Using Geometry to do Number Theory

Mckenzie West
Kalamazoo College
April 12, 2018
Introduction
Suppose $f$ is a polynomial in $n$ variables with integer coefficients. How do we show there are no rational solutions to $f = 0$?
Suppose $f$ is a polynomial in $n$ variables with integer coefficients.

- What are the solutions to $f = 0$?
Suppose $f$ is a polynomial in $n$ variables with integer coefficients.

- What are the solutions to $f = 0$?
- What are the rational solutions to $f = 0$?
Suppose $f$ is a polynomial in $n$ variables with integer coefficients.

- What are the solutions to $f = 0$?
- What are the rational solutions to $f = 0$?
- Are there rational solutions to $f = 0$?
Main Question

Question

Suppose $f$ is a polynomial in $n$ variables with integer coefficients.

- What are the solutions to $f = 0$?
- What are the rational solutions to $f = 0$?
- Are there rational solutions to $f = 0$?
- How do we show there are no rational solutions to $f = 0$?
First Attempts

1. \( y = x + 1 \)
2. \( y = x + \sqrt{2} \)
3. \( x^2 + y^2 = z^2 \)
4. \( x^n + y^n = z^n \quad n \geq 3 \)
5. \( 2x^2 = y^2 \)
First Attempts

Examples

1. \( y = x + 1 \)
First Attempts

Examples

1. \( y = x + 1 \)
2. \( y = x + \sqrt{2} \)
First Attempts

Examples

1. \( y = x + 1 \)
2. \( y = x + \sqrt{2} \)
3. \( x^2 + y^2 = z^2 \)
First Attempts

Examples

1. \( y = x + 1 \)
2. \( y = x + \sqrt{2} \)
3. \( x^2 + y^2 = z^2 \)
4. \( x^n + y^n = z^n \quad n \geq 3 \)
First Attempts

Examples

1. $y = x + 1$
2. $y = x + \sqrt{2}$
3. $x^2 + y^2 = z^2$
4. $x^n + y^n = z^n \quad n \geq 3$
5. $2x^2 = y^2$
Modular arithmetic

Definition

Let \( q, n \in \mathbb{Z} \) we say \( q \equiv r \pmod{n} \) if there is an \( a \in \mathbb{Z} \) such that \( q = an + r \).

Idea: Fix \( n \), then classify all integers by their remainder when dividing by \( n \), call the set of these remainders \( \mathbb{Z}/n\mathbb{Z} \).

Example

1. \( 7 \equiv 2 \pmod{5} \)
2. \( -4 \equiv 2 \pmod{3} \)
3. \( 56 \equiv 1 \pmod{5} \)
Modular arithmetic

**Definition**

Let $q, n \in \mathbb{Z}$ we say $q \equiv r \pmod{n}$ if there is an $a \in \mathbb{Z}$ such that $q = an + r$. 

Example

1. $7 \equiv 2 \pmod{5}$
2. $-4 \equiv 2 \pmod{3}$
3. $56 \equiv 1 \pmod{5}$
Modular arithmetic

Definition

Let $q, n \in \mathbb{Z}$ we say $q \equiv r \pmod{n}$ if there is an $a \in \mathbb{Z}$ such that $q = an + r$.

Idea: Fix $n$, then classify all integers by their remainder when dividing by $n$, call the set of these remainders $\mathbb{Z}/n\mathbb{Z}$.

Example

1. $7 \equiv 2 \pmod{5}$
2. $-4 \equiv 2 \pmod{3}$
3. $56 \equiv 1 \pmod{5}$
Modular arithmetic

Definition

Let $q, n \in \mathbb{Z}$ we say $q \equiv r \pmod{n}$ if there is an $a \in \mathbb{Z}$ such that $q = an + r$.

Idea: Fix $n$, then classify all integers by their remainder when dividing by $n$, call the set of these remainders $\mathbb{Z}/n\mathbb{Z}$.

Example

1. $7 \equiv 2 \pmod{5}$
Modular arithmetic

**Definition**

Let $q, n \in \mathbb{Z}$ we say $q \equiv r \pmod{n}$ if there is an $a \in \mathbb{Z}$ such that $q = an + r$.

Idea: Fix $n$, then classify all integers by their remainder when dividing by $n$, call the set of these remainders $\mathbb{Z}/n\mathbb{Z}$.

**Example**

1. $7 \equiv 2 \pmod{5}$
2. $-4 \equiv 2 \pmod{3}$
## Modular arithmetic

### Definition

Let $q, n \in \mathbb{Z}$ we say $q \equiv r \pmod{n}$ if there is an $a \in \mathbb{Z}$ such that $q = an + r$.

Idea: Fix $n$, then classify all integers by their remainder when dividing by $n$, call the set of these remainders $\mathbb{Z}/n\mathbb{Z}$.

### Example

1. $7 \equiv 2 \pmod{5}$
2. $-4 \equiv 2 \pmod{3}$
3. $56 \equiv 1 \pmod{5}$
Modular arithmetic

**Definition**

Let \( q, n \in \mathbb{Z} \) we say \( q \equiv r \pmod{n} \) if there is an \( a \in \mathbb{Z} \) such that \( q = an + r \).

Idea: Fix \( n \), then classify all integers by their remainder when dividing by \( n \), call the set of these remainders \( \mathbb{Z}/n\mathbb{Z} \).

**Example**

1. \( 7 \equiv 2 \pmod{5} \)
2. \( -4 \equiv 2 \pmod{3} \)
3. \( 56 = 7 \cdot 8 \equiv 2 \cdot 3 = 6 \equiv 1 \pmod{5} \)
Fact
Suppose \( a \equiv r \pmod{n} \) and \( b \equiv q \pmod{n} \) then \( ab \equiv rq \pmod{n} \).

Example
\( 2 \times 2 = y^2 \)
Assume \( \gcd(x, y) = 1 \).

What are the possible values of \( x^2 \) and \( y^2 \pmod{4} \)?
Fact

Suppose \( a \equiv r \pmod{n} \) and \( b \equiv q \pmod{n} \) then \( ab \equiv rq \pmod{n} \).
Modular arithmetic (Cont.)

Fact
Suppose \( a \equiv r \pmod{n} \) and \( b \equiv q \pmod{n} \) then \( ab \equiv rq \pmod{n} \).

Example

\[ 2x^2 = y^2 \]

Assume \( \gcd(x, y) = 1 \).
What are the possible values of \( x^2 \) and \( y^2 \) mod 4?
**Fact**

Suppose \(a \equiv r \pmod{n}\) and \(b \equiv q \pmod{n}\) then \(ab \equiv rq \pmod{n}\).

**Example**

\[2x^2 = y^2\]

Assume \(\gcd(x, y) = 1\).

What are the possible values of \(x^2\) and \(y^2 \pmod{4}\)?

- \(0^2 \equiv 0 \pmod{4}\)
- \(1^2 \equiv 1 \pmod{4}\)
- \(2^2 \equiv 0 \pmod{4}\)
- \(3^2 \equiv 1 \pmod{4}\)
Fact

Suppose $a \equiv r \pmod{n}$ and $b \equiv q \pmod{n}$ then $ab \equiv rq \pmod{n}$.

Example

$$2x^2 = y^2$$

Assume $\gcd(x, y) = 1$.

What are the possible values of $x^2$ and $y^2 \pmod{4}$?

$$\{0, 1\}$$
Fact
Suppose \( a \equiv r \pmod{n} \) and \( b \equiv q \pmod{n} \) then \( ab \equiv rq \pmod{n} \).

Example

\[ 2x^2 = y^2 \]

Assume \( \gcd(x, y) = 1 \).
What are the possible values of \( x^2 \) and \( y^2 \) \( \pmod{4} \)?

\[ \{0, 1\} \]

Thus \( x^2 \equiv 0 \pmod{4} \) and \( y^2 \equiv 0 \pmod{4} \) but this is a contradiction to the assumption that \( \gcd(x, y) = 1 \).
• A homogeneous polynomial of degree $n$ is a polynomial for which each monomial is degree $n$.

• Degree $n$ projective space over $\mathbb{Q}$, $\mathbb{P}^n_\mathbb{Q}$, is the set of points $[x_0:x_1: \cdots :x_n] \in \mathbb{Q}^{n+1} \setminus \{0\}$ such that $\forall \lambda \in \mathbb{Q} \setminus \{0\}$ $[x_0:x_1: \cdots :x_n] = [\lambda x_0: \lambda x_1: \cdots :\lambda x_n]$.

• Suppose $f_1, \ldots, f_m$ are homogeneous polynomials in $n$ variables. The projective variety, $X = V(f_1, \ldots, f_m)$, is the set of points $P$ such that $f_i(P) = 0 \forall i$. Further $X(\mathbb{Q}) := \{P \in \mathbb{P}^n_\mathbb{Q} \mid f_i(P) = 0 \forall i\}$. 

7
Definitions

- A **homogeneous polynomial of degree** \( n \) is a polynomial for which each monomial is degree \( n \).
Varieties

Definitions

- A **homogeneous polynomial of degree** \( n \) is a polynomial for which each monomial is degree \( n \).
- **Degree** \( n \) **projective space over** \( \mathbb{Q} \), \( \mathbb{P}^n_{\mathbb{Q}} \), is the set of points \([x_0 : x_1 : \cdots : x_n] \in \mathbb{Q}^{n+1} \setminus \{0\}\) such that \( \forall \lambda \in \mathbb{Q} \setminus \{0\} \)
  \[ [x_0 : x_1 : \cdots : x_n] = [\lambda x_0 : \lambda x_1 : \cdots : \lambda x_n]. \]
Definitions

• A **homogeneous polynomial of degree** $n$ is a polynomial for which each monomial is degree $n$.

• **Degree $n$ projective space over** $\mathbb{Q}$, $\mathbb{P}_\mathbb{Q}^n$, is the set of points $[x_0 : x_1 : \cdots : x_n] \in \mathbb{Q}^{n+1} \setminus \{0\}$ such that $\forall \lambda \in \mathbb{Q} \setminus \{0\}$
  
  $[x_0 : x_1 : \cdots : x_n] = [\lambda x_0 : \lambda x_1 : \cdots : \lambda x_n]$.

• Suppose $f_1, \ldots, f_m$ are homogeneous polynomials in $n$ variables. The **projective variety**, $X = V(f_1, \ldots, f_m)$, is the set of points $P$ such that $f_i(P) = 0 \forall i$. Further
  
  $X(\mathbb{Q}) := \{ P \in \mathbb{P}_\mathbb{Q}^{n-1} \mid f_i(P) = 0 \forall i \}$.
Note \( Q \)-points = \( Z \)-points

Claim \( X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \) for all \( n > 0 \), \( p \) is much easier to determine than \( X(\mathbb{Z}) \neq \emptyset \).

• By Hensel's Lemma, only need to check finitely many \( n \) for each \( p \).

• By the Weil Conjectures, only need to check finitely many \( p \).
Mod $p$ Points

Note

$\mathbb{Q}$-points $= \mathbb{Z}$-points
Note

\( \mathbb{Q}\)-points = \( \mathbb{Z}\)-points

Claim

\( X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \ \forall \ n, \ p \) is much easier to determine than \( X(\mathbb{Z}) \neq \emptyset \)
Note

\( \mathbb{Q}\text{-points} = \mathbb{Z}\text{-points} \)

Claim

\[ X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \ \forall \ n, \ p \text{ is much easier to determine than } X(\mathbb{Z}) \neq \emptyset \]

- By *Hensel’s Lemma* only need to check finitely many \( n \) for each \( p \).
Mod $p$ Points

Note

$\mathbb{Q}$-points $= \mathbb{Z}$-points

Claim

$X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \forall n, p$ is much easier to determine than $X(\mathbb{Z}) \neq \emptyset$

- By Hensel’s Lemma only need to check finitely many $n$ for each $p$.
- By the Weil Conjectures only need to check finitely many $p$. 
The Hasse Principle

We say $X$ satisfies the Hasse Principle if $X(R) \neq \emptyset$ and $X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset$ for all $n, p$. Note the Adelic points of $X$ are denoted $X(A_{\mathbb{Q}})$. The condition that $X(R) \neq \emptyset$ and $X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset$ for all $n, p$ is equivalent to saying $X(A_{\mathbb{Q}}) \neq \emptyset$. 
The Hasse Principle

Note

\[ X(\mathbb{Z}) \neq \emptyset \Rightarrow X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \ \forall \ n, p \ \text{and} \ X(\mathbb{R}) \neq \emptyset \]
The Hasse Principle

Note

\[ X(\mathbb{Z}) \neq \emptyset \Rightarrow X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \ \forall \ n, p \ \text{and} \ \ X(\mathbb{R}) \neq \emptyset \]

The Hasse Principle

We say \( X \) satisfies the **Hasse Principle** if

\[ X(\mathbb{R}) \neq \emptyset \text{ and } X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \ \forall \ n, p \ \Rightarrow \ X(\mathbb{Z}) \neq \emptyset. \]
The Hasse Principle

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X(\mathbb{Z}) \neq \emptyset \Rightarrow X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \ \forall n, p$ and $X(\mathbb{R}) \neq \emptyset$.</td>
</tr>
</tbody>
</table>

The Hasse Principle

We say $X$ satisfies the **Hasse Principle** if

$$X(\mathbb{R}) \neq \emptyset \text{ and } X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \ \forall n, p \Rightarrow X(\mathbb{Z}) \neq \emptyset.$$ 

Note

The **Adelic points** of $X$ are denoted $X(A_{\mathbb{Q}})$. The condition that $X(\mathbb{R}) \neq \emptyset$ and $X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \ \forall n, p$ is equivalent to saying $X(A_{\mathbb{Q}}) \neq \emptyset$. 
Examples

1. $x^2 - 2y^2 = 0$ has $X(\mathbb{Z}/4\mathbb{Z}) = \emptyset$ so $X(\mathbb{Q}) = \emptyset$.

2. $3x^2 - 5y^2 - 7z^2 = 0$ has $X(\mathbb{Q}) \neq \emptyset$ and $X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset$ for $p = 2, 3, 5, 7, 11, \ldots, M$.

Use a computer with $M = 499$:

```magma
MAGMA
> time {IsLocallySolvable(X,p) : p in primesToM};
{ true }
Time: 0.100
```
Examples

Quadratic equations satisfy the Hasse Principle.
Examples

Quadratic equations satisfy the Hasse Principle.

1. $X : y^2 - 2x^2 = 0$ has $X(\mathbb{Z}/4\mathbb{Z}) = \emptyset$ so $X(\mathbb{Q}) = \emptyset$
Examples

Quadratic equations satisfy the Hasse Principle.

1. $X: y^2 - 2x^2 = 0$ has $X(\mathbb{Z}/4\mathbb{Z}) = \emptyset$ so $X(\mathbb{Q}) = \emptyset$

2. $X: 3x^2 - 5y^2 - 7z^2 = 0$ has $X(\mathbb{A}_\mathbb{Q}) \neq \emptyset$

Check $X(\mathbb{R}) \neq \emptyset$ and $X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset$ for $p = 2, 3, 5, 7, 11, \ldots, M$. 

Use a computer with $M = 499$:

```plaintext
MAGMA > time {IsLocallySolvable(X,p) : p in primesToM};
{ true }
Time: 0.100
```
Examples

Quadratic equations satisfy the Hasse Principle.

1. \( X : y^2 - 2x^2 = 0 \) has \( X(\mathbb{Z}/4\mathbb{Z}) = \emptyset \) so \( X(\mathbb{Q}) = \emptyset \)

2. \( X : 3x^2 - 5y^2 - 7z^2 = 0 \) has \( X(\mathbb{A}_\mathbb{Q}) \neq \emptyset \)
   
   Check \( X(\mathbb{R}) \neq \emptyset \) and \( X(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset \) for \( p = 2, 3, 5, 7, 11, \ldots, M \).
   
   Use a computer with \( M = 499 \):

```
> time {IsLocallySolvable(X,p) : p in primesToM};
{ true }
Time: 0.100
```
Examples (Cont.)

Actually for $X: 3x^2 - 5y^2 - 7z^2 = 0$, there are some easy rational points.

MAGMA

```plaintext
> PointSearch(X, 2);
[ (-2 : 1 : 1), (2 : -1 : 1), (-2 : -1 : 1), (2 : 1 : 1) ]
```
Actually for

\[ X : 3x^2 - 5y^2 - 7z^2 = 0, \]

there are some easy rational points.
Examples (Cont.)

Actually for

\[ X : 3x^2 - 5y^2 - 7z^2 = 0, \]

there are some easy rational points.

**MAGMA**

```
> PointSearch(X,2);
[ (-2 : 1 : 1), (2 : -1 : 1), (-2 : -1 : 1), (2 : 1 : 1) ]
```
Consider $X$: 

\begin{align*}
&x^2 + y^2 - z^2 = 0, \\
&xy - 2 \cdot 157w^2 = 0.
\end{align*}

In this case, $X(A_Q) \neq \emptyset$ so $X(Q) \neq \emptyset$.

Actually, the smallest rational point with $w \neq 0$ is

\begin{align*}
x &= 2^2 \cdot 3^4 \cdot 5^2 \cdot 13^2 \cdot 17^2 \cdot 37^2 \cdot 101^2 \cdot 157^2 \cdot 17401^2 \cdot 46997^2 \cdot 356441^2, \\
y &= 157^{841} \cdot 4947203^2 \cdot 526771095761^2, \\
z &= 20085078913 \cdot 1185369214457 \cdot 9425458255024420419074801, \\
w &= 2^2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 157841 \cdot 356441 \cdot 4947203 \cdot 526771095761.
\end{align*}
Consider

\[ X: \begin{cases} x^2 + y^2 - z^2 = 0, \\ xy - 2 \cdot 157w^2 = 0. \end{cases} \]
Consider

\[ X : \begin{cases} 
  x^2 + y^2 - z^2 &= 0, \\
  xy - 2 \cdot 157 w^2 &= 0. 
\end{cases} \]

In this case, \( X(\mathbb{A}_\mathbb{Q}) \neq \emptyset \) so \( X(\mathbb{Q}) \neq \emptyset \).
Examples (Cont.)

Consider

$$X: \begin{cases} x^2 + y^2 - z^2 &= 0, \\ xy - 2 \cdot 157w^2 &= 0. \end{cases}$$

In this case, $X(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ so $X(\mathbb{Q}) \neq \emptyset$. Actually, the smallest rational point with $w \neq 0$ is

$$\begin{align*}
x &= 2^3 \cdot 3^4 \cdot 5^2 \cdot 13^2 \cdot 17^2 \cdot 37^2 \cdot 101^2 \cdot 157 \cdot 17401^2 \cdot 46997^2 \cdot 356441^2, \\
y &= 157841^2 \cdot 4947203^2 \cdot 526771095761^2, \\
z &= 20085078913 \cdot 1185369214457 \cdot 9425458255024420419074801, \\
w &= 2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 157841 \cdot 356441 \cdot 4947203 \cdot 526771095761.\end{align*}$$
Cubic Surfaces
Example (Swinnerton-Dyer (1962))

The following surface does not satisfy the Hasse Principle

\[ X: y(y + x)(2y + x) = \prod (x + \phi z + \phi^2 w), \]

where the product is taken over the roots of

\[ T^3 - 7T^2 + 14T - 7 = 0. \]
Conjecture (Mordell (1949))

Cubic surfaces defined over $\mathbb{Q}$ satisfy the Hasse Principle.

Example (Swinnerton-Dyer (1962))

The following surface does not satisfy the Hasse Principle:

$$X = y(y + x)(2y + x) = \prod (x + \phi z + \phi^2 w),$$

where the product is taken over the roots of $T^3 - 7T^2 + 14T - 7 = 0.$
Conjecture (Mordell (1949))

Cubic surfaces defined over \( \mathbb{Q} \) satisfy the Hasse Principle.

Example (Swinnerton-Dyer (1962))

The following surface does not satisfy the Hasse Principle

\[ X : y(y + x)(2y + x) = \prod (x + \phi z + \phi^2 w), \]

where the product is taken over the roots of \( T^3 - 7 T^2 + 14 T - 7 = 0. \)
Diagonal Cubics?

Theorem (Selmer (1953))
Cubic surfaces of the form
\[ ax^3 + by^3 + cz^3 + dw^3 = 0. \]
where \( ab = cd \) satisfy the Hasse Principle.

Conjecture (Selmer (1953))
Diagonal cubic surfaces satisfy the Hasse principle.
Theorem (Selmer (1953))

Cubic surfaces of the form

\[ ax^3 + by^3 + cz^3 + dw^3 = 0. \]

where \( ab = cd \) satisfy the Hasse Principle.
Theorem (Selmer (1953))

Cubic surfaces of the form

\[ ax^3 + by^3 + cz^3 + dw^3 = 0. \]

where \( ab = cd \) satisfy the Hasse Principle.

Conjecture (Selmer (1953))

Diagonal cubic surfaces satisfy the Hasse principle.
The diagonal cubic surface defined by
\[5x^3 + 9y^3 + 12z^3 + 10w^3 = 0,\]
does not satisfy the Hasse Principle.
Diagonal Cubics? (Cont.)

Example (Cassels–Guy (1966))

The diagonal cubic surface defined by

\[ 5x^3 + 9y^3 + 12z^3 + 10w^3 = 0, \]

does not satisfy the Hasse Principle.
Central Simple Algebras

Definition

A central simple algebra, \( A \), over a field \( k \) is

- a \( k \)-algebra, i.e. a vector space over \( k \) that also has a multiplicative structure
- central, i.e. \( Z(A) := \{ x \in A | x \cdot a = a \cdot x \ \forall a \in A \} = k \),
- and simple, i.e. \( \{0\} \) and \( A \) are the only two-sided ideals of \( A \).

Example (Quaternions over \( \mathbb{R} \))

Suppose \( i^2 = j^2 = -1 \) and \( ji = -ij \), the quaternions over \( \mathbb{R} \) are \( A = H := \{a + ib + jc +ijd : a, b, c, d \in \mathbb{R} \} \).
A central simple algebra, $\mathcal{A}$, over a field $k$ is

- a $k$-algebra i.e. a vector space over $k$ that also has a multiplicative structure

Example (Quaternions over $\mathbb{R}$)

Suppose $i^2 = j^2 = -1$ and $ji = -ij$, the quaternions over $\mathbb{R}$ are $\mathcal{A} = \mathbb{H} := \{a + ib + jc + jd : a, b, c, d \in \mathbb{R}\}$. 
Central Simple Algebras

Definition

A central simple algebra, $\mathcal{A}$, over a field $k$ is

- a **k-algebra** i.e. a vector space over $k$ that also has a multiplicative structure
- it is **central** i.e. $Z(\mathcal{A}) := \{ x \in \mathcal{A} \mid x \cdot a = a \cdot x \ \forall \ a \in \mathcal{A} \} = k$.

Example (Quaternions over $\mathbb{R}$)

Suppose $i^2 = j^2 = -1$ and $ji = -ij$, the quaternions over $\mathbb{R}$ are $\mathcal{A} = \mathbb{H} := \{ a + ib + jc + jd : a, b, c, d \in \mathbb{R} \}$. 
Central Simple Algebras

Definition

A central simple algebra, $\mathcal{A}$, over a field $k$ is

- a $k$-algebra i.e. a vector space over $k$ that also has a multiplicative structure
- it is central i.e. $Z(\mathcal{A}) := \{x \in \mathcal{A} \mid x \cdot a = a \cdot x \forall a \in \mathcal{A}\} = k$,
- and simple i.e. $\{0\}$ and $\mathcal{A}$ are the only two-sided ideals of $\mathcal{A}$.

Example (Quaternions over $\mathbb{R}$)

Suppose $i^2 = j^2 = -1$ and $ji = -ij$, the quaternions over $\mathbb{R}$ are $\mathcal{A} = \mathbb{H} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$. 

17
Definition

A central simple algebra, $A$, over a field $k$ is

- a $k$-algebra i.e. a vector space over $k$ that also has a multiplicative structure
- it is central i.e. $Z(A) := \{x \in A \mid x \cdot a = a \cdot x \forall a \in A\} = k$,
- and simple i.e. $\{0\}$ and $A$ are the only two-sided ideals of $A$.

Example (Quaternions over $\mathbb{R}$)

Suppose $i^2 = j^2 = -1$ and $ji = -ij$, the quaternions over $\mathbb{R}$ are

$$A = \mathbb{H} := \{a + ib + jc + ijd : a, b, c, d \in \mathbb{R}\}.$$
The Brauer Group

Definition

Suppose $k$ is a field. Then the Brauer group of $k$ is

$$\text{Br}(k) := \{ \text{CSA's} / k \} / \sim$$

where $A \sim B$ if $M_a(A) \cong M_b(B)$ for some $a, b$.

Examples

• $\text{Br} \mathbb{R} = \{ [\mathbb{R}], [\mathbb{H}] \} \cong \mathbb{Z} / 2\mathbb{Z}$

• $\text{Br} \mathbb{C} = \{ [\mathbb{C}] \}$

• $\text{Br} \mathbb{Q}$ is infinite

• $\text{Br} \mathbb{Q}_p \cong \mathbb{Q} / \mathbb{Z}$
Suppose $k$ is a field. Then the **Brauer group of $k$** is

$$\text{Br}(k) := \{\text{CSA's}/k\}/\sim$$

where $\mathcal{A} \sim \mathcal{B}$ if $M_a(\mathcal{A}) \cong M_b(\mathcal{B})$ for some $a, b$. 

**Examples**

- $\text{Br}\mathbb{R} = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z}$
- $\text{Br}\mathbb{C} = \{[\mathbb{C}]\}$
- $\text{Br}\mathbb{Q}$ is infinite
- $\text{Br}\mathbb{Q}_p \cong \mathbb{Q}/\mathbb{Z}$
The Brauer Group

Definition
Suppose $k$ is a field. Then the **Brauer group of $k$** is

$$\text{Br}(k) := \{\text{CSA's}/k\}/\sim$$

where $\mathcal{A} \sim \mathcal{B}$ if $M_a(\mathcal{A}) \cong M_b(\mathcal{B})$ for some $a, b$.

Examples

- $\text{Br} \mathbb{R} = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z}$
The Brauer Group

Definition

Suppose \( k \) is a field. Then the **Brauer group of \( k \)** is

\[
\text{Br}(k) := \{\text{CSA’s}/k\}/ \sim
\]

where \( \mathcal{A} \sim \mathcal{B} \) if \( M_a(\mathcal{A}) \cong M_b(\mathcal{B}) \) for some \( a, b \).

Examples

- \( \text{Br } \mathbb{R} = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z} \)
- \( \text{Br } \mathbb{C} = \{[\mathbb{C}]\} \)
The Brauer Group

Definition

Suppose $k$ is a field. Then the **Brauer group of** $k$ is

$$\text{Br}(k) := \{\text{CSA's}/k\}/ \sim$$

where $A \sim B$ if $M_a(A) \cong M_b(B)$ for some $a, b$.

Examples

- $\text{Br } \mathbb{R} = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z}$
- $\text{Br } \mathbb{C} = \{[\mathbb{C}]\}$
- $\text{Br } \mathbb{Q}$ is infinite
The Brauer Group

**Definition**

Suppose \( k \) is a field. Then the **Brauer group of \( k \)** is

\[
\text{Br}(k) := \{\text{CSA's}/k\}/ \sim
\]

where \( \mathcal{A} \sim \mathcal{B} \) if \( M_a(\mathcal{A}) \cong M_b(\mathcal{B}) \) for some \( a, b \).

**Examples**

- \( \text{Br } \mathbb{R} = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z} \)
- \( \text{Br } \mathbb{C} = \{[\mathbb{C}]\} \)
- \( \text{Br } \mathbb{Q} \) is infinite
- \( \text{Br } \mathbb{Q}_p \cong \mathbb{Q}/\mathbb{Z} \)
The Brauer–Manin Obstruction

Idea

\[ X(\mathbb{Q}) \subseteq X(A_{\mathbb{Q}}) \]

\[ \text{Br} \subseteq X(A_{\mathbb{Q}}) \]

Definition (Manin (1971, '74))

We say \( X \) has a Brauer–Manin obstruction to the Hasse Principle if

\[ X(A_{\mathbb{Q}}) \neq \emptyset \]

\[ X(A_{\mathbb{Q}})_{\text{Br}} = \emptyset \]

Conjecture (Colliot-Thélène–Sansuc, 1979)

The Brauer–Manin obstruction is the only obstruction to the Hasse principle for cubic surfaces.
The Brauer–Manin Obstruction

**Definition (Manin (1971, '74))**
We say $X$ has a Brauer–Manin obstruction to the Hasse Principle if $X(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ and $X(\mathbb{A}_\mathbb{Q})^{Br} = \emptyset$.

**Conjecture (Colliot-Thélène–Sansuc, 1979)**
The Brauer–Manin obstruction is the only obstruction to the Hasse principle for cubic surfaces.

**Idea**

\[
X(\mathbb{Q}) \subseteq X(\mathbb{A}_\mathbb{Q})^{Br} \subseteq X(\mathbb{A}_\mathbb{Q})
\]
The Brauer–Manin Obstruction

**Idea**

\[ X(\mathbb{Q}) \subseteq X(\mathbb{A}_\mathbb{Q})^{\text{Br}} \subseteq X(\mathbb{A}_\mathbb{Q}) \]

**Definition (Manin (1971, ’74))**

We say \( X \) has a **Brauer–Manin obstruction to the Hasse Principle** if \( X(\mathbb{A}_\mathbb{Q}) \neq \emptyset \) and \( X(\mathbb{A}_\mathbb{Q})^{\text{Br}} = \emptyset \).
The Brauer–Manin Obstruction

**Idea**

\[ X(\mathbb{Q}) \subseteq X(A_{\mathbb{Q}})^{Br} \subseteq X(A_{\mathbb{Q}}) \]

**Definition (Manin (1971, ’74))**

We say \( X \) has a **Brauer–Manin obstruction to the Hasse Principle** if \( X(A_{\mathbb{Q}}) \neq \emptyset \) and \( X(A_{\mathbb{Q}})^{Br} = \emptyset \).

**Conjecture (Colliot-Thélène–Sansuc, 1979)**

The Brauer–Manin obstruction is the only obstruction to the Hasse principle for cubic surfaces.
Some Evidence

\[ X : 5x^3 + 9y^3 + 12z^3 + 10w^3 = 0 \]

\[ X(A_\mathcal{Q}) \neq \emptyset, \quad \text{and} \quad (X(A_\mathcal{Q}))_{Br} = \emptyset \]
$X : 5x^3 + 9y^3 + 12z^3 + 10w^3 = 0$
Some Evidence

Example

\[ X: 5x^3 + 9y^3 + 12z^3 + 10w^3 = 0 \]

\[ X(A_Q) \neq \emptyset, \text{ and } (X(A_Q))^{Br} = \emptyset \]
Some Evidence

Example

\[ X : 5x^3 + 9y^3 + 12z^3 + 10w^3 = 0 \]

\[ X(\mathbb{A}_\mathbb{Q}) \neq \emptyset, \text{ and } (X(\mathbb{A}_\mathbb{Q}))^{Br} = \emptyset \]

Theorem (Colliot-Thélène–Kanevsky–Sansuc (1987), Corn (2005))

For all integers 0 < a, b, c, d \leq 200, the Brauer–Manin obstruction is the only obstruction to the Hasse Principle for the diagonal cubics

\[ X : ax^3 + by^3 + cz^3 + dw^3 = 0. \]
The Clebsch Cubic

\[ x^3 + y^3 + z^3 + w^3 = (x + y + z + w)^3 \]

Note: Every cubic surface in \( \mathbb{P}^3 \) contains exactly 27 lines!!
The Clebsch Cubic

\[ x^3 + y^3 + z^3 + w^3 = (x + y + z + w)^3 \]
The Clebsch Cubic

\[ x^3 + y^3 + z^3 + w^3 = (x + y + z + w)^3 \]

**Note**

Every cubic surface in \( \mathbb{P}^3_C \) contains exactly 27 lines!!

For $X$ a cubic surface, there is an explicit way to compute $\text{Br}_X$ using the lines on $X$. 

For $X$ a cubic surface, there is an explicit way to compute $\text{Br} X$ and $X(\mathbb{A}_\mathbb{Q})^{\text{Br}}$ using the lines on $X$. 
x^3 + y^3 + z^3 + w^3 = 0

We have 3 possibilities:

ax^3 + by^3 = 0

ax^3 + cz^3 = 0

ax^3 + dw^3 = 0

cz^3 + dw^3 = 0

by^3 + dw^3 = 0

by^3 + cz^3 = 0

x = -\zeta^i_3 \left( \frac{b}{a} \right)^{1/3}

y = -\zeta^i_3 \left( \frac{c}{a} \right)^{1/3}

z = -\zeta^i_3 \left( \frac{d}{a} \right)^{1/3}

w = -\zeta^j_3 \left( \frac{d}{c} \right)^{1/3}

w = -\zeta^j_3 \left( \frac{c}{b} \right)^{1/3}

where \( \zeta_3 \) is a primitive third root of unity and 1 \( \leq i, j \leq 3 \).
Lines on a Diagonal Surface

\[ X : ax^3 + by^3 + cz^3 + dw^3 = 0 \]
\[ X : ax^3 + by^3 + cz^3 + dw^3 = 0 \]

We have 3 possibilities:

\[
\begin{align*}
ax^3 + by^3 &= 0 \\
ax^3 + cz^3 &= 0 \\
ax^3 + dw^3 &= 0 \\
cz^3 + dw^3 &= 0 \\
by^3 + dw^3 &= 0 \\
by^3 + cz^3 &= 0 \\
\end{align*}
\]

where \( \zeta^3 \) is a primitive third root of unity and \( 1 \leq i, j \leq 3 \).
Lines on a Diagonal Surface

\[ X : ax^3 + by^3 + cz^3 + dw^3 = 0 \]

We have 3 possibilities:

<table>
<thead>
<tr>
<th>[ ax^3 + by^3 = 0 ]</th>
<th>[ ax^3 + cz^3 = 0 ]</th>
<th>[ ax^3 + dw^3 = 0 ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ cz^3 + dw^3 = 0 ]</td>
<td>[ by^3 + dw^3 = 0 ]</td>
<td>[ by^3 + cz^3 = 0 ]</td>
</tr>
</tbody>
</table>

| \[ x = -\zeta_3^i(b/a)^{1/3}y \] | \[ x = -\zeta_3^i(c/a)^{1/3}z \] | \[ x = -\zeta_3^i(d/a)^{1/3}w \] |
| \[ z = -\zeta_3^j(d/c)^{1/3}w \] | \[ y = -\zeta_3^j(d/b)^{1/3}w \] | \[ y = -\zeta_3^j(c/b)^{1/3}z \] |

where \( \zeta_3 \) is a primitive third root of unity and \( 1 \leq i, j \leq 3 \).
Suppose \( L/\mathbb{Q} \) is the splitting field of the cubic polynomial \( f(t) \) with \( \text{Gal}(L/\mathbb{Q}) = S_3 \) and \( K(\theta)/\mathbb{Q} \) is the unique quadratic extension contained in \( L \). Take \( \phi_1, \phi_2, \phi_3 \) to be the roots of \( f(t) \).

Theorem (W.) With certain assumptions on \( L \), \( \theta \), and \( p \),

\[
py(x + \theta y)(x + \theta y) = 3 \prod_{i=1}^{\infty} (x + \phi_i z + \phi_i w),
\]

has a Brauer–Manin obstruction to the Hasse Principle.
Suppose $L/\mathbb{Q}$ is the splitting field of the cubic polynomial $f(t)$ with $\text{Gal}(L/\mathbb{Q}) = S_3$ and $K(\theta)/\mathbb{Q}$ is the unique quadratic extension contained in $L$. Take $\phi_1, \phi_2, \phi_3$ to be the roots of $f(t)$. 

Theorem (W.) With certain assumptions on $L$, $\theta$, and $p$, $p(y)(x + \theta y) = 3 \prod_{i=1}^3 (x + \phi_i z + \phi_i w)$, has a Brauer–Manin obstruction to the Hasse Principle.
Another Family of Cubic Surfaces

Suppose $L/\mathbb{Q}$ is the splitting field of the cubic polynomial $f(t)$ with $\text{Gal}(L/\mathbb{Q}) = S_3$ and $K(\theta)/\mathbb{Q}$ is the unique quadratic extension contained in $L$. Take $\phi_1, \phi_2, \phi_3$ to be the roots of $f(t)$.

**Theorem (W.)**

_With certain assumptions on $L$, $\theta$, and $p$,$_

\[ py(x + \theta y)(x + \overline{\theta} y) = \prod_{i=1}^{3} (x + \phi_i z + \phi_i^2 w), \]

has a Brauer–Manin obstruction to the Hasse Principle._
What Are the Lines?

\[ py(x + \theta y)(x + \overline{\theta} y) = \prod_{i=1}^{3} (x + \phi_i z + \phi_i^2 w), \]
What Are the Lines?

\[ py(x + \theta y)(x + \bar{\theta} y) = \prod_{i=1}^{3} (x + \phi_i z + \phi_i^2 w), \]

The easy ones:

- \( L_{i,1} \):
  \[
  \begin{align*}
  x + \phi_i z + \phi_i^2 w &= 0 \\
  y &= 0
  \end{align*}
  \]

- \( L_{i,2} \):
  \[
  \begin{align*}
  x + \phi_i z + \phi_i^2 w &= 0 \\
  x + \theta y &= 0
  \end{align*}
  \]

- \( L_{i,3} \):
  \[
  \begin{align*}
  x + \phi_i z + \phi_i^2 w &= 0 \\
  x + \bar{\theta} y &= 0
  \end{align*}
  \]
In 3 dimensions, lines have 2 parameters:

\[
\begin{align*}
    x &= as + bt \\
    y &= cs + dt \\
    z &= es + ft \\
    w &= gs + ht
\end{align*}
\]
Parametrization of Lines

In 3 dimensions, lines have 2 parameters:

\[
\begin{align*}
x &= as + bt \\
y &= cs + dt \\
z &= es + ft \\
w &= gs + ht
\end{align*}
\]

\[
\begin{bmatrix} x & y & z & w \end{bmatrix} = \begin{bmatrix} s & t \end{bmatrix} \begin{bmatrix} a & c & e & g \\ b & d & f & h \end{bmatrix}
\]

Therefore \([x \ y \ z \ w]\) is in the row space of the matrix above, thus it will suffice to consider the reduced echelon form of \(A\).
In 3 dimensions, lines have 2 parameters:

\[
\begin{align*}
x &= as + bt \\
y &= cs + dt \\
z &= es + ft \\
w &= gs + ht
\end{align*}
\]

\[
\Rightarrow \begin{bmatrix} x & y & z & w \end{bmatrix} = \begin{bmatrix} s & t \end{bmatrix} \begin{bmatrix} a & c & e & g \\ b & d & f & h \end{bmatrix}
\]

Therefore \(\begin{bmatrix} x & y & z & w \end{bmatrix}\) is in the row space of the matrix above, \(A\), thus it will suffice to consider the reduced echelon form of \(A\).
### Possible Parametrizations

| 27 |
|---|---|---|---|---|
| $\alpha$ | $\beta$ | 0 | 0 | 0 | 1 |
| 0 | 1 | $\alpha$ | 0 | 0 | 1 | $\gamma$ |
| 0 | 1 | $\alpha$ | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 |
Possible Parametrizations

\[
\begin{bmatrix}
1 & 0 & \alpha & \beta \\
0 & 1 & \gamma & \delta
\end{bmatrix}
\begin{bmatrix}
1 & \alpha & 0 & \beta \\
0 & 0 & 1 & \gamma
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & \alpha & \beta & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
0 & 1 & 0 & \alpha \\
0 & 0 & 1 & \gamma
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & \alpha & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]
Possible Parametrizations

\[
\begin{bmatrix}
1 & 0 & \alpha & \beta \\
0 & 1 & \gamma & \delta \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & \alpha & 0 & \beta \\
0 & 0 & 1 & \gamma \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & \alpha & \beta & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & \gamma \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & \alpha & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{bmatrix}
\]
Possible Parametrizations

\[
\begin{bmatrix}
1 & 0 & \alpha & \beta \\
0 & 1 & \gamma & \delta
\end{bmatrix} \quad \begin{bmatrix}
1 & \alpha & 0 & \beta \\
0 & 0 & 1 & \gamma
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & \alpha & \beta & 0 \\
0 & 0 & 0 & 1
\end{bmatrix} \quad \begin{bmatrix}
0 & 1 & 0 & \alpha \\
0 & 0 & 1 & \gamma
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & \alpha & 0 \\
0 & 0 & 0 & 1
\end{bmatrix} \quad \begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]
The Other Lines

Using MAGMA and Gröbner Bases, we find

\[
\begin{align*}
1 + A\phi_i + C\phi_2^i &= 0, \\
\theta(1 + A\phi_j + C\phi_2^j) &= (B\phi_j + D\phi_2^j), \\
\theta(1 + A\phi_k + C\phi_2^k) &= (B\phi_k + D\phi_2^k), \\
(B\phi_0 + D\phi_2^0)(B\phi_1 + D\phi_2^1)(B\phi_2 + D\phi_2^2) &= \theta^2.
\end{align*}
\]
L: $\begin{cases} Ax + By = z \\ Cx + Dy = w \end{cases}$
\[ L: \begin{cases} Ax + By &= z \\ Cx + Dy &= w \end{cases} \]

Using MAGMA and Gröbner Bases, we find

\[
\begin{align*}
1 + A\phi_i + C\phi_i^2 &= 0, \\
\theta(1 + A\phi_j + C\phi_j^2) &= (B\phi_j + D\phi_j^2), \\
\bar{\theta}(1 + A\phi_k + C\phi_k^2) &= (B\phi_k + D\phi_k^2), \\
(B\phi_0 + D\phi_0^2)(B\phi_1 + D\phi_1^2)(B\phi_2 + D\phi_2^2) &= p\theta\bar{\theta}.
\end{align*}
\]
Degree 2 del Pezzo Surfaces
Degree 2 del Pezzo Surface
Degree 2 del Pezzo Surface

\[ w^2 = ax^4 + by^4 + cz^4 + dx^2y^2 \]
Projection

\[ \pi : X \to \mathbb{P}^2 \]

where \( x : y : z : w \mapsto x : y : z \). Notice that \( \pi \) is surjective. We can find important curves on \( X \) by finding bitangents to \( ax^4 + by^4 + cz^4 + dx^2y^2 = 0 \) in \( \mathbb{P}^2 \).
Projection

\[ \pi : X \rightarrow \mathbb{P}^2 \]

\[ [x : y : z : w] \mapsto [x : y : z] \]

Notice that \( \pi \) is surjective. We can find important curves on \( X \) by finding bitangents to \( ax^4 + by^4 + cz^4 + dx^2y^2 = 0 \) in \( \mathbb{P}^2 \).
Projection

\[ \pi : X \rightarrow \mathbb{P}^2 \]

\[ [x : y : z : w] \mapsto [x : y : z] \]

**Fact**

Notice that \( \pi \) is surjective. We can find important curves on \( X \) by finding bitangents to \( ax^4 + by^4 + cz^4 + dx^2y^2 = 0 \) in \( \mathbb{P}^2 \).
Projection

\[ \pi : X \rightarrow \mathbb{P}^2 \]

\[ \left[ x : y : z : w \right] \mapsto \left[ x : y : z \right] \]

**Fact**

Notice that \( \pi \) is surjective. We can find important curves on \( X \) by finding bitangents to \( ax^4 + by^4 + cz^4 + dx^2y^2 = 0 \) in \( \mathbb{P}^2 \).
Projection

\[ \pi: X \rightarrow \mathbb{P}^2 \]
\[ [x: y: z: w] \mapsto [x: y: z] \]

Fact
Notice that \( \pi \) is surjective. We can find important curves on \( X \) by finding bitangents to \( ax^4 + by^4 + cz^4 + dx^2y^2 = 0 \) in \( \mathbb{P}^2 \).
We now consider lines in $\mathbb{P}^2$. They are defined by a single homogeneous linear equation:

$$Ax + By + Cz = 0.$$ 

If $A \neq 0$, we get:

$$x = \alpha y + \beta z.$$ 

If $A = 0$ and $B \neq 0$, we get:

$$y = \gamma z.$$ 

If $A = B = 0$, we get:

$$z = 0.$$
We now consider lines in $\mathbb{P}^2$. They are defined by a single homogeneous linear equation:

$$Ax + By + Cz = 0.$$
We now consider lines in $\mathbb{P}^2$. They are defined by a single homogeneous linear equation:

$$Ax + By + Cz = 0.$$ 

If $A \neq 0$, we get $x = \alpha y + \beta z$. 
We now consider lines in $\mathbb{P}^2$. They are defined by a single homogeneous linear equation:

$$Ax + By + Cz = 0.$$ 

If $A \neq 0$, we get $x = \alpha y + \beta z$.

If $A = 0$ and $B \neq 0$, we get $y = \gamma z$. 
We now consider lines in $\mathbb{P}^2$. They are defined by a single homogeneous linear equation:

$$Ax + By + Cz = 0.$$ 

If $A \neq 0$, we get $x = \alpha y + \beta z$.

If $A = 0$ and $B \neq 0$, we get $y = \gamma z$.

If $A = B = 0$, we get $z = 0$. 
Bitangents of the form $y = \gamma z$

Recall $f = x^4 + y^4 + z^4 + dx^2 y^2$, and we want bitangents to the curve given by $f = 0$. If $y = \gamma z$ intersects the curve given by $f = 0$ two times, tangentially, we should have $f(x, \gamma z, z) = q(x, z)^2$ where $q$ is a quadratic homogeneous equation in $x$ and $z$ whose roots correspond to the two bitangent intersections. Therefore, we want $x^4 + (\gamma z)^4 + z^4 + dx^2 (\gamma z)^2 = (ax^2 + bxz + cz^2)^2$. 

33
Recall $f = x^4 + y^4 + z^4 + dx^2y^2$, and we want bitangents to the curve given by $f = 0$. 

Bitangents of the form $y = \gamma z$
Recall $f = x^4 + y^4 + z^4 + dx^2y^2$, and we want bitangents to the curve given by $f = 0$.

If $y = \gamma z$ intersects the curve given by $f = 0$ two times, tangentially, we should have $f(x, \gamma z, z) = (q(x, z))^2$ where $q$ is a quadratic homogeneous equation in $x$ and $z$ whose roots correspond to the two bitangent intersections.
Recall $f = x^4 + y^4 + z^4 + dx^2y^2$, and we want bitangents to the curve given by $f = 0$.

If $y = \gamma z$ intersects the curve given by $f = 0$ two times, tangentially, we should have $f(x, \gamma z, z) = (q(x, z))^2$ where $q$ is a quadratic homogeneous equation in $x$ and $z$ whose roots correspond to the two bitangent intersections.

Therefore, we want

$$x^4 + (\gamma z)^4 + z^4 + dx^2(\gamma z)^2 = (ax^2 + bzx + cz^2)^2.$$
Bitangents of the form $y = \gamma z$ (Cont.)
Bitangents of the form $y = \gamma z$ (Cont.)

\[
x^4 + (\gamma z)^4 + z^4 + dx^2(\gamma z)^2 = (ax^2 + bxz + cz^2)^2
\]
\[
x^4 + d\gamma^2 x^2 y^2 + (\gamma^4 + 1)z^4 = a^2 x^4 + 2abx^3 z + (2ac + b)x^2 z^2
\]
\[
+ 2bcxz^2 + c^2 z^2
\]
Bitangents of the form $y = \gamma z$ (Cont.)

\[
x^4 + (\gamma z)^4 + z^4 + dx^2(\gamma z)^2 = (ax^2 + bxz + cz^2)^2
\]
\[
x^4 + d\gamma^2 x^2 y^2 + (\gamma^4 + 1)z^4 = a^2 x^4 + 2abx^3 z + (2ac + b)x^2 z^2 + 2bcxz^2 + c^2 z^2
\]

Matching up the coefficients, we get

\[
1 = a^2 \\
0 = 2ab \\
d\gamma^2 = 2ac + b \\
0 = 2bc \\
\gamma^4 + 1 = c^2
\]
Bitangents of the form $y = \gamma z$ (Cont.)

\[
x^4 + (\gamma z)^4 + z^4 + d x^2 (\gamma z)^2 = (a x^2 + b x z + c z^2)^2
\]

\[
x^4 + d \gamma^2 x^2 y^2 + (\gamma^4 + 1) z^4 = a^2 x^4 + 2 a b x^3 z + (2 a c + b) x^2 z^2 + 2 b c x z^2 + c^2 z^2
\]

Matching up the coefficients, we get

\[
\begin{align*}
1 &= a^2 & a &= \pm 1 \\
0 &= 2 a b & b &= 0 \\
d \gamma^2 &= 2 a c + b & \Rightarrow c &= \pm \frac{d}{\sqrt{d^2 - 4}} \\
0 &= 2 b c & \gamma &= \pm \left(\frac{4}{d^2 - 4}\right)^{1/4}
\end{align*}
\]
Now we have $y = \gamma z$ and $f(x, \gamma z, z) = (ax^2 + bxz + cz^2)^2$. What are the curves upstairs?

$y = \gamma z, w = ax^2 + bxz + cz^2$
Now we have $y = \gamma z$ and $f(x, \gamma z, z) = (ax^2 + bxz + cz^2)^2$. What are the curves upstairs?
Now we have $y = \gamma z$ and $f(x, \gamma z, z) = (ax^2 + bzx + cz^2)^2$. What are the curves upstairs?

\[
\begin{align*}
y &= \gamma z \\
w &= ax^2 + bzx + cz^2
\end{align*}
\]
Now we have $y = \gamma z$ and $f(x, \gamma z, z) = (ax^2 + bxz + cz^2)^2$. What are the curves upstairs?

\[
\begin{align*}
y &= \gamma z \\
w &= ax^2 + bxz + cz^2
\end{align*}
\]
Thanks!