

Fix $d > 0$ integer, not a square

Note Title

2/13/2009

If $\alpha > 0$
 $\exists n > 0$ such
 $\forall j > n$ then $\alpha_j = \frac{p_j + \sqrt{d}}{q_j}$
then $|\alpha_j - \sqrt{d}| < \frac{1}{q_j^2}$.

Assert: a_j, b_j so that

$\frac{a_j}{b_j}$ j th convergent to \sqrt{d} .

Looking for a convergent $\frac{a_j}{b_j}$ with
 $a_j^2 - db_j^2 = \pm 1$.

First observation: $\forall j \geq 2$

$$a_{j-1}^2 - d b_{j-1}^2 = (-1)^j Q_j$$

Proof:

$$\sqrt{d} = \frac{a_{j-1} d_j + a_{j-2}}{b_{j-1} d_j + b_{j-2}} = \frac{a_{j-1} \left(\frac{P_j + \sqrt{d}}{Q_j} \right) + a_{j-2}}{b_{j-1} \left(\frac{P_j + \sqrt{d}}{Q_j} \right) + b_{j-2}}$$

Multiply top + bottom by Q_j .

$$\sqrt{d} (b_{j-1} (P_j + \sqrt{d}) + Q_j b_{j-2}) = a_{j-1} (P_j + \sqrt{d}) + Q_j a_{j-2}$$

$$\sqrt{d} (b_{j-1} P_j + Q_j b_{j-2}) + d b_{j-1} = \sqrt{d} a_{j-1} + a_{j-1} P_j + Q_j a_{j-2}$$

$$\begin{array}{l}
 \text{I} \quad a_{j-1} = b_{j-1} p_j + Q_j b_{j-2} \\
 \text{II} \quad d b_{j-1} = a_{j-1} p_j + Q_j a_{j-2}
 \end{array}
 \left| \begin{array}{l}
 \text{Mult I by} \\
 a_{j-1}, \text{ II} \\
 \text{by } b_{j-1}
 \end{array} \right.$$

Subtract and get

$$\begin{aligned}
 a_{j-1}^2 - d b_{j-1}^2 &= Q_j (-a_{j-1} b_{j-2} - a_{j-2} b_{j-1}) \\
 &= (-1)^j Q_j.
 \end{aligned}$$

Consider j even and $j > n$

$$\begin{array}{l}
 a_{j-1}^2 - d b_{j-1}^2 = Q_j \quad Q_j > 0. \\
 \text{Known} \quad 1 \leq Q_j < d.
 \end{array}$$

Conclusion there exists $e > 0, e \in \mathbb{Z}$

such that

$x^2 - dy^2 = e$ has an infinite number of solutions.

If $e = 1$ we have an infinite number of solutions. If $e > 1$.

If $x^2 - dy^2 = e$ let

$$S(x, y) = \left\{ (u, v) \left(\begin{array}{l} u, v > 0 \text{ in } \mathbb{Z} \text{ such} \\ \text{that } u^2 - dv^2 = e \\ \text{and } u \equiv x \text{ mod } d \\ v \equiv y \text{ mod } d \end{array} \right) \right\}.$$

There exists (x, y) such that $S(x, y)$ is infinite.

$\exists (x_1, y_1) \neq (x_2, y_2) \in S(x, y)$.

write $(x_1 - \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) = x_3 + \sqrt{d}y_3$

$$\sigma(u + \sqrt{d}v) = u - \sqrt{d}v.$$

$$\begin{aligned} (x_3 + \sqrt{d}y_3)(x_3 - \sqrt{d}y_3) &= (x_3 + \sqrt{d}y_3)\sigma(x_3 + \sqrt{d}y_3) \\ x_3^2 - dy_3^2 &= (x_1 - \sqrt{d}y_1)(x_2 + \sqrt{d}y_2)(x_1 + \sqrt{d}y_1) \\ &\quad (x_2 - \sqrt{d}y_2) \end{aligned}$$

$$= (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = e^2$$

Need is $e \mid x_3$ and $e \mid y_3$.

$$(x_1 - \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) = x_3 + \sqrt{d}y_3$$

$$\begin{aligned} x_1 x_2 - d y_1 y_2 &= x_3 && \text{consider congruence} \\ x_1 y_2 - x_2 y_1 &= y_3 && \text{mod } e \end{aligned}$$

$$\begin{aligned} x_3 &\equiv x^2 - dy^2 \pmod{e} && \Rightarrow e \mid x_3 \text{ \& } \\ y_3 &\equiv xy - xy \pmod{e} && e \mid y_3 \end{aligned}$$

If
Thus $x = \frac{x_3}{e}$, $y = \frac{y_3}{e}$ then

$$\underline{x^2 - dy^2 = 1.}$$

Replace (x, y) $(|x|, |y|)$ still a solution.

$$(x + \sqrt{d}y)^m = x_m + \sqrt{d}y_m, \quad x_m^2 - dy_m^2 = 1.$$

Theorem. If $x, y > 0$ give a solution
if $x^2 - dy^2 = 1$ and $x + \sqrt{d}y$
is minimal, then every solution
is of this form.

Transcendental Numbers.

Louville proved existence.

A number $\alpha \in \mathbb{R}$ is called algebraic if there exists $f(x)$ a polynomial with coefficients in \mathbb{Q} such that $f(\alpha) = 0$.

$$\sqrt[n]{d} \longleftrightarrow x^n - d.$$

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m$$

$$a_i = p_i/q_i \quad q_i > 0 \quad q_i \in \mathbb{Z}$$

Multiply by $q_0 \dots q_m$

Then we have polynomial with
coeff. in \mathbb{Z} .

$$\alpha = r/s \quad s > 0$$

and $\frac{a}{b}$ rational $b > 0$
 $\alpha \neq a/b$ then $|\alpha - \frac{a}{b}| \geq \frac{1}{b}$.

Suppose α algebraic and $f(x)$ is

a polynomial of minimal degree, m ,
with integral coefficients such
that $f(\alpha) = 0$. (Note $m \geq 1$ if α is
irrational).

Theorem (Liouville) \rightarrow There exists $C > 0$
If $\frac{a}{b} \in \mathbb{Q}$, $a, b \in \mathbb{Z}$
 $b > 0$ and α alg. and irrational
with m as above (degree of α).
Then $|\alpha - \frac{a}{b}| \geq \min(\frac{C}{b^m}, 1)$.

Let α be irrational of degree $m > 1$
Then $\exists C > 0$ such that if $\frac{a}{b}$ is

rational, $b > 0$, $a, b \in \mathbb{Z}$ then

$$\left| d - \frac{a}{b} \right| \geq \min\left(\frac{c}{b^{m+1}}, 1\right)$$