Markov's Theorem on quadratic forms([1],[2])

First we look at a chain of theorems for indefinite quadratic forms, these are exspressions of the form

$$f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$$

with positive discriminant $\delta(f) = \delta = \beta^2 - 4\alpha\gamma$ and α, β, γ real or integer numbers.

Definition 0.1. Two quadratic forms $f(x,y), f'(x,y)$ are equivalent if there are integers a, b, c, d, st.

$$f'(ax+by, cx+dy) = f(x,y), \text{ where } ad - bc = \pm 1 \tag{1}$$

identically in x, y.

This forms an equivalence realtion in the usual sense. It is also easily verified that two equivalent forms have the same discriminant. We write

$$\mu(f) = \inf_{x,y \in \mathbb{N}} \mid f(x,y) \mid \ \text{ x,y not both 0.}$$

The chain of theorems is now as follows:

$$\mu(f) \leq 5^{-\frac{1}{2}} \delta^{\frac{1}{2}}(f)$$

equality is only for the forms equivalent to a multiple of $x^2 + xy - y^2$, else

$$\mu(f) \leq 2^{-\frac{3}{2}} \delta^{\frac{1}{2}}(f)$$

with equality only for the forms equivalent to a multiple of $x^2 + 2xy - y^2$, and so on. The sequence of numbers $5^{-\frac{1}{2}}, 2^{-\frac{3}{2}}, ...$ converges to $\frac{1}{3}$.

This brings us to the theorem we want to prove

Theorem 0.1. *Suppose that*

$$f(x,y) = \alpha x^2 + \beta xy + \gamma y^2, \ \delta(f) = \beta^2 - 4\alpha\gamma$$

and put

$$\mu = \inf_{x,y \in \mathbb{N}} \mid f(x,y) \mid \ \textit{ x,y not both 0.}$$

- *If*

$$\mu > \frac{1}{3}\delta^{\frac{1}{2}}, \tag{2}$$

  then f is equivalent to a Markov form (definition later).

- *Conversely (2) holds for all forms equivalent to multiple of Markov forms.*

- *There are non-enumerably many forms, none of which is equivalent to a multiple of any other, st. $\mu = \frac{1}{3}\delta^{\frac{1}{2}}$*

The poof is the goal of this notes.

Definition 0.2. Consider the diophantine equation defined by

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2. \tag{3}$$

We call the positive integer solutions (m, m_1, m_2) which may occur a Markov triple.

Lemma 0.2. *The triples $(1, 1, 1)$ and $(2, 1, 1)$ are the only Markov triples with repeated numbers.*

Proof. Suppose, without loss of generality, $m_1 = m_2$. Then $m_1^2 \mid m^2$, say $m = dm_1$. Plugging this into (3) gives $d^2 + 2 = 3dm_1$, which implies $d \mid 2$, hence $d = 1$ or $d = 2$. In either case $m_1 = m_2 = 1$ with $m = 1$ or 2. □

The triples $(1, 1, 1)$, $(2, 1, 1)$ are called singular, and all other Markov triples with three different entries non-singular. The smallest non-singular Markov triple is $(1, 5, 2)$. The following clever idea permits a recursive construction of all Markov triples. Suppose (m, m_1, m_2) is a non-singular triple. Then m is a root of the polynomial

$$\phi(x) = x^2 - 3xm_1m_2 + m_1^2 + m_2^2 = (x - m)(x - m').$$

The other root m' satisfies $m + m' = 3m_1m_2$, $mm' = m_1^2 + m_2^2$. So $m' = 3m_1m_2 - m = \frac{m_1^2+m_2^2}{m}$ implies m' is an integer and m' is positive. Therefore (m', m_1, m_2) is a different Markov triple. Similarly we get that

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

where $m_1' = 3mm_2 - m_1$, $m_2' = 3mm_1 - m_2$ are Markov triple. Now we need to check that they are distinct. Assume $m > m_1 > m_2$, then

$$m_1' > m > m_2, m_2' > m > m_1. \tag{4}$$

and

$$(m_1 - m)(m_1 - m') = \phi(m_1) = 2m_1^2 - 3m_1^2m_2 + m_2^2 < 0.$$

Hence, $max(m_1, m_2)$ lies strictly between m and m' except for the singular solutions; hence

$$m_1 > m', m_2 \tag{5}$$

We see that

$$m_2' > m_1' > m > m_1.$$

Hence this are four different triples. Thus every non-singular solution gives rise to three distinct solutions, called the neighbouring triples

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

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

Definition 0.3. The solutions are arranged as in Figure 1. The branches "going down" from a solution (a, b, c) correspond to taking the neighbours with higher maximum, and the branch "going up" corresponds to taking the neighbour with lower maximum. This constructed tree is the Markov tree.

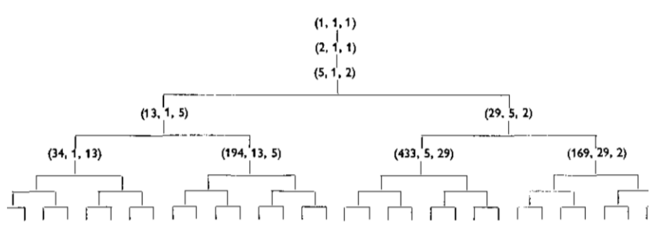

Figure 1: Markov tree

Theorem 0.3. *All Markov triples appear exactly once in the Markov tree.*

Proof. Suppose (a, m, b) is a non-singular triple with maximum m. By (4) and (5), there is exactly one neighbour with smaller maximum a or b, namely $(a, b, 3ab - m)$ if $b > a$ respectively $(3ab - m, a, b)$ if $a > b$. Going back in this way, we decrease the maximum each time and end up eventually at $(1, 5, 2)$ or $(2, 5, 1)$, since this is the only triple with maximum 5. Retracing our steps in the tree from $(1, 5, 2)$, we find that (a, m, b) or (b, m, a) is in the tree.Uniqueness is clear, since the neighbor with smaller maximum is uniquely determined, and we can argue by induction on the maximum. $\square$

Remark. A direct proof gives

$$g.c.d(m, m_1) = g.c.d(m, m_2) = g.c.d(m_2, m_1) = 1.$$

From the Markov equation

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

it follows that m divides $m_1^2 + m_2^2$, whence

$$m_1^2 = -m_2^2 (mod\ m)$$

Since m, m_1, and m_2 are coprime, the two congruences

$$m_1 x = \pm m_2 (mod\ m)$$

have unique solutions u, u' with $0 < u, u' < m$. Therefore we find integer numbers k, k_1, k_2, st.

$$\begin{aligned} k &= \frac{m_2}{m_1} = \frac{-m_1}{m_2} (mod\ m) \text{ with } 0 \leq k < m \\ k_1 &= \frac{m}{m_2} = \frac{-m_2}{m} (mod\ m_1) \text{ with } 0 \leq k_1 < m_1 \\ k_2 &= \frac{m_1}{m} = \frac{-m}{m_1} (mod\ m_2) \text{ with } 0 < k_2 \leq m_2 \end{aligned}$$

Definition 0.4. We call

$$(m, k; m_1, k_1; m_2, k_2)$$

an ordered Markov set.

Remark. It holds

$$k^2 = \frac{m_2}{m_1} \frac{-m_1}{m_2} = -1 (mod\ m) \text{ ect.}$$

and therefore $\exists l, l_1, l_2$, st.

$$k^2 + 1 = lm,\ k_1^2 + 1 = l_1 m_1,\ k_2^2 + 1 = l_2 m_2.$$

Lemma 0.4 (see [2] p.30 Lemma 7)**.** *For non-singular (m, m_1, m_2) we have*

$$\begin{aligned} mk_2 - m_2 k &= m_1 \\ mk_1 - m_1 k &= m_2 \\ m_1 k_2 - m_2 k_1 &= m' = 3m_1 m_2 - m \end{aligned}$$

Definition 0.5. The Form F_m, defined by

$$mF_m(x, y) = mx^2 + (3m - 2k)xy + (l - 3k)y^2$$

is called a Markov form.

Identically one can write

$$m^2 F_m(x, y) = \phi_m(y, z) \tag{6}$$

where $z = mx - ky$ and $\phi_m(y, z) = y^2 + 3myz + z^2$.
Trivially

$$\phi_m(y, z) = \phi_m(z, y) = \phi_m(-z, y + 3mz) \tag{7}$$
$$= \phi_m(z + 3my, -y) \tag{8}$$

The discriminant of $mF_m(x, y)$ is $9m^2 - 4$ and so

$$F_m = (x + \frac{3m - 2k}{2m} y)^2 - (\frac{9}{4} - \frac{1}{m^2})y^2. \tag{9}$$

We can see that the definition of F_m is asymetric in m_1, m_2. Suppose that $m_2 k' = m_1 (mod\ m), 0 \leq k' < m$ and $k'^2 + 1 = l'm$. Let F'_m be the corresponding form. By (6) we have $k + k' = 0 (mod\ m)$ and so either $m = 1, k = k'$ or $m > 0$ and $k + k' = m$ In the first case $F'_m = F_m$ and in the second $F'_m(x, y) = F_m(x - 2y, -y)$ by (9). Since we deal only with equvalence of forms we need not consider F_m and F'_m seperately. If we order m_1, m_2 so that $k \leq k'$, the $0 \leq 2k \leq m$.
Each Markov triple corresponds to a Markov form. If we look at the first triple $(1, 1, 1)$ we have $k = 0$ and we get the form $x^2 + 3xy + y^2$ (short $(1, 3, 1)$) which is equivalent to $x^2 + xy - y^2$ like in the introduction. Therefore to the tree of solutions of $m^2 + m_1^2 + m_2^2 = 3mm_1m_2$ corresponds a tree of Markov forms (see Figure 2)

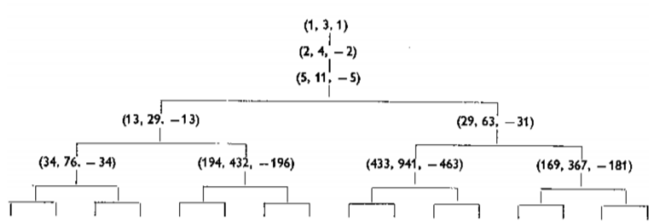

Figure 2: Markov tree of forms

Lemma 0.5. *For non-singular* (m, m_1, m_2),

$$F_m(k, m) = F_m(k - 3m, m) = 1,$$
$$F_m(k_1, m_1) F_m(k_2 - 3m_2, m_2) = -1.$$

Proof.

$$m^2 = F_m(k, m) = \phi_m(m, 0) = m^2 \text{ by (6).}$$

Similarly (6), (8) give

$$m^2F_m(k-3m,m)=\phi_m(m,-3m^2)=\phi_m(0,-m)=m^2.$$

By Lemma 0.4, $(x,y)=(k_1,m_1)$ gives $z=-m_2$, so

$$\begin{aligned} m^2F_m(k_1,m_1) &= \phi_m(m_1,-m_2) \\ &= m_1^2-3mm_1m_2+m_2^2=-m^2. \end{aligned}$$

Finally

$$\begin{aligned} m^2F_m(k_2-3m_2,m_2) &= \phi_m(m_2,m_1-3mm_2) \\ &= \phi_m(m_1,-m_2)=(-m^2). \end{aligned}$$

□

Corollary 0.5.1. *Let $f(x,y)=x^2+\beta xy+\gamma y^2$ for some β and γ and suppose that,*

$$\begin{aligned} &f(k,m)\geq 1,\ f(k-3m)\geq 1 \\ &f(k_1,m_1)\leq -1,\ f(k_2-3m_2,m_2)\leq -1 \end{aligned}$$

Then $f(x,y)=F_m(x,y)$.

Proof. Let $F_m(x,y)=x^2+\beta_m xy+\gamma_m y^2$. Use Lemma 0.5 to show $\gamma=\gamma_m$ and $\beta=\beta_m$. □

References

[1] M. Aigner, *Markov's Theorem and 100 years of the uniqueness conjecture*, Springer-Verlag, **2013**.

[2] J. Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Math., vol. 45, Cambridge Univ. Press, Cambridge, **1957**.