20 Approximation by rationals (Diophantine approximation)

We all know that real numbers can be approximated by the rationals $\frac{p}{q}$ (with $(p,q)=1$). But how well can this be done? And does it depend on the nature of x? We will try to answer these questions now.

For any $x \in \mathbb{R}$, let $[x]$ denote its integral part.

Theorem 1 (Dirichlet) Let x be an irrational number. There $\exists$ infinitely many rationals $\frac{p}{q}$ (with $(p,q)=1$) such that

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

Remark 1: This theorem is false for the rationals. Indeed, suppose4 $x = \frac{a}{b}$ and $\frac{p}{q} \neq \frac{a}{b}$ a rational with $|q| > |b|$. Then $|x - \frac{p}{q}| = |\frac{aq-bp}{bq}| \geq \frac{1}{bq} > \frac{1}{q^2}$. Let $I = [[x]-1, [x]+1]$. If $\frac{p}{q} \notin I$, then clearly, $|x - \frac{p}{q} > 1$. We are done now, because the number of $\frac{p}{q}$ in I with $|q| \leq |b|$ is finite.

Proof of Theorem 1. This is done by first establishing the following result, also due to Dirichlet:

Proposition Let $x, t \in \mathbb{R}$ with $t > 1$. Then $\exists p, q \in \mathbb{Z}$ such that $1 \leq q < t$ and $|qx - p| \leq \frac{1}{t}$.

Proof of Proposition Let $\{x\}$ denote the fractional part of x, lying in $[0,1)$. Suppose t is an integer > 1. Then the $t+1$ numbers $0, 1, \{x\}, \{2x\}, \ldots, \{(t-1)x\}$ lie in $[0,1]$, and so the difference between some pair among these must be in absolute value bounded by t^{-1}. Then $\exists m_1, m_2, n_1, n_2 \in \mathbb{Z}$ with $0 \leq m_i \leq t-1,\ i = 1,2$, and $m_1 \neq m_2$, such that $|(m_1x - n_1) - (m_2x - n_2)| \leq \frac{1}{t}$. We may assume that $m_1 > m_2$. Then the Proposition is satisfied by taking $p = n_1 - n_2$ and $q = m_1 - m_2$. Done if $t \in \mathbb{Z}$. Suppose $t \notin \mathbb{Z}$. Then $t' = [t]+1$ is an integer > 1, and $\exists p, q$ with $1 \leq q < t'$ and $|qx - p| \leq \frac{1}{t'}$. Evidently we have: $1 \leq q < t$ and $|qx - p| < \frac{1}{t'}$. Hence the proposition.

Proposition $\Rightarrow$ Theorem 1: Since x is irrational, the bound $|qx - p| \leq \frac{1}{t}$ can hold, for a fixed (p,q), only for bounded values of t, say for $t \leq t + - = t_0(p,q)$. Hence, as $t \to \infty$, there will be infinitely many distinct coprime integers (p,q) as in Proposition, giving rise to infintely many $\frac{p}{q}$ satifying $|x - \frac{p}{q}| < \frac{1}{q^2}$.

Theorem 2 (Hurwitz) Let x be irrational. Then $\exists$ infinitely many $\frac{p}{q}$ with $(p,q)=1$ such that $|x-\frac{p}{q}|<\frac{1}{\sqrt{5}q^2}$.

Remark 2: Hurwitz's theorem is the best possible. Indeed, suppose x is a real **quadratic** irrational and suppose $\exists$ infinitely many $\frac{p}{q}\in\mathbb{Q}$ with $(p,q)=1$ such that

$$\left|x-\frac{p}{q}\right|<\frac{1}{Cq^2} \qquad (*)$$

for some $C>1$. Let $f(X)=aX^2+bX+c$ be the integral polynomial with root x. Then $f(X)=a(X-x)(X-x')$ (over $\mathbb{R}$) where x' is the conjugate root. For every $\frac{p}{q}$ satisfying $(*)$ we have

$$\frac{q}{q^2}\leq\left|f\left(\frac{p}{q}\right)\right)=\left|x-\frac{p}{q}\right|\cdot\left|a\left(x'-\frac{p}{q}\right)\right|<\frac{1}{Cq^2}\left|a\left(x'-x+x-\frac{p}{q}\right)\right|$$
$$<\frac{\sqrt{D}}{Cq^2}+\frac{|a|}{C^2q^4},$$

where $D=b^2-4ac=a^2(x-x')^2$. It follows that $C\leq\sqrt{D}$. In the special case when $x=\frac{\sqrt{5}-1}{2}$, $f(x)=x^2+x-1$, we have $D=5$, and so $C\leq\sqrt{5}$.

Definition $x\in\mathbb{R}$ is an **algebraic number** iff $\exists\ f(X)\in\mathbb{Q}(X)$ such that $f(x)=0$. It is **transcendental** if it is not algebraic.

Fact π, e are not **algebraic**.

Definition An algebraic number x has degree d if d is the minimum of the degrees of polynominals $f(x)$ such that $f(x)=0$.

Theorem 3 (Liouville) Suppose x is a real algebraic number of degree d. Then $\exists\ c=c(x)>0$ such that

$$\left|x-\frac{p}{q}\right|>\frac{c(x)}{q^d},$$

for all rational numbers $\frac{p}{q}\neq x$, with $(p,q)=1$.

Corollary: $\alpha:=\sum_{n\geq 1}\frac{1}{2^{n!}}$ is transcendental.

Indeed, let us put $p_m=2^{m!}\sum_{n=1}^{m}\frac{1}{2^{n!}}$ and $q_m=2^{m!}$. Then

$$\left|x-\frac{p_m}{q_m}\right|=\sum_{n>m}\frac{1}{2^{n!}}<\frac{2}{2^{(m+1)!}}=\frac{2}{q_m^{m+1}}$$

Hence for any d and any constant $c > 0$ we have

$$\left| x - \frac{p_m}{q_m} \right| < \frac{c}{q_m^d}$$

for all large enough m.

So x can't be algebraic of any degree d. Done.

Proof of Theorem 3 Let $f(x)$ be the (minimal) polynominal of x with deg $f = d_0$, coprime coefficients, and positive leading coefficient. Taylor's formula gives

$$\left| f\left(\frac{p}{q}\right) \right| = \left| \sum_{n=1}^{d} \left(\frac{p}{q} - x \right)^n \frac{1}{n!} f^{(n)}(x) \right| < \frac{1}{c(x)} \left| \frac{p}{q} - x \right|$$

$$\text{if } \left| \frac{p}{q} - x \right| \leq 1.$$

Let $\frac{p}{q}$ be a rational such that $\frac{p}{q} \neq x$. Then $f(\frac{p}{q}) \neq 0$ by the minimality of f. So $|f(\frac{p}{q})| \leq \frac{1}{q^d}$. So we get

$$\frac{1}{q^d} < \frac{1}{c(x)} \left| \tfrac{p}{q} - x \right|$$

if $|\frac{p}{q} - x| \leq 1$. The Theorem is of course obvious if $|\frac{p}{q} - x| > 1$.