigr), \quad B_N = \frac{8}{(N+1)(N+2)}\bigl(ai^{N+2} + c(-i)^{N+2}\bigr)$$

and

$$C_N = \sum_{n \geq N+3} \frac{N!2^n}{n!2^{N-1}}\bigl(ai^n + c(-i)^n\bigr).$$

Take for N a power of 2, so that the numbers $N!/n!2^{N-n-1}$ are rational integers for $0 \leq n \leq N$. Hence in equation (1), the left hand side is in $\mathbb{Z}[i]$. Assume further that N is sufficiently large. In equation (1), the right hand side has modulus ≤ 1, hence both sides vanish. Also for N sufficiently large

$$(N+1)|A_N| = (N+1)|B_N + C_N| < 1,$$

and since $(N+1)A_N$ is in $\mathbb{Z}[i]$ we deduce $A_N = 0$ and $B_N + C_N = 0$. Now

$$(N+1)(N+2)|B_N| = (N+1)(N+2)|C_N| < 1,$$

while $(N+1)(N+2)B_N$ is in $\mathbb{Z}[i]$, hence $B_N = 0$. From $A_N = B_N = 0$ we deduce $a = c = 0$, and finally also $b = 0$.
c) Fix $m \geq 1$. Define

$$\alpha = e^{i/m}, \quad a_1 = \cos(1/m), \quad b_1 = \sin(1/m), \quad c_1 = \cos(1/m)\sin(1/m),$$

$$a_2 = \cos(2/m), \quad \text{and} \quad b_2 = \sin(2/m).$$

We have

$$\alpha + \alpha^{-1} = 2a_1, \quad \alpha - \alpha^{-1} = 2ib_1,$$
$$\alpha^2 + \alpha^{-2} = 2a_2, \quad \alpha^2 - \alpha^{-2} = 2ib_2,$$

hence

$$\alpha^2 + \alpha^{-2} + 2 = 4a_1^2, \quad \alpha^2 + \alpha^{-2} - 2 = -4b_1^2, \quad \alpha^2 - \alpha^{-2} = 4ia_1b_1.$$

Since α^2 is not root of a quadratic equation with coefficients in $\mathbb{Q}(i)$, it follows that each of the numbers a_1^2, b_1^2, a_1b_1, a_2, b_2 is not in $\mathbb{Q}(i)$.

Solution exercise 6.
To say that 0 is an accumulation point of

$$\left\{a + bx \; ; \; (a,b) \in \mathbb{Z}^2\right\} \subset \mathbb{R}$$

means that for any $\epsilon > 0$, there exists $(a,b) \in \mathbb{Z}^2$ such that $0 < |a + bx| \leq \epsilon$. According to the irrationality criterion, this is equivalent to x being irrational.