The Hasse-Minkowski Theorem on $\mathbb{Q}$

Linn Htut Zaw

jerrylin3.141592@gmail.com

Euler Circle

Abstract

The Hasse-Minkowski Theorem is a fundamental result on Quadratic forms defined over $\mathbb{Q}$, which states that, if there is a nontrivial solution in $\mathbb{Q}_p$ and $\mathbb{R}$, there is exists a nontrivial solution in $\mathbb{Q}$. However, this doesn't always hold for higher degrees of homogeneous polynomials, as was first shown by Selmer in 1951. In addition, his cubic form is an explicit example of an element of the Tate-Shafarevich Group for $x^3 + y^3 + 60z^3$. This paper provides an expository proof for the Hasse-Minkowski Theorem, including a proof for the existence of local solutions for Selmer's cubic form.

Notation

1. $\mathbb{Q}$ - Rational numbers.
2. $\mathbb{Q}_v$ - The Cauchy-Sequence completion of the rationals with respect to either the euclidean norm ($\mathbb{R}$) or to the p-adic norm ($\mathbb{Q}_p$).
3. $\mathbb{Q}_v^* - \mathbb{Q}_v/\{0\}$.
4. p refers to a prime number.
5. Local Fields are the completion of a Global Field with respect to a valuation–$\mathbb{Q}_v$ are Local-Fields and $\mathbb{Q}$ is a Global Field.

Local and Global Fields over $\mathbb{Q}$

Definition 1 (Valuation)**.** *A valuation on a $\mathbb{Q}$, is a function such that, for $a, b \in \mathbb{Q}$ [4]*

1. $|a| \geq 0$
2. $|a| \cdot |b| = |ab|$
3. $|a + b| \leq |a| + |b|$

Theorem 1 (Ostrowski)**.** *[1916]*

The only non-discrete valuations on $\mathbb{Q}$ are,

1. The p-adic valuation $|x|_p = p^{-v_p(x)}$. Where p is a prime number
2. The standard absolute value $|x|_\infty = -x$ if $(x < 0)$ and $|x|_\infty = x$ if $(x \geq 0)$

The full proof is simple but tedious, So we'll give a sketch. More can be read at [4]

Proof Sketch. Suppose we have an arbitrary absolute value on $\mathbb{Q}$, we want to show that it is equivalent to $|\cdot|_\infty$ or $|\cdot|_p$.

Let 1) $n \in \mathbb{Z}_{\geq 1}$ and, $|n| \leq 1$ or 2) $|n| > 1$

For 1), we can write $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots$. Then one has some prime p_i such that $|p_i| < 1$. One shows that $|p_k| = 1$ for $k \neq i$. Which leaves us with

$$|n| = |n|_p^a$$

Where a $= -\dfrac{log|p|}{log|p|}$.

For 2), we can take any $|m| > 1, m \in \mathbb{Z}$ and take it's base-n expansion (for $0 \leq a_i < n$)

$$m = a_0 + a_1 n + a_2 n^2 + \ldots + a_k n^k$$

We then have

$$|m| \leq |n|^{\dfrac{log(m)}{log(n)}}$$

Which implies $|n| > 1$. Raising to $\dfrac{1}{log(m)}$, we get

$$|m|^{\dfrac{1}{logm}} \leq |n|^{\dfrac{1}{logn}} \tag{1}$$

Since m, n are arbitrary, this is an equality, so one gets

$|n| = |n|_\infty^a$. [4] □

Remark. *$\mathbb{Q}_p$ and $\mathbb{R}$ are Local-Fields. However, they are the only Local-Fields which exists up to isomorphism, of characteristic 0.* [6]

Quadratic Forms

Quadratic forms are Homogeneous polynomials of degree 2. They must always fufill $Q(\lambda x_1, \lambda x_2 \ldots, \lambda x_n) = \lambda^2 Q(x_1, x_2, \ldots, x_n)$ Additionally, this implies that if we have one representation of zero (When $Q(x_1, x_2, \ldots, x_n) = 0$), we have infinitely many values of Q where it represents 0.

A few examples of Quadratic forms are;

$$x^2 + 2xy + y^2, z^2 + w^2 + 3y^2, q^2 + qy, a^2 + b^2 - c^2$$

By the Principle Axis Theorem [1], we can show that all three of these equations have a "diagonal" form, that is, to be represented as a sum of the squares of it's variables–a fact not necessarily true for cubic forms unfortunately. Nevertheless, this will allow us to consider only diagonal forms when proving the Hasse-Minkowski Theorem on quadratic forms.

Theorem 2 (Principle Axis Theorem)**.** *[1]*

Let $Q(x_1, x_2, \ldots, x_n)$ be a quadratic form on $\mathbb{Q}_v^n$. Then we can write

$$Q(x_1, x_2, \ldots, x_n) = \sum_{i \leq j} a_{ij} x_i x_j = b_1 x_1 + \ldots + b_n x_n$$

Every quadratic form can be diagonalised. We can define a symmetric Matrix, $\mathbf{A}$ for $Q(x_1, x_2, \ldots, x_n)$,

$$\mathbf{A} = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \cdots & \frac{a_{1n}}{2} \\ \frac{a_{12}}{2} & a_{22} & \cdots & \frac{a_{2n}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{1n}}{2} & \frac{a_{2n}}{2} & \cdots & a_{nn} \end{pmatrix}$$

Which gives us

$$Q(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)\mathbf{A} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

This defines a bijective correspondence between the set of symmetric $n \times n$ matrices in $\mathbb{Q}^n$ and *quadratic forms* in $\mathbb{Q}^n$. Now we only have to show that $\mathbf{A}$ can be diagonalised. One has,

$$\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^\top$$

Where

$$\mathbf{D} = \begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_k \end{pmatrix}$$

The important thing to note is that $\mathbf{D}$ has the coefficients of our quadratic form in it's diagonals entries. [1]

$$Q(x_1, x_2, \ldots, x_n) = b_1 x_1^2 + \cdots + b_k x_k^2$$

Lets try this on an example from earlier, let $(q, y) \in \mathbb{Q}^2$,

$$Q(q, y) = q^2 + qy$$

We find that

$$Q(Q, Y) = \frac{1 + \sqrt{2}}{2} Q^2 + \frac{1 - \sqrt{2}}{2} Y^2$$

[1] k = n iff Q is nondegenerate ([5])

Hasse Minkowski Theorem

[5]

Before we begin the Hasse Minkowski theorem, note that, a nontrivial solution in $\mathbb{Q}$ implies a solution in $\mathbb{Q}_v$.

Proof. $\mathbb{Q} \subset \mathbb{R}$ and $\mathbb{Q} \subset \mathbb{Q}_p$ so any $(x_1, x_2, \ldots, x_n) \in \mathbb{Q}$ is in $\mathbb{Q}_p$ and $\mathbb{R}$. □

Theorem 3 (Hasse-Minkowski Theorem)**.** *Let Q be a quadratic form that represents 0 in $\mathbb{Q}_v$. Then Q represents 0 in $\mathbb{Q}$.*

We'll tackle the problem with case checking for n = 1,2,3 and $n \geq 4$.

Case 1. *$n = 1$.*

Proof. $Q(x_1) = a_1 x_1^2 \to x_1 = 0$
There are no nontrivial zeroes in 1 variable. □

Case 2. *$n = 2$.*

Proof. We have $Q(x_1, x_2) = ax_1^2 + bx_2^2$.

$$Q(x_1, x_2) = 0 \to \frac{x_1^2}{x_2^2} = -\frac{b}{a}.$$

Then, non-trivial solutions only exist if and only if $\sqrt{-\frac{a_2}{a_1}} \in \mathbb{Q}$. One should note that, a, b has to have signs of different parity to satisfy a solution in $\mathbb{R}$. □

Lemma 1. *The Square Theorem*

Let $x \neq 0, x \in \mathbb{Q}$. Then x is a square in $\mathbb{Q}$ if and only if it is a square in $\mathbb{Q}_p$ and $\mathbb{R}$.

Proof. We only have to show that x is a square in $\mathbb{Q}_p$ and $\mathbb{R}$.
Let $x = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots p_i^{k_i}$. Then, $k_1, k_2, \ldots, k_i$ is even for all i. This means it's a square in $\mathbb{Q}_p$ and $\mathbb{R}$. □

Case 3. $n = 3$ *(Legendre)*

Proof. We have $Q(x_1, x_2, x_3) = x_1^2 - ax_2^2 - bx_3^2$. Suppose that a, b are squarefree and WLOG assume that $|a| \geq |b|$. We can use induction on $m = |a| + |b|, m \in \mathbb{Z}$.
If $m = 2$ (base case), one has

$$Q(x_1, x_2, x_3) = x_1^2 \pm x_2^2 \pm x_3^2.$$

The solutions to which are $(1, 1, 0)$ or $(1, 0, 1)$. We won't consider $x_1^2 + x_2^2 + x_3^2$, though. Since it has no solutions in $\mathbb{R}$.
Let $m > 2 \to |a| > 2$ and, for distinct primes p let

$$b = \pm p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$$

If $b \equiv 0 \pmod{p_i}$, then, b is a square modulo p_i. Let's assume Q_{p_i} represents 0, so one has

$$(x_1')^2 - a(x_2)^2 - b(x_3)^2 = 0$$

The triplet (x_1', x_2', x_3') is primitive. One has

$$(x_1')^2 - b(x_3')^2 = 0$$

We can't have $x_3' \equiv 0 \bmod (p_i)$, because that implies that $(x_2') \equiv 0 \bmod (p_i)$, meaning that the triplet isn't primitive anymore. Hence, b must be a square mod p. Then there must exist integers c, d such that $d^2 = b + ac$. (a,b are squarefree). If we choose $|d| \leq |a|/2$, one has $ac = d^2 - b$, where both (b, d^2) are squares. Because $|a| = |c||a|$, Q represents 0 if and only if the form $Q'(x_1, x_2, x_3) = x_1^2 - b^2 x_2^2 - c^2 x_3^2$.
Then we rewrite $c = c'u^2$ for some squarefree c'. Since $c' < b$, Having,

$$Q''(x_1, x_2, x_3) = x_1^2 - bx_2^2 - c'x_3^2$$

Is equivalent to $Q'(x_1, x_2, x_3)$, which is equivalent to $Q(x_1, x_2, x_3)$ in representing 0. □

Definition 2 (Hilbert Symbol)**.** *The Hilbert symbol on $\mathbb{Q}_v$ is defined as, for* $a, b \in \mathbb{Q}_v^*$

$$(a,b)_v = \begin{cases} 1 \text{ if } x^2 - ay^2 - bz^2 = 0 \text{ has a nontrivial solution in } \mathbb{Q}_v \\ -1 \text{ otherwise} \end{cases}$$

The Hilbert symbol satisfies the following[2];

1. $(a,b)_v = (b,a)_v$
2. $if a \neq 1, (a, 1-a)_v = 1$
3. $(a,b)_v = 1$ for any b if and only if a is a square in $\mathbb{Q}_v$

Case 4. $n = 4$

Proof. Lets write $Q(x_1, x_2, x_3, x_4) = (ax_1^2 + bx_2^2) - (cx_3^2 + dx_4^2)$ If Q represents 0, there must be values of $y_v \in \mathbb{Q}_v^*$, such that

$$y_v = ax_1^2 + bx_2^2 = cx_3^2 + dx_4^2$$

This is only true if $(y_v, -ab)_v = (a,b)_v$ and $(y_v, cd)_v = (c,d)_v$. The product formula for the Hilbert symbols allow us to get $\prod_v (a,b)_v = \prod_v (c,d)_v = 1$.

We finally have $yz^2 - ax_1^2 + bx_2^2$ and $yz^2 - cx_3^2 - dx_4^2$, which have been shown to represent 0 in the case n = 3. Both of these forms represent the same element, so the case n = 4 is proven.

□

Case 5. $n \geq 5$ *[5] [2]*

Proof. Rewrite our form $Q = Q_1 - Q_2$, with $Q_1 = a_1x_1^2 + a_2x_2^2$, $Q_2 = -(a_3x_3^2 + \ldots a_nx_n^2)$.

Let $S \subset v$, such that S contains ∞, 2, and the numbers p such that $v_p(a_i) \neq 0$ for one $i \geq 3$. This set is finite. Then for $s \in S$, f_s represents 0, there exists $y_s \in \mathbb{Q}_s$ such that

$$y_s = Q_1(x_1, x_2) = Q_2(x_3, \ldots, x_n)$$

Now, the squares of our $\mathbb{Q}_s$ forms an open set. The weak approximation theorem[6] can be applied such that if we have $y' = (x_1', x_2')$, then $\dfrac{y}{y_s} \in \mathbb{Q}_s^2$, for all $s \in S$. Also, y_s is represented by Q_2. Then $yz^2 - Q_2$ represents 0. This form is one rank lower than Q so it represents 0 in $\mathbb{Q}^*$. Both Q_2 and Q_1 represents y in $\mathbb{Q}$, Hence, Q represents 0, which proves the case $n \geq 5$. □

General Homogeneous forms

The minimum amount of variables for a cubic to always obey the Local-Global Principle is 10, proven by Heath-Brown. However, there isn't a definite formula for the minimum values in which a Homogeneous polynomial obeys a Local-Global principle. Anyhow, the earliest example of a cubic that didn't obey the Hasse-Minkowski principle was discovered in 1951 by Ernst Selmer.

This cubic is known as Selmer's counterexample, in the form.

$$S(x,y,z) = 3x^3 + 4y^3 + 5z^3.$$

It was originally proven to not have any representations of 0 in $\mathbb{Q}^*$ but to have representations in $\mathbb{Q}_v^*$ by Selmer in 1951. The proof for having points at $\mathbb{Q}_v^*$ will be covered, but the proof for having no points at $\mathbb{Q}^*$ won't–the techniques required to show that is out of the scope of this paper. However, the proof in it's entirety can be found at [[3]].

Proof. A solution in $\mathbb{R}^3$ is straightforward–$(1, 1, \sqrt[3]{\frac{-7}{5}})$ works.

Let's consider $p = 3, 5$ and the other primes separately.

On $\mathbb{Q}_3$, Suppose $z = -1, x = 3$.

One has, $4y^3 - 5 = 0$. We'd like to use Hensel's Lemma to lift y to higher powers of 3, and to do that, we simply need to show that

[2]A more thorough treatment can be found at [5]

$|f(y)| = 0$ and $|f'(y) > 0|$. y = 2 works and $f'(2) = 43 = 1 \pmod 3$.

Next, we'll let $x = 1$ and $z = 0$ to get $4y^2 + 3 = 0$. Surprisingly, we can take $y = 2$ again!

One obtains $4(2)^3 + 3 = 35$.

$|f(2)| = 0$ and $|f'(y) > 0|$. y = 2 works and $f'(2) = 51 = 1 \pmod 3$.

If $3 \equiv t^3 (\text{mod } p)$, we can solve with $(x, 1, -1)$, where $x^3 = \frac{1}{3}$. If $p \equiv 1 \pmod 3$, everything in $\mathbb{Z}/p\mathbb{Z}^*$ can be written as $t^3, 3t^3$ or $9t^3$. If $5 \equiv t^3 (\text{mod } p)$, $(-x, x, -1)$ with $x^3 = 5$ works. If $5 \equiv 3t^3 \pmod{\text{p}}$, then, $(x, 0, -1)$ with $x^3 = \frac{5}{3}$ works. If $5 \equiv 9t^3 \pmod p$, $(3x, 5, -7)$ with $x^3 = 15$ works. These are the nontrivial representations of Selmer's cubic at all $\mathbb{Q}_v$.

□

Remark. *Selmer's cubic is an element of the Tate-Shafarevich Group of the elliptic curve $x^3 + y^3 + 60z^3 = 0$[3]. It is a major open problem to determine whether all Tate-Shafarevich Groups are finitely generated, but in this case, the Group is in the form $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. There are 8 other curves on said elliptic curve similar to Selmer's cubic.*

References

[1] Sheldon Axler. "Linear Algebra Done Right". In: *Springer Undergraduate Texts in Mathematics* pp. 343 ().

[2] T.M Brednek. "The Hasse-Minkowski Theorem". In: *University of Groningen* pp. 30-32 ().

[3] Keith Conrad. "Selmer's Example". In: *University of Michigan* pp. 1-7 ().

[4] Bjorne Poonen. "Introduction to Arithmetic Geometry". In: *MIT* pp. 7 ().

[5] Jean Pierre Serre. "A Course in Arithmetic". In: *Springer Graduate Texts in Mathematics* pp.1-50 ().

[6] Chris Williams. "MA4M3 Local Fields". In: *Warwick Mathematical Institute* pp. 46 ().