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

Third course: september 17, 2007. [4]

We now show that Lemma 1.8 is optimal.

Denote again by $\Phi = 1.6180339887499\ldots$ the Golden ratio, which is the root >1 of the polynomial $X^2 - X - 1$. The discriminant of this polynomial is 5. Recall also the definition of the Fibonacci sequence $(F_n)_{n\geq 0}$:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

Lemma 1.12. *For any $q \geq 1$ and any $p \in \mathbb{Z}$,*

$$\left|\Phi - \frac{p}{q}\right| > \frac{1}{\sqrt{5}q^2 + (q/2)}\cdot$$

On the other hand

$$\lim_{n\to\infty} F_{n-1}^2 \left|\Phi - \frac{F_n}{F_{n-1}}\right| = \frac{1}{\sqrt{5}}\cdot$$

Proof. It suffices to prove the lower bound when p is the nearest integer to $q\Phi$. From $X^2 - X - 1 = (X - \Phi)(X + \Phi^{-1})$ we deduce

$$p^2 - pq - q^2 = q^2 \left(\frac{p}{q} - \Phi\right)\left(\frac{p}{q} + \Phi^{-1}\right).$$

The left hand side is a non-zero rational integer, hence has absolute value at least 1. We now bound the absolute value of the right hand side from above. Since $p < q\Phi + (1/2)$ and $\Phi + \Phi^{-1} = \sqrt{5}$ we have

$$\frac{p}{q} + \Phi^{-1} \leq \sqrt{5} + \frac{1}{2q}\cdot$$

Hence

$$1 \leq q^2 \left|\frac{p}{q} - \Phi\right| \left(\sqrt{5} + \frac{1}{2q}\right)$$

The first part of Lemma 1.12 follows.

The real vector space of sequences $(v_n)_{n\geq 0}$ satisfying $v_n = v_{n-1} + v_{n-2}$ has dimension 2, a basis is given by the two sequences $(\Phi^n)_{n\geq 0}$ and $((-\Phi^{-1})^n)_{n\geq 0}$. From this one easily deduces the formula

$$F_n = \frac{1}{\sqrt{5}}(\Phi^n - (-1)^n\Phi^{-n})$$

[4] Updated: October 12, 2007

due to A. De Moivre (1730), L. Euler (1765) and J.P.M. Binet (1843). It follows that F_n is the nearest integer to

$$\frac{1}{\sqrt{5}}\Phi^n,$$

hence the sequence $(u_n)_{n\geq 2}$ of quotients of Fibonacci numbers

$$u_n = F_n/F_{n-1}$$

satisfies $\lim_{n\to\infty} u_n = \Phi$.

By induction one easily checks

$$F_n^2 - F_nF_{n-1} - F_{n-1}^2 = (-1)^n$$

for $n \geq 1$. The left hand side is $F_{n-1}^2(u_n - \Phi)(u_n + \Phi^{-1})$, as we already saw. Hence

$$F_{n-1}^2|\Phi - u_n| = \frac{1}{\Phi^{-1} + u_n},$$

and the limit of the right hand side is $1/(\Phi + \Phi^{-1}) = 1/\sqrt{5}$. The result follows. □

Remark. *The sequence $u_n = F_n/F_{n-1}$ is also defined by*

$$u_2 = 2,\ u_n = 1 + \frac{1}{u_{n-1}}, \quad (n \geq 3).$$

Hence

$$u_n = 1 + \cfrac{1}{1 + \cfrac{1}{u_{n-2}}} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{u_{n-3}}}} = \cdots$$

Remark. *It is known (see for instance [4] p. 25) that if k is a positive integer, if an irrational real number ϑ has a continued fraction expansion $[a_0; a_1, a_2, \dots]$ with $a_n \geq k$ for infinitely many n, then*

$$\liminf_{q\to\infty} q^2 \left|\vartheta - \frac{p}{q}\right| \leq \frac{1}{\sqrt{4+k^2}}.$$

This proof of Lemma 1.12 can be extended by replacing $X^2 - X - 1$ by any irreducible polynomial with integer coefficients. Recall that the ring $\mathbb{Z}[X]$ is factorial, its irreducible elements of positive degree are the non-constant polynomials with integer coefficients which are irreducible in $\mathbb{Q}[X]$ (i.e. not a product of two non-constant polynomials in $\mathbb{Q}[X]$) and have content 1. The *content* of a polynomial in $\mathbb{Z}[X]$ is the greatest common divisor of its coefficients.

The *minimal polynomial* of an algebraic number α is the unique irreducible polynomial $P \in \mathbb{Z}[X]$ which vanishes at α and has a positive leading coefficient.

The next lemma ([4] p. 6 Lemma 2E) is a variant of Liouville's inequality that we shall study more throughly later.

Lemma 1.13. *Let α be a real algebraic number of degree $d \geq 2$ and minimal polynomial $P \in \mathbb{Z}[X]$. Define $c = |P'(\alpha)|$. Let $\epsilon > 0$. Then there exists an integer q_0 such that, for any $p/q \in \mathbb{Q}$ with $q \geq q_0$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}\cdot$$

Proof. Let q be a sufficiently large positive integer and let p be the nearest integer to α. In particular

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2}\cdot$$

Denote a_0 the leading coefficient of P and by $\alpha_1, \ldots, \alpha_d$ its the roots with $\alpha_1 = \alpha$. Hence

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

and

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d}\left(\frac{p}{q} - \alpha_i\right). \tag{1.14}$$

Also

$$P'(\alpha) = a_0 \prod_{i=2}^{d}(\alpha - \alpha_i).$$

The left hand side of (1.14) is a rational integer. It is not zero because P is irreducible of degree ≥ 2. For $i \geq 2$ we use the estimate

$$\left|\alpha_i - \frac{p}{q}\right| \leq |\alpha_i - \alpha| + \frac{1}{2q}\cdot$$

We deduce

$$1 \leq q^d a_0 \left|\alpha - \frac{p}{q}\right| \prod_{i=2}^{d}\bigl(|\alpha_i - \alpha| + \frac{1}{2q}\bigr).$$

For sufficiently large q the right hand side is bounded from above by

$$q^d \left|\alpha - \frac{p}{q}\right| (|P'(\alpha)| + \epsilon).$$

□

If α is a real root of a quadratic polynomial $P(X) = aX^2 + bX + c$, then $P'(\alpha) = 2a\alpha + b$ is a square root of the discriminant of P. So Hurwitz Lemma 1.8 is optimal for all quadratic numbers having a minimal polynomial of discriminant 5. Incidentally, this shows that 5 is the smallest positive discriminant of an irreducible quadratic polynomial in $\mathbb{Z}[X]$ (of course it is easily checked directly that if a, b, c are three rational integers with $a > 0$ and $b^2 - 4ac$ positive and not a perfect square in $\mathbb{Z}$, then $b^2 - 4ac \geq 5$).

It follows that for the numbers of the form $(a\Phi + b)/(c\Phi + d)$ with integers a, b, c, d having $ad - bc = \pm 1$, one cannot replace in Lemma 1.8 the number $\sqrt{5}$ by a larger number.

If one omits these irrational numbers in the field generated by the Golden ratio, then Hurwitz showed that one can replace $\sqrt{5}$ by $2\sqrt{2}$, and again this is optimal. This is the beginning of the so-called *Markoff* [5] *spectrum* $\sqrt{5}$, $\sqrt{8}$, $\sqrt{221}/5$, $\sqrt{1517}/13$, ... which tends to 1/3 and is obtained as follows. First consider the set of integers m for which the *Markoff equation*

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2$$

has a solution in positive integers (m_1, m_2) with $0 < m_1 \leq m_2 \leq m$. The infinite increasing sequence of these integers m starts with

$$1,\ 2,\ 5,\ 13,\ 29,\ 34,\ 89,\ 169,\ 194,\ 233,\ 433,\ 610,\ 985,\ 1325,\ 1597, \dots \quad (1.15)$$

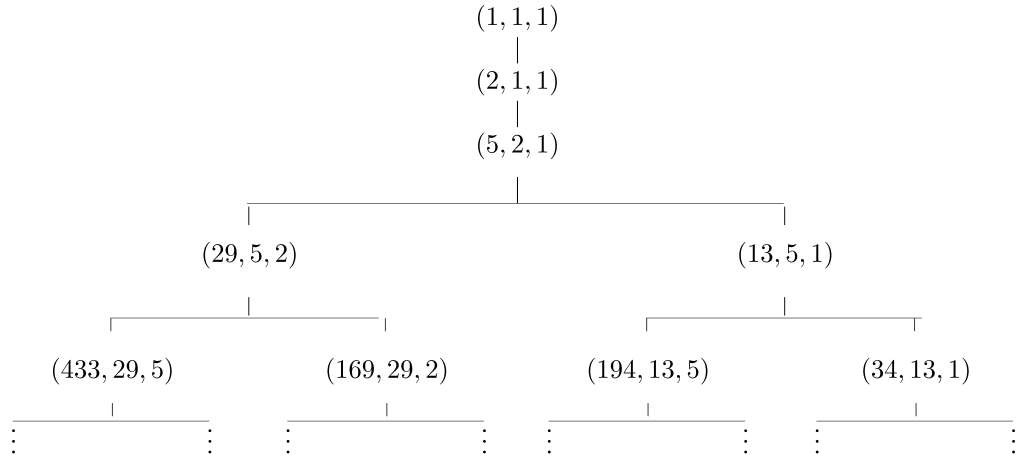
and there is an easy and well known algorithm to construct it (see for instance [8]): apart from $(1,1,1)$ and $(2,1,1)$, for any solution (m, m_1, m_2) there are three exactly solutions sharing two components with (m, m_1, m_2), namely

$$(m', m_1, m_2), \quad (m, m_1', m_2), \quad (m, m_1, m_2'),$$

where

$$m' = 3m_1m_2 - m, \quad m_1' = 3mm_2 - m_1, \quad m_2' = 3mm_1 - m_2.$$

This produces the *Markoff tree*



For each m in the Markoff sequence (1.15), we define

$$\mu_m = \frac{\sqrt{9m^2 - 4}}{m}.$$

[5] His name is spelled *Markov* in probability theory.

Then there is an explicit quadratic form $f_m(x, y)$ such that $f_m(x, 1) = 0$ and there is a root α_m of f_m for which

$$\limsup_{q\in\mathbb{Z},\; q\to\infty} (q\|q\alpha_m\|) = \frac{1}{\mu_m},$$

where $\|\cdot\|$ denotes the distance too the nearest integer:

$$\|x\| = \min_{m\in\mathbb{Z}} |x - m| = \min\bigl\{\{x\}\,;\, 1 - \{x\}\bigr\}.$$

The sequence of $(m, f_m, \alpha_m, \mu_m)$ starts as follows,

m	1	2	5	13
$f_m(x, 1)$	$x^2 + x - 1$	$x^2 + 2x - 1$	$5x^2 + 11x - 5$	$13x^2 + 29x - 13$
α_m	$[0; \overline{1}]$	$[0; \overline{2}]$	$[0; \overline{2211}]$	$[0; \overline{221111}]$
μ_m	$\sqrt{5}$	$\sqrt{8}$	$\sqrt{221}/5$	$\sqrt{1517}/13$

The third row gives the continued fraction expansion for α_m.

1.3.5 Irrationality of series studied by Liouville and Fredholm

The implication (ii)⇒(i) in lemma 1.6 was used implicitely in § 1.1. We give here another application.

Several methods are available to investigate the arithmetic nature of numbers of the form

$$\sum_{n\geq 0} a^{-n^2} \quad \text{and} \quad \sum_{n\geq 0} a^{-2^n} \tag{1.16}$$

where a is a positive integer.

There is apparently a confusion in the litterature between these two series. The name *Fredholm series* is often wrongly attributed to the power series

$$\sum_{n\geq 0} z^{2^n}.$$

However Fredholm studied rather the series

$$\sum_{n\geq 0} z^{n^2}$$

(see the book [1] by Allouche & Shallit, Notes on chapter 13, page 403 as well as Shallit's paper [7]).

The series $\sum_{n\geq 0} z^{n^2}$ was explicitly quoted by Liouville (see for instance [3]). We shall come back to this question later (where we discuss Nesterenko's result in 1995 according to which this number is transcendental). Right now we only prove the irrationality of the numbers (1.16) for $a \in \mathbb{Z}$, $a \geq 2$ by means of Lemma 1.6. More generally we replace the sequences $(n^2)_{n\geq 0}$ and $(2^n)_{n\geq 0}$ by more general ones: one requires that they grow and tend to infinity sufficiently fast.

Lemma 1.17. *Let $(u_n)_{n\geq 0}$ be an increasing sequence of positive numbers. Assume there exists $c > 0$ such that, for all sufficiently large n,*

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

Let $a \in \mathbb{Z}$, $a \geq 2$. Then the number

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

is irrational.

Proof. Let $\epsilon > 0$. Let N be a sufficiently large integer. Set

$$q_N = a^{u_N}, \quad p_N = \sum_{n=0}^{N} a^{u_N - u_n} \quad \text{and} \quad R_N = q_N\vartheta - p_N.$$

Then p_N and q_N are rational integers, while

$$R_N = \sum_{k=1}^{\infty} a^{u_N - u_{N+k}}$$

is > 0.

By induction on $k \geq 1$ one checks

$$u_{N+k} \geq u_N + ckN + v_k \quad \text{where} \quad v_k := c\frac{k(k-1)}{2}\cdot$$

Therefore

$$u_{N+k} - u_N - cN \geq (k-1)cN + v_k \geq v_k$$

and

$$0 < R_N \leq a^{-cN} \sum_{k\geq 1} a^{-v_k}.$$

Hence R_N tends to 0 as N tends to infinity and Lemma 1.6 shows that ϑ is irrational. □

1.3.6 A further irrationality criterion

Lemma 1.18. *Let ϑ be a real number. The following conditions are equivalent*
(i) *ϑ is irrational.*
(ii) *For any $\epsilon > 0$ there exists p/q and r/s in $\mathbb{Q}$ such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s}, \quad qr - ps = 1$$

and

$$\max\{q\vartheta - p\ ;\ r - s\vartheta\} < \epsilon.$$

(iii) *There exist infinitely many pairs* $(p/q, r/s)$ *of rational numbers such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s}, \quad qr - ps = 1$$

and

$$\max\{q(q\vartheta - p)\ ;\ s(r - s\vartheta)\} < 1.$$

Proof. The implications (iii)⇒(ii)⇒(i) are easy. For (i)⇒(iii) we use the arguments in the proof of Lemma 1.9, but we use also an auxiliary result from the theory of continued fractions.

Since ϑ is irrational, Hurwitz Lemma 1.8 shows that there are infinitely many p/q such that

$$\left|\vartheta - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

We shall use the fact that such a p/q is a so-called *best approximation to* ϑ: this means that for any $a/b \in \mathbb{Q}$ with $1 \le b \le q$ and $a/b \ne p/q$, we have

$$\left|\vartheta - \frac{a}{b}\right| > \left|\vartheta - \frac{p}{q}\right|.$$

Assume first $p/q < \vartheta$. Let r/s be defined by $qr - ps = 1$ and $1 \le s < q$, $|r| < |p|$. We have

$$0 < \frac{r}{s} - \vartheta < \frac{r}{s} - \frac{p}{q} = \frac{1}{qs} \le \frac{1}{s^2}.$$

Next assume $p/q > \vartheta$. In this case rename it r/s and define p/q by $qr - ps = 1$ and $1 \le q < s$, $|p| < |r|$.

Finally repeat the argument in the proof of Lemma 1.9 to get an infinite set of approximations. Lemma 1.18 follows. □

1.4 Irrationality of e^r and π, following Nesterenko

The proofs given in subsection 1.2 of the irrationality of e^r for several rational values of r (namely $r \in \{1/a, 2/a, \sqrt{2}/a, \sqrt{3}/a\ ;\ a \in \mathbb{Z},\ a \ne 0\}$) are similar: the idea is to start from the expansion of the exponential function, to truncate it and to deduce rational approximations to e^r. In terms of the exponential function this amounts to approximate e^z by a polynomial. The main idea, due to C. Hermite [4], is to approximate e^z by rational functions $A(z)/B(z)$. The word “approximate” has the following meaning (Hermite-Padé): an analytic function is well approximated by a rational function $A(z)/B(z)$ (where A and B are polynomial) if the difference $B(z)f(z) - A(z)$ has a zero at the origin of high multiplicity.

When we just truncate the series expansion of the exponential function, we approximate e^z by a polynomial in z with rational coefficients; when we substitute $z = a$ where a is a positive integer, this polynomial produces a rational number, but the denominator of this number is quite large (unless $a = \pm 1$). A trick gave the result also for $a = \pm 2$, but definitely for a a larger prime number for instance there is a problem: if we multiply by the denominator then the "remainder" is by no means small. To produce a sufficiently large gap in the power expansion of $B(z)e^z$ will solve the problem.

Our first goal in this section is to prove the irrationality of e^r when r is a non-zero rational number. Next we show how a slight modification implies the irrationality of π.

1.4.1 Irrationality of e^r for $r \in \mathbb{Q}$

If $r = a/b$ is a rational number such that e^r is also rational, then $e^{|a|}$ is also rational, and therefore the irrationality of e^r for any non-zero rational number r follows from the irrationality of e^a for any positive integer a. We shall approximate the exponential function e^z by a rational function $A(z)/B(z)$ and show that $A(a)/B(a)$ is a good rational approximation to e^a, sufficiently good in fact so that one may use Lemma 1.6.

Write

$$e^z = \sum_{k \geq 0} \frac{z^k}{k!} \cdot$$

We wish to multiply this series by a polynomial so that the Taylor expansion at the origin of the product $B(z)e^z$ has a large gap: the polynomial preceding the gap will be $A(z)$, the remainder $R(z) = B(z)e^z - A(z)$ will have a zero of high multiplicity at the origin.

In order to create such a gap, we shall use the differential equation of the exponential function - hence we introduce derivatives.

We first explain how to produce, from an analytic function whose Taylor development at the origin is

$$f(z) = \sum_{k \geq 0} a_k z^k, \tag{1.19}$$

another analytic function with one given Taylor coefficient, say the coefficient of z^m, is zero. The coefficient of z^m for f is $f^{(m)}(0) = a^m/m!$. The same number a_m occurs when one computes the Taylor coefficient of z^{m-1} for the derivative f' of f, it is also the Taylor coefficient of z^m in the development of $zf'(z)$:

$$(zf')^{(m)}(0) = \frac{a^m}{(m-1)!} \cdot$$

Hence the coefficient of z^m in the Taylor development of $zf'(z) - mf(z)$ is 0, which is what we wanted.

It is the same thing to write

$$zf'(z) = \sum_{k\geq 0} ka_k z^k$$

so that

$$zf'(z) - mf(z) = \sum_{k\geq 0}(k-m)a_k z^k.$$

Now we want that several consecutive Taylor coefficients cancel. It will be convenient to introduce derivative operators.

We start with $D = d/dz$. As usual D^2 denotes $D \circ D$ and $D^m = D^{m-1} \circ D$ for $m \geq 2$. The derivation D and the multiplication by z do not commute:

$$D(zf) = f + zD(f),$$

relation which we write $Dz = 1 + zD$. From this relation it follows that the non-commutative ring generated by z and D over $\mathbb{C}$ is also the ring of polynomials in D with coefficients in $\mathbb{C}[z]$. In this ring $\mathbb{C}[z][D]$ there is an element which will be very useful for us, namely $\delta = zd/dz$. It satisfies $\delta(z^k) = kz^k$. To any polynomial $T \in \mathbb{C}[X]$ one associate the derivative operator $T(\delta)$.

By induction on m one checks $\delta^m z^k = k^m z^k$ for all $m \geq 0$. By linearity, one deduces that if T is a polynomial with complex coefficients, then

$$T(\delta)z^k = T(k)z^k.$$

For our function f with the Taylor development (1.19) we have

$$T(\delta)f(z) = \sum_{k\geq 0} a_k T(k) z^k.$$

Hence if we want a function with a Taylor expansion having 0 as coefficient of z^k, it suffices to consider $T(\delta)f(z)$ where T is a polynomial satisfying $T(k) = 0$. For instance if n_0 and n_1 are two non-negative integers and if we take

$$T(X) = (X - n_0 - 1)(X - n_0 - 2)\cdots(X - n_0 - n_1),$$

then the series $T(\delta)f(z)$ can be written $A(z) + R(z)$ with

$$A(z) = \sum_{k=0}^{n_0} T(k)a_k z^k$$

and

$$R(z) = \sum_{k\geq n_0+n_1+1} T(k)a_k z^k.$$

This means that in the Taylor expansion at the origin of $T(\delta)f(z)$, all coefficients of $z^{n_0+1}, z^{n_0+2}, \ldots, z^{n_0+n_1}$ are 0.

References

[1] J.-P. ALLOUCHE & J. SHALLIT – *Automatic sequences, Theory, applications, generalizations*, Cambridge University Press, Cambridge, 2003,

[2] J.W.S. CASSELS– *An introduction to Diophantine approximation.* Cambridge Tracts in Mathematics and Mathematical Physics, **45**. Cambridge University Press, New York, 1957.

[3] N. I. FEL′DMAN & Y. V. NESTERENKO – *Transcendental numbers*, in *Number Theory, IV*, Encyclopaedia Math. Sci., vol. **44**, Springer, Berlin, 1998, p. 1–345.

[4] C. HERMITE – *Sur la fonction exponentielle*, C. R. Acad. Sci. Paris, **77** (1873), 18–24; 74–79; 226–233; 285–293; *Oeuvres*, Gauthier Villars (1905), III, 150–181. See also *Oeuvres* III, 127–130, 146–149, and *Correspondance Hermite-Stieltjes*, II, lettre 363, 291–295.

[5] H. LAMBERT - *Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques*, Mémoires de l'Académie des Sciences de Berlin, 17 (1761), 1768, p. 265-322; lu en 1767; Math. Werke, t. II.

[6] W. M. SCHMIDT – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980.

[7] J. SHALLIT – *Real numbers with bounded partial quotients: a survey*, L'Enseignement Mathématique, **38** (1992), 151-187).

[8] M. WALDSCHMIDT, *Open Diophantine Problems*, Moscow Mathematical Journal **4** N°1, 2004, 245–305.