1 Hasse Minkowski Theorem

Theorem 1.1. Let $X$ be a smooth projective $n$-dimensional variety defined in $\mathbb{P}^{n+1}$ by a single homogeneous quadratic polynomial in $n+2$ variables. Then if $X$ has a point in every completion of $\mathbb{Q}$ then it has a point in $\mathbb{Q}$.

The first step is to say that we can bring any homogenous quadratic polynomial to the diagonal form

$$\sum_i a_i x_i^2$$

Now the case $n = 0$ is trivial (a positive rational number which is a square in every $\mathbb{Q}_p$ is a square in $\mathbb{Q}$). The next step of the proof is the reduce all cases to the case of $n = 1$. I didn’t write it in the notes but you can find it online. Hence we shall prove the case of $n = 1$. By using Hensel lemma and the fact that the quadratic equation has a real solution we can reduce to the following claim:

Theorem 1.2. Let $a, b, c$ be pairwise coprime positive integers. Consider the quadratic form

$$q(x, y, z) = ax^2 - by^2 - cz^2$$

Then the equation $q(x, y, z) = 0$ has a non-trivial solution in $\mathbb{Z}$ if and only if it has a non-trivial solution mod $N$ for every $N$.

Proof. Let $p \neq 2$ be a prime dividing $abc$. Then mod $p$ the form $q$ becomes a quadratic form in two variables. Since it has a non-trivial zero mod $p$ it has to split mod $p$ to a product of two linear forms:

$$ax^2 - by^2 - cz^2 = L_p(x, y, z)M_p(x, y, z) \mod p$$

Hence $L_p(x, y, z) = 0 \mod p$ implies that $(x, y, z)$ is a zero of $q$ mod $p$.

At the prime 2 we separate between two cases. If 2 $\not| abc$ then either $a = b$ (mod 4) or $a = c$ (mod 4), other wise a quick check will verify that there isn’t any solution mod 4 in which at least one of $x, y, z$ is odd. Assume WLOG that $a = b$ then we take the two linear forms

$$L_2^1(x, y, z) = z$$

0
\[ L_2^2(x, y, z) = x - y \]
and note that if \( L_2^1(x, y, z) = L_2^2(x, y, z) = 0 \pmod{2} \) then \( q(x, y, z) = 0 \pmod{4} \).

If \( 2 | abc \) then assume that \( 2 | a \) and \( b, c \) are odd. Let \( d = \frac{b + c}{2} \) and define
\[
L_1^1(x, y, z) = y - z
\]
\[
L_2^2(x, y, z) = x - dy
\]
Then a quick check verifies that if \( L_1^1(x, y, z) = 0 \pmod{4} \) and \( L_2^2(x, y, z) = 0 \pmod{2} \) then actually \( q(x, y, z) = 0 \pmod{8} \).

Hence to conclude we find that if \( (x, y, z) \) is such that
\[
L_p(x, y, z) = 0 \pmod{p}
\]
for all \( p | abc \) and
\[
L_1^1(x, y, z) = 0 \pmod{2 (or 4)}
\]
\[
L_2^2(x, y, z) = 0 \pmod{2}
\]
then \( q(x, y, z) = 0 \pmod{4abc} \).

We now claim that we can find a non-trivial zero of \( q \) in the box \( B \subseteq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \) defined by the boundaries
\[
|x| < 2\sqrt{bc}
\]
\[
|y| < \sqrt{2ac}
\]
\[
|z| < \sqrt{2ab}
\]
Note that unless \( a = b = c = 1 \) (in which clearly there is an integer solution) we get that this box contains strictly more than \( 4abc \) vectors \( (x, y, z) \) with \( x, y, z \geq 0 \). By the bird cage principle there exist two distinct such vectors \( (x_1, y_1, z_1), (x_2, y_2, z_2) \) such that
\[
L_p(x_1, y_1, z_1) = L_p(x_2, y_2, z_2) \pmod{p}
\]
for all \( p | abc \) and
\[
L_1^1(x_1, y_1, z_1) = L_1^1(x_2, y_2, z_2) \pmod{2 (or 4)}
\]
\[
L_2^2(x_1, y_1, z_1) = L_2^2(x_2, y_2, z_2) \pmod{2}
\]
Define \( (x_0, y_0, z_0) = (x_1, y_1, z_1) - (x_2, y_2, z_2) \). Then \( 0 \neq (x_0, y_0, z_0) \in B \) and
\[
L_p(x_0, y_0, z_0) = 0 \pmod{p}
\]
for all \( p | abc \),
\[
L_1^1(x_0, y_0, z_0) = L_1^1(x_1, y_1, z_1) = 0 \pmod{2}
\]
Hence we get that \( q(x, y, z) = 0 \pmod{2abc} \). But \( (x, y, z) \in B \) and so
\[
4abc < ax^2 - by^2 - cz^2 < 4abc
\]
so \( ax^2 - by^2 - cz^2 = 0 \) and we are done.
2 Counterexamples to the Hasse Principle

2.1 The Brauer-Manin Obstruction

The Brauer-Manin obstruction is a general tool to "bound" the set of rational points on a given variety. The idea is as follows:

Let $X$ be a (projective) variety defined over $\mathbb{Q}$. Consider the product $X(A) = X(\mathbb{R}) \times \prod_p X(\mathbb{Q}_p)$.

We can regard the rational points $X(\mathbb{Q})$ as a subset of $X(A)$ because every rational point $q \in X(\mathbb{Q})$ can be considered as a point in $X(\mathbb{Q}_p)$ for every $p$ and $X(\mathbb{R})$ as well via the natural inclusions $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ and $\mathbb{Q} \hookrightarrow \mathbb{R}$.

Now let $A$ be an Azumaya algebra on $X$. For every $p = (p_\mathbb{R}, p_{\mathbb{Q}_2}, p_{\mathbb{Q}_3}, \ldots) \in X(A)$ we can evaluate $A$ at $p_{\mathbb{Q}_p}$ and get a central simple algebra over $\mathbb{Q}_p$. This algebra is characterized by an element in $\text{inv}(A, p_{\mathbb{Q}_p}) \in \mathbb{Q}/\mathbb{Z}$. Similarly we can evaluate the algebra at $p_\mathbb{R}$ and get a central simple algebra over $\mathbb{R}$. This central simple algebra is either trivial or isomorphic to the quaternion algebra so we can encode it as an element in the subgroup $\text{inv}(A, p_{\mathbb{R}}) \subseteq \{0, 1/2\} \subseteq \mathbb{Q}/\mathbb{Z}$.

Summing up all these elements we get a new element $\text{inv}(A, p) \in \mathbb{Q}/\mathbb{Z}$. If $p$ was actually in $X(\mathbb{Q})$ then the Hasse-Neother theorem tells us that $\text{inv}(A, p) = 0$.

Hence every Azumaya algebra gives us an "equation" on $X(A)$ which is satisfied by the subset of rational points. In particular $X(\mathbb{Q})$ is contained in the set $X^{Br}$ which is defined as set of all the points $p \in X(A)$ which satisfy $\text{inv}(A, p) = 0$ for all Azumaya algebras $A$. Hence the subset $X^{Br}$ can be considered as a sort of bound on $X(\mathbb{Q})$. In particular if $X^{Br}$ is empty then so is $X(\mathbb{Q})$.

Examples:

1. Consider the affine curve $y^2 = h(x) = -(x^2 + 1)(x^3 + x^2 + 2x + 1)(x^3 + 2x^2 + x + 1)$

We first claim that $C$ has a point in every completion of $\mathbb{Q}$. For that note $h(-1)h(0)h(1) = 100$ is a square which is coprime to every $p \neq 2, 5$. Hence at $\mathbb{R}$ and every $\mathbb{Q}_p$ for $p \neq 2, 5$ at least one of $h(-1), h(0)$ and $h(1)$ are squares. For $p = 2$ we note that $h(2) = 1 \mod 8$ and so is a square in $\mathbb{Q}_2$ and $h(0) = -1$ is a square in $\mathbb{Q}_5$.

We now want to show that $C$ doesn’t have rational points. Let

$$f(x) = x^2 + 1$$
$$g(x) = -(x^3 + x^2 + 2x + 1)(x^3 + 2x^2 + x + 1)$$

We can then define an Azumaya algebra on $C$ by setting it to be the quaternion algebra $(2, f(x))$ when $f(x) \neq 0$ and $(2, g(x))$ when $g(x) \neq 0$. This Azumaya algebra is trivial at every real point because $2 > 0$. Now consider a point $(x, y) \in C(\mathbb{Q}_p)$.
We claim that $f(x)$ must have an even valuation: if $\nu_p(f(x)) < 0$ then 
$\nu_p(f(x)) = 2\nu_p(x)$. If $\nu_p(f(x)) \geq 0$ and $\nu_p(f(x))$ is odd then $\nu_p(g(x))$ is 
odd and so $f(x) = g(x) = 0 \mod p$. But the resultant of $f$ and $g$ is 1 and 
so $f, g$ can’t have a common root mod any $p$, so we get a contradiction. 
Hence $\nu_p(x)$ is even.

This means that unless $p = 2$ the Azumaya algebra $A$ is trivial at $(x, y)$.
Now if $(x, y) \in C(Q_2)$ then by checking all the possibilities one sees that 
$f(x) = 5u^2 \in Q_2$. But the equation $-2t^2 + 5s^2 = 1$ doesn’t have a solution 
in $Q_2$ because $1 - 5s^2$ can’t have an odd valuation. Hence we get that for 
every Adelic point $q \in X(A)$ we have $inv(A, q) = 1/2 \neq 0$ and so $X^{Br} = \emptyset$
which means that $X(Q) = \emptyset$.

2. Consider the affine surface $X$ given by the equation 
$$y^2 + z^2 = h(x) = (x^2 - 2)(3 - x^2)$$
and set 
$$f(x) = x^2 - 2$$ 
$$g(x) = 3 - x^2$$

We first show that this surface has a point in every completion of $Q$. We 
have the real point $(\sqrt{2}, 0, 0) \in X(R)$ and for every $p \neq 2$ then number 
h(1) = -2 is a sum of two squares. In $p = 2$ we have that $h(4) = 2 \mod 8$ is 
a sum of two squares mod 8 and hence in $Q_2$.

We shall now show that there isn’t any rational point using the Brauer-
Manin obstruction. Consider the quaternion Azumaya algebra $A$ given 
by $(-1, f(x))$ when $f(x) \neq 0$ and $(-1, g(x))$ when $f(x) \neq 0$. This is well 
defined because when $f(x) \neq 0$ and $g(x) \neq 0$ we have that 
$$r = \frac{f(x)}{g(x)} = \frac{y^2}{g^2(x)} + \frac{z^2}{g^2(x)}$$
is a sum of two squares and so $(-1, r)$ is trivial and 
$$(-1, f(x)) \cong (-1, f(x)r) = (-1, g(x))$$

Now let $(x, y, z) \in X(R)$. Then a quick check verifies that $x^2 - 2$ and $3 - x^2$
can’t both be negative and so must both be positive. Hence $A$ is trivial 
at $(x, y, z)$. Now let $(x, y, z) \in X(Q_p)$ for $p \neq 2$. Then as before since 
the resultant of $f, g$ is 1 we see that $f(x)$ must have an even valuation 
and so is a sum of two squares. If $(x, y, z) \in X(Q_2)$ then a quick check 
verifies that if $\nu_2(x) \geq 2$ so $f(x) = 6 \mod 8$ is not a sum of two squares 
mod 8 and so not a sum of two squares in $Q_2$. Hence $A$ is non-trivial at 
$(x, y, z)$. This means that for every $q \in X(A)$ we have $inv(A, q) = 1/2$ and 
so $X^{Br} = \emptyset$ and $X(Q) = \emptyset$. 

4
How did we find these Azumaya algebras? In principle this is obtained by the relevant theory in arithmetic algebraic geometry which studies Brauer groups of varieties. We can however explain a simple construction which can be used in both the examples above.

Let $X$ be a variety defined over $\mathbb{Q}$ and let $f$ be a rational function on $X$ which is defined over $\mathbb{Q}$. Suppose that there is a quadratic extension $K = \mathbb{Q}(\sqrt{a})$ of $\mathbb{Q}$ and a divisor $D$ on $X$ defined over $K$ such that

$$D + \sigma(D) = \text{div}(f)$$

where $\sigma \in \text{Gal}(K/\mathbb{Q})$ is the non-trivial element. We claim that we can construct from this an Azumaya algebra. Cover $X$ by open sets $U_\alpha$ (defined over $\mathbb{Q}$) such that on every $U_\alpha$ there exists a rational function $f_\alpha$ defined over $K$ satisfying

$$\text{div}(f_\alpha)|_{U_\alpha} = D|_{U_\alpha}$$

$$\text{div} (f_\alpha \sigma(f_\alpha)) |_{U_\alpha} = (D + D_\alpha)|_{U_\alpha} = \text{div}(f)|_{U_\alpha}$$

which means that

$$g_\alpha = \frac{f}{f_\alpha \sigma(f_\alpha)}$$

is a no-where vanishing regular function on $U_\alpha$. Define the quaternion Azumaya algebra by setting it to be $(a, g_\alpha)$ on $U_\alpha$. Note that on the intersection $U_\alpha \cap U_\beta$ the difference

$$\frac{g_\alpha}{g_\beta} = \frac{f_\beta \sigma(b_\beta)}{f_\alpha \sigma(f_\alpha)} = N_{K/\mathbb{Q}} \left( \frac{f_\beta}{f_\alpha} \right)$$

which means that $(a, g_\alpha) \cong (a, g_\beta)$. The relevant $f$ was called $f$ in both the examples above.