Arithmetic of Markoff surfaces

Fei XU

School of Mathematical Sciences

Capital Normal University

July 9, 2023 1 / 34

• Let X be a smooth and projective curve over \mathbb{Q} .

Theorem (Fermat): When the genus of X is 0, then

$$X(\mathbb{Q}) = \emptyset$$
 or $|X(\mathbb{Q})| = \infty$

Theorem (Mordell): When the genus of X is 1, then

 $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is a finitely generated abelian group

Theorem (Faltings-Vojta-Lawrence-Venkatesh): When the genus of X is bigger than 1, then

 $|X(\mathbb{Q})| < \infty.$

- **4 ∃ ≻** 4

• Let X be a smooth and projective curve over \mathbb{Q} .

Theorem (Fermat): When the genus of X is 0, then

$$X(\mathbb{Q}) = \emptyset$$
 or $|X(\mathbb{Q})| = \infty$

Theorem (Mordell): When the genus of X is 1, then

 $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is a finitely generated abelian group

Theorem (Faltings-Vojta-Lawrence-Venkatesh): When the genus of X is bigger than 1, then

 $|X(\mathbb{Q})| < \infty.$

.

• Let X be a smooth and projective curve over \mathbb{Q} .

Theorem (Fermat): When the genus of X is 0, then

$$X(\mathbb{Q}) = \emptyset$$
 or $|X(\mathbb{Q})| = \infty$

Theorem (Mordell): When the genus of X is 1, then

 $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is a finitely generated abelian group

Theorem (Faltings-Vojta-Lawrence-Venkatesh): When the genus of X is bigger than 1, then

 $|X(\mathbb{Q})| < \infty.$

(日) (周) (三) (三)

• Let X be a smooth and projective curve over \mathbb{Q} .

Theorem (Fermat): When the genus of X is 0, then

$$X(\mathbb{Q}) = \emptyset$$
 or $|X(\mathbb{Q})| = \infty$

Theorem (Mordell): When the genus of X is 1, then

 $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is a finitely generated abelian group

Theorem (Faltings-Vojta-Lawrence-Venkatesh): When the genus of X is bigger than 1, then

 $|X(\mathbb{Q})| < \infty.$

イロト イヨト イヨト

- For higher dimensional smooth and projective variety X over \mathbb{Q} , one also expect that $|X(\mathbb{Q})|$ is close related to the geometry of $\overline{X} = X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$.
- Let $\Omega_{\overline{X}}$ be the sheaf of differentials of \overline{X} and

$$\omega_{\overline{X}} = \bigwedge^{\dim(X)} \Omega_{\overline{X}}$$

be the canonical divisor of \overline{X}

Definition

1) X is Fano if $\omega_{\overline{X}}^{-1}$ is ample (g=0).

- 2) X is Calabi-Yau if $\omega_{\overline{X}}$ is trivial (g = 1).
- 3) X is of general type if $\omega_{\overline{X}}$ is ample (g > 1).

- For higher dimensional smooth and projective variety X over \mathbb{Q} , one also expect that $|X(\mathbb{Q})|$ is close related to the geometry of $\overline{X} = X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$.
- Let $\Omega_{\overline{X}}$ be the sheaf of differentials of \overline{X} and

$$\omega_{\overline{X}} = \bigwedge^{\dim(X)} \Omega_{\overline{X}}$$

be the canonical divisor of \overline{X}

Definition

1) X is Fano if $\omega_{\overline{X}}^{-1}$ is ample (g=0).

- 2) X is Calabi-Yau if $\omega_{\overline{X}}$ is trivial (g = 1).
- 3) X is of general type if $\omega_{\overline{X}}$ is ample (g > 1).

- For higher dimensional smooth and projective variety X over \mathbb{Q} , one also expect that $|X(\mathbb{Q})|$ is close related to the geometry of $\overline{X} = X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$.
- Let $\Omega_{\overline{X}}$ be the sheaf of differentials of \overline{X} and

$$\omega_{\overline{X}} = \bigwedge^{\dim(X)} \Omega_{\overline{X}}$$

be the canonical divisor of \overline{X}

Definition.

1) X is Fano if $\omega_{\overline{X}}^{-1}$ is ample (g=0).

- 2) X is Calabi-Yau if $\omega_{\overline{X}}$ is trivial (g = 1).
- 3) X is of general type if $\omega_{\overline{X}}$ is ample (g > 1).

- For higher dimensional smooth and projective variety X over \mathbb{Q} , one also expect that $|X(\mathbb{Q})|$ is close related to the geometry of $\overline{X} = X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$.
- Let $\Omega_{\overline{X}}$ be the sheaf of differentials of \overline{X} and

$$\omega_{\overline{X}} = \bigwedge^{\dim(X)} \Omega_{\overline{X}}$$

be the canonical divisor of \overline{X}

Definition.

- 1) X is Fano if $\omega_{\overline{X}}^{-1}$ is ample (g=0).
- 2) X is Calabi-Yau if $\omega_{\overline{X}}$ is trivial (g = 1).

3) X is of general type if $\omega_{\overline{X}}$ is ample (g > 1).

- For higher dimensional smooth and projective variety X over \mathbb{Q} , one also expect that $|X(\mathbb{Q})|$ is close related to the geometry of $\overline{X} = X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$.
- Let $\Omega_{\overline{X}}$ be the sheaf of differentials of \overline{X} and

$$\omega_{\overline{X}} = \bigwedge^{\dim(X)} \Omega_{\overline{X}}$$

be the canonical divisor of \overline{X}

Definition.

- 1) X is Fano if $\omega_{\overline{X}}^{-1}$ is ample (g=0).
- 2) X is Calabi-Yau if $\omega_{\overline{X}}$ is trivial (g = 1).
- 3) X is of general type if $\omega_{\overline{X}}$ is ample (g > 1).

Conjecture (Colliot-Thelene). If X is Fano, then either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

Conjecture (Bombieri-Lang). If X is of general type, then $X(\mathbb{Q})$ is not Zariski dense in X.

- Case of Calabi-Yau varieties.
- For abelian varieties, there is a generalization of BSD conjecture.

• There are two classes of 2-dimensional Calabi-Yau varieties: abelian surfaces and K3 surfaces which are simply connected.

Conjecture (Colliot-Thelene). If X is Fano, then either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

Conjecture (Bombieri-Lang). If X is of general type, then $X(\mathbb{Q})$ is not Zariski dense in X.

• Case of Calabi-Yau varieties.

• For abelian varieties, there is a generalization of BSD conjecture.

• There are two classes of 2-dimensional Calabi-Yau varieties: abelian surfaces and K3 surfaces which are simply connected.

Conjecture (Colliot-Thelene). If X is Fano, then either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

Conjecture (Bombieri-Lang). If X is of general type, then $X(\mathbb{Q})$ is not Zariski dense in X.

• Case of Calabi-Yau varieties.

• For abelian varieties, there is a generalization of BSD conjecture.

• There are two classes of 2-dimensional Calabi-Yau varieties: abelian surfaces and K3 surfaces which are simply connected.

Conjecture (Colliot-Thelene). If X is Fano, then either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

Conjecture (Bombieri-Lang). If X is of general type, then $X(\mathbb{Q})$ is not Zariski dense in X.

- Case of Calabi-Yau varieties.
- For abelian varieties, there is a generalization of BSD conjecture.

• There are two classes of 2-dimensional Calabi-Yau varieties: abelian surfaces and K3 surfaces which are simply connected.

• For a K3 surface X, it is conjectured that either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

- 4 同 6 4 三 6 4

Conjecture (Colliot-Thelene). If X is Fano, then either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

Conjecture (Bombieri-Lang). If X is of general type, then $X(\mathbb{Q})$ is not Zariski dense in X.

- Case of Calabi-Yau varieties.
- For abelian varieties, there is a generalization of BSD conjecture.
- There are two classes of 2-dimensional Calabi-Yau varieties: abelian surfaces and K3 surfaces which are simply connected.

• For a K3 surface X, it is conjectured that either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

Conjecture (Colliot-Thelene). If X is Fano, then either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

Conjecture (Bombieri-Lang). If X is of general type, then $X(\mathbb{Q})$ is not Zariski dense in X.

- Case of Calabi-Yau varieties.
- For abelian varieties, there is a generalization of BSD conjecture.
- There are two classes of 2-dimensional Calabi-Yau varieties: abelian surfaces and K3 surfaces which are simply connected.

Example. Euler generalized the Fermat equation and conjectured

$$X: \quad x_1^n + x_2^n + \dots + x_{n-1}^n = x_n^n$$

has no solution of positive integers for n > 2.

• X is a Calabi-Yau variety.

• Lander and Parkin (1966) found a counterexample

 $27^5 + 84^5 + 110^5 + 133^5 = 144^5$

by a direct computer searching.

Example. Euler generalized the Fermat equation and conjectured

$$X: \quad x_1^n + x_2^n + \dots + x_{n-1}^n = x_n^n$$

has no solution of positive integers for n > 2.

• X is a Calabi-Yau variety.

• Lander and Parkin (1966) found a counterexample

 $27^5 + 84^5 + 110^5 + 133^5 = 144^5$

by a direct computer searching.

Example. Euler generalized the Fermat equation and conjectured

$$X: \quad x_1^n + x_2^n + \dots + x_{n-1}^n = x_n^n$$

has no solution of positive integers for n > 2.

- X is a Calabi-Yau variety.
- Lander and Parkin (1966) found a counterexample

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

by a direct computer searching.

Example. Euler generalized the Fermat equation and conjectured

$$X: \quad x_1^n + x_2^n + \dots + x_{n-1}^n = x_n^n$$

has no solution of positive integers for n > 2.

- X is a Calabi-Yau variety.
- Lander and Parkin (1966) found a counterexample

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

by a direct computer searching.

• Elkies (1988) provided a counterexample for n = 4

```
2682440^4 + 15365639^4 + 18796760^4 = 20615673^4
```

and $X(\mathbb{Q})$ is Zariski dense in X.

Sketch of Elkies' idea: There is a morphism ψ

$$Y: \begin{cases} (u^2+2)(\frac{r-s}{2})^2 = -(3u^2-8u+6)(\frac{r+s}{2})^2 - 2(u^2-2)(\frac{r+s}{2}) - 2u\\ \pm (u^2+2)t^2 = 4(u^2-2)(\frac{r+s}{2})^2 + 8u(\frac{r+s}{2}) + (2-u^2) \end{cases}$$

$$\longrightarrow Z: \{r^4 + s^4 + t^4 = 1\}$$

based on the work of Demjanenko (1974 in Russian).

• Elkies (1988) provided a counterexample for n = 4

```
2682440^4 + 15365639^4 + 18796760^4 = 20615673^4
```

and $X(\mathbb{Q})$ is Zariski dense in X.

Sketch of Elkies' idea: There is a morphism ψ

$$Y: \begin{cases} (u^2+2)(\frac{r-s}{2})^2 = -(3u^2-8u+6)(\frac{r+s}{2})^2 - 2(u^2-2)(\frac{r+s}{2}) - 2u\\ \pm (u^2+2)t^2 = 4(u^2-2)(\frac{r+s}{2})^2 + 8u(\frac{r+s}{2}) + (2-u^2)\\ \longrightarrow Z: \{r^4+s^4+t^4=1\} \end{cases}$$

based on the work of Demjanenko (1974 in Russian).

• One can partially compactify Y to Y^c with the fibration $Y^c \xrightarrow{\phi} \mathbb{P}^1$ by sending $(r, s, t, u) \mapsto [u, 1]$. Moreover, the morphism ψ can be extended to

$$\psi: Y^c \to Z \text{ and } \psi(Y^c(\mathbb{Q})) = Z(\mathbb{Q}).$$

• Each fiber of ϕ over $\mathbb{P}^1(\mathbb{Q})$ is an intersection of two conics over \mathbb{Q} . By using the Hasse principle for conics with several testing, one can choose $\phi^{-1}([16, -5])$ which is

$$153y^2 = -779x^2 - 206x + 80, \quad 153t^2 = 412x^2 - 320x - 103$$

where $x = \frac{r+s}{2}$ and $y = \frac{r-s}{2}$.

• One can partially compactify Y to Y^c with the fibration $Y^c \xrightarrow{\phi} \mathbb{P}^1$ by sending $(r, s, t, u) \mapsto [u, 1]$. Moreover, the morphism ψ can be extended to

$$\psi: Y^c \to Z$$
 and $\psi(Y^c(\mathbb{Q})) = Z(\mathbb{Q}).$

• Each fiber of ϕ over $\mathbb{P}^1(\mathbb{Q})$ is an intersection of two conics over \mathbb{Q} . By using the Hasse principle for conics with several testing, one can choose $\phi^{-1}([16,-5])$ which is

$$153y^2 = -779x^2 - 206x + 80, \quad 153t^2 = 412x^2 - 320x - 103$$

where $x = \frac{r+s}{2}$ and $y = \frac{r-s}{2}$.

• All rational points of first conic can parametrized by

$$x = \frac{51k^2 - 34k - 5221}{14(17k^2 + 779)}, \quad y = \frac{17k^2 + 7558k - 779}{42(17k^2 + 779)}$$

by Fermat's method. Substituting this x into the second conic and using the new coordinates $\xi = (k+2)/7$ and $\eta = 3(17k^2 + 779)t/14$, one has

$$\eta^2 = -31790\xi^4 + 36941\xi^3 - 56158\xi^2 + 28849\xi + 22030.$$

• By computer searching, one obtains

$$(\xi,\eta) = \left(-\frac{31}{467}, \frac{30731278}{467^2}\right)$$

• All rational points of first conic can parametrized by

$$x = \frac{51k^2 - 34k - 5221}{14(17k^2 + 779)}, \quad y = \frac{17k^2 + 7558k - 779}{42(17k^2 + 779)}$$

by Fermat's method. Substituting this x into the second conic and using the new coordinates $\xi = (k+2)/7$ and $\eta = 3(17k^2 + 779)t/14$, one has

$$\eta^2 = -31790\xi^4 + 36941\xi^3 - 56158\xi^2 + 28849\xi + 22030.$$

• By computer searching, one obtains

$$(\xi,\eta) = (-\frac{31}{467}, \frac{30731278}{467^2})$$

Definition. Let X be a smooth and geometrically integral variety over \mathbb{Q} . Then X is called a log K3 surface if X satisfies

- 1) \overline{X} is simply connected.
- 2) There is a smooth compactification $X \hookrightarrow X^c$ over \mathbb{Q} such that $D = X^c \setminus X$ is a simple normal crossing divisor.
- 3) $[D] + \omega_{X^c} = 0$ in $\operatorname{Pic}(X^c)$.
- A log K3 surface is a generalization of K3 surface.

Conjecture (Vojta). If X be a log K3 surface over \mathbb{Q} and \mathfrak{X} be an integral model of X over \mathbb{Z} , then there is a number field F such that $\mathfrak{X}(\mathcal{O}_F)$ is Zariski dense in \mathfrak{X} where \mathcal{O}_F is the ring of integers of F.

Definition. Let X be a smooth and geometrically integral variety over \mathbb{Q} . Then X is called a log K3 surface if X satisfies

1) \overline{X} is simply connected.

2) There is a smooth compactification $X \hookrightarrow X^c$ over \mathbb{Q} such that $D = X^c \setminus X$ is a simple normal crossing divisor.

3) $[D] + \omega_{X^c} = 0$ in $\operatorname{Pic}(X^c)$.

• A log K3 surface is a generalization of K3 surface.

Conjecture (Vojta). If X be a log K3 surface over \mathbb{Q} and \mathfrak{X} be an integral model of X over \mathbb{Z} , then there is a number field F such that $\mathfrak{X}(\mathcal{O}_F)$ is Zariski dense in \mathfrak{X} where \mathcal{O}_F is the ring of integers of F.

Definition. Let X be a smooth and geometrically integral variety over \mathbb{Q} . Then X is called a log K3 surface if X satisfies

- 1) \overline{X} is simply connected.
- 2) There is a smooth compactification $X \hookrightarrow X^c$ over \mathbb{Q} such that $D = X^c \setminus X$ is a simple normal crossing divisor.
- 3) $[D] + \omega_{X^c} = 0$ in $\operatorname{Pic}(X^c)$.
- A log K3 surface is a generalization of K3 surface.

Conjecture (Vojta). If X be a log K3 surface over \mathbb{Q} and \mathfrak{X} be an integral model of X over \mathbb{Z} , then there is a number field F such that $\mathfrak{X}(\mathcal{O}_F)$ is Zariski dense in \mathfrak{X} where \mathcal{O}_F is the ring of integers of F.

< ロ > < 同 > < 三 > < 三

Definition. Let X be a smooth and geometrically integral variety over \mathbb{Q} . Then X is called a log K3 surface if X satisfies

- 1) \overline{X} is simply connected.
- 2) There is a smooth compactification $X \hookrightarrow X^c$ over \mathbb{Q} such that $D = X^c \setminus X$ is a simple normal crossing divisor.
- 3) $[D] + \omega_{X^c} = 0$ in $\operatorname{Pic}(X^c)$.

• A log K3 surface is a generalization of K3 surface.

Conjecture (Vojta). If X be a log K3 surface over \mathbb{Q} and \mathfrak{X} be an integral model of X over \mathbb{Z} , then there is a number field F such that $\mathfrak{X}(\mathcal{O}_F)$ is Zariski dense in \mathfrak{X} where \mathcal{O}_F is the ring of integers of F.

< ロ > < 同 > < 三 > < 三

Definition. Let X be a smooth and geometrically integral variety over \mathbb{Q} . Then X is called a log K3 surface if X satisfies

- 1) \overline{X} is simply connected.
- 2) There is a smooth compactification $X \hookrightarrow X^c$ over \mathbb{Q} such that $D = X^c \setminus X$ is a simple normal crossing divisor.
- 3) $[D] + \omega_{X^c} = 0$ in $Pic(X^c)$.
- A log K3 surface is a generalization of K3 surface.

Conjecture (Vojta). If X be a log K3 surface over \mathbb{Q} and \mathfrak{X} be an integral model of X over \mathbb{Z} , then there is a number field F such that $\mathfrak{X}(\mathcal{O}_F)$ is Zariski dense in \mathfrak{X} where \mathcal{O}_F is the ring of integers of F.

イロト イヨト イヨト イヨト

Definition. Let X be a smooth and geometrically integral variety over \mathbb{Q} . Then X is called a log K3 surface if X satisfies

1) \overline{X} is simply connected.

2) There is a smooth compactification $X \hookrightarrow X^c$ over \mathbb{Q} such that $D = X^c \setminus X$ is a simple normal crossing divisor.

3) $[D] + \omega_{X^c} = 0$ in $\operatorname{Pic}(X^c)$.

• A log K3 surface is a generalization of K3 surface.

Conjecture (Vojta). If X be a log K3 surface over \mathbb{Q} and \mathfrak{X} be an integral model of X over \mathbb{Z} , then there is a number field F such that $\mathfrak{X}(\mathcal{O}_F)$ is Zariski dense in \mathfrak{X} where \mathcal{O}_F is the ring of integers of F.

(日) (周) (三) (三)

• Let X be a variety over \mathbb{Q} and $\operatorname{Br}(X) = \operatorname{H}^2_{\operatorname{et}}(X, \mathbb{G}_m)$ and $\operatorname{Br}_1(X) = \ker(\operatorname{Br}(X) \to \operatorname{Br}(\overline{X})).$

• Let $\mathbf{A}_{\mathbb{Q}}$ be the adeles and $\mathbf{A}_{\mathbb{Q}}^{f}$ be the finite adeles of \mathbb{Q} . Write

$$X(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}(X)} = \{(x_p) \in X(\mathbf{A}_{\mathbb{Q}}) : \sum_{p \le \infty} inv_p(\xi(x_p)) = 0; \quad \forall \ \xi \in \mathrm{Br}(X)\}$$

where

$$inv_p: \operatorname{Br}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is the invariant map from the local class field theory for $p\leq\infty.$

• The class field theory implies

$$X(\mathbb{Q}) \subseteq X(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}(X)} \subseteq X(\mathbf{A}_{\mathbb{Q}}).$$

- Let X be a variety over \mathbb{Q} and $Br(X) = H^2_{et}(X, \mathbb{G}_m)$ and $Br_1(X) = \ker(Br(X) \to Br(\overline{X})).$
- Let $\mathbf{A}_{\mathbb{Q}}$ be the adeles and $\mathbf{A}_{\mathbb{Q}}^{\mathit{f}}$ be the finite adeles of $\mathbb{Q}.$ Write

$$X(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}(X)} = \{(x_p) \in X(\mathbf{A}_{\mathbb{Q}}) : \sum_{p \le \infty} inv_p(\xi(x_p)) = 0; \quad \forall \ \xi \in \mathrm{Br}(X)\}$$

where

$$inv_p: \operatorname{Br}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is the invariant map from the local class field theory for $p \leq \infty$.

• The class field theory implies

 $X(\mathbb{Q}) \subseteq X(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}(X)} \subseteq X(\mathbf{A}_{\mathbb{Q}}).$

- Let X be a variety over \mathbb{Q} and $Br(X) = H^2_{et}(X, \mathbb{G}_m)$ and $Br_1(X) = \ker(Br(X) \to Br(\overline{X})).$
- Let $\mathbf{A}_{\mathbb{Q}}$ be the adeles and $\mathbf{A}_{\mathbb{Q}}^f$ be the finite adeles of $\mathbb{Q}.$ Write

$$X(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}(X)} = \{(x_p) \in X(\mathbf{A}_{\mathbb{Q}}) : \sum_{p \le \infty} inv_p(\xi(x_p)) = 0; \quad \forall \ \xi \in \mathrm{Br}(X)\}$$

where

$$inv_p: \operatorname{Br}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is the invariant map from the local class field theory for $p \leq \infty$.

• The class field theory implies

$$X(\mathbb{Q}) \subseteq X(\mathbf{A}_{\mathbb{Q}})^{\operatorname{Br}(X)} \subseteq X(\mathbf{A}_{\mathbb{Q}}).$$

Definition. We say X satisfies strong approximation with the Brauer-Manin obstruction if

$$X(\mathbb{Q})$$
 is dense in $pr^f(X(\mathbf{A}_{\mathbb{Q}})^{\operatorname{Br}(X)})$

where

$$pr^f: X(\mathbf{A}_{\mathbb{Q}}) \to X(\mathbf{A}_{\mathbb{Q}}^f)$$

is the projection map.

Conjecture (Skorobogatov). If X is a K3 surface, then X satisfies strong approximation with the Brauer-Manin obstruction.

Proposition. Skorobogatov's conjecture implies that either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.
II. Brauer-Manin obstruction

Definition. We say X satisfies strong approximation with the Brauer-Manin obstruction if

$$X(\mathbb{Q})$$
 is dense in $pr^f(X(\mathbf{A}_{\mathbb{Q}})^{\operatorname{Br}(X)})$

where

$$pr^f: X(\mathbf{A}_{\mathbb{Q}}) \to X(\mathbf{A}_{\mathbb{Q}}^f)$$

is the projection map.

Conjecture (Skorobogatov). If X is a K3 surface, then X satisfies strong approximation with the Brauer-Manin obstruction.

Proposition. Skorobogatov's conjecture implies that either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

II. Brauer-Manin obstruction

Definition. We say X satisfies strong approximation with the Brauer-Manin obstruction if

$$X(\mathbb{Q})$$
 is dense in $pr^f(X(\mathbf{A}_{\mathbb{Q}})^{\operatorname{Br}(X)})$

where

$$pr^f: X(\mathbf{A}_{\mathbb{Q}}) \to X(\mathbf{A}_{\mathbb{Q}}^f)$$

is the projection map.

Conjecture (Skorobogatov). If X is a K3 surface, then X satisfies strong approximation with the Brauer-Manin obstruction.

Proposition. Skorobogatov's conjecture implies that either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is Zariski dense in X.

Let

$$\mathfrak{U}_m: \quad x^2 + y^2 + z^2 - xyz = m$$

where m is a fixed integer. Then $U_m = \mathfrak{U}_m \times_{\mathbb{Z}} \mathbb{Q}$ is called a Markoff surface over \mathbb{Q} .

• When $m \neq 0$ and 4, then U_m is smooth.

• A smooth compactification X_m of U_m is

$$t(x^2 + y^2 + z^2) - xyz = mt^3$$

a cubic surfaces in \mathbb{P}^3 for $m \neq 0$ and 4.

Let

$$\mathfrak{U}_m: \quad x^2 + y^2 + z^2 - xyz = m$$

where m is a fixed integer. Then $U_m = \mathfrak{U}_m \times_{\mathbb{Z}} \mathbb{Q}$ is called a Markoff surface over \mathbb{Q} .

• When $m \neq 0$ and 4, then U_m is smooth.

• A smooth compactification X_m of U_m is

$$t(x^2 + y^2 + z^2) - xyz = mt^3$$

a cubic surfaces in \mathbb{P}^3 for $m \neq 0$ and 4.

Let

$$\mathfrak{U}_m: \quad x^2 + y^2 + z^2 - xyz = m$$

where m is a fixed integer. Then $U_m = \mathfrak{U}_m \times_{\mathbb{Z}} \mathbb{Q}$ is called a Markoff surface over \mathbb{Q} .

- When $m \neq 0$ and 4, then U_m is smooth.
- A smooth compactification X_m of U_m is

$$t(x^2 + y^2 + z^2) - xyz = mt^3$$

a cubic surfaces in \mathbb{P}^3 for $m \neq 0$ and 4.

• Let $\overline{X}_m \xrightarrow{\pi} \mathbb{P}^2$ be a blowing down the following six lines in \overline{X}_m

$$l_{1}: x = 2t, y - z = (\sqrt{m-4})t$$

$$l_{2}: y = 2t, z - x = (\sqrt{m-4})t$$

$$l_{3}: z = 2t, x - y = (\sqrt{m-4})t$$

$$l_{4}: x = (\sqrt{m})t, y = \frac{1}{2}(\sqrt{m} + \sqrt{m-4})z$$

$$l_{5}: y = (\sqrt{m})t, z = \frac{1}{2}(\sqrt{m} + \sqrt{m-4})x$$

$$l_{6}: z = (\sqrt{m})t, x = \frac{1}{2}(\sqrt{m} + \sqrt{m-4})y$$

and L is the inverse image of a line in \mathbb{P}^2 . Then $\operatorname{Pic}(\overline{X}_m) \cong \mathbb{Z}^7$ is generated by L, l_1, \cdots, l_6 such that

$$\langle L,L\rangle=1, \quad \langle L,l_i\rangle=0 \quad \text{and} \quad \langle l_i,l_i\rangle=-1$$

for $1 \leq i \leq 6$ and $\langle l_i, l_j \rangle = 0$ for $i \neq j$.

 \bullet The canonical divisor $\omega_{\overline{X}_m}$ of \overline{X}_m satisfies

$$\omega_{\overline{X}_m} = -3L + \sum_{i=1}^6 l_i \text{ in } \operatorname{Pic}(\overline{X}_m).$$

• The divisor $D_m = X_m \setminus U_m$ consists of three lines

$$L_1: \{t = x = 0\}, \ L_2: \{t = y = 0\}, \ L_3: \{t = z = 0\}$$

and

$$L_1 = L - l_1 - l_4$$
, $L_2 = L - l_2 - l_5$, $L_3 = L - l_3 - l_6$ in $\operatorname{Pic}(\overline{X}_m)$

• \overline{U}_m is simply connected.

 \bullet The canonical divisor $\omega_{\overline{X}_m}$ of \overline{X}_m satisfies

$$\omega_{\overline{X}_m} = -3L + \sum_{i=1}^6 l_i \text{ in } \operatorname{Pic}(\overline{X}_m).$$

• The divisor $D_m = X_m \setminus U_m$ consists of three lines

$$L_1: \{t = x = 0\}, \ L_2: \{t = y = 0\}, \ L_3: \{t = z = 0\}$$

and

$$L_1 = L - l_1 - l_4$$
, $L_2 = L - l_2 - l_5$, $L_3 = L - l_3 - l_6$ in $\operatorname{Pic}(\overline{X}_m)$

• \overline{U}_m is simply connected.

 \bullet The canonical divisor $\omega_{\overline{X}_m}$ of \overline{X}_m satisfies

$$\omega_{\overline{X}_m} = -3L + \sum_{i=1}^6 l_i \text{ in } \operatorname{Pic}(\overline{X}_m).$$

• The divisor $D_m = X_m \setminus U_m$ consists of three lines

$$L_1: \{t = x = 0\}, \ L_2: \{t = y = 0\}, \ L_3: \{t = z = 0\}$$

and

$$L_1 = L - l_1 - l_4$$
, $L_2 = L - l_2 - l_5$, $L_3 = L - l_3 - l_6$ in $\operatorname{Pic}(\overline{X}_m)$

• \overline{U}_m is simply connected.

 \bullet The canonical divisor $\omega_{\overline{X}_m}$ of \overline{X}_m satisfies

$$\omega_{\overline{X}_m} = -3L + \sum_{i=1}^6 l_i \text{ in } \operatorname{Pic}(\overline{X}_m).$$

• The divisor $D_m = X_m \setminus U_m$ consists of three lines

$$L_1: \{t = x = 0\}, \ L_2: \{t = y = 0\}, \ L_3: \{t = z = 0\}$$

and

$$L_1 = L - l_1 - l_4$$
, $L_2 = L - l_2 - l_5$, $L_3 = L - l_3 - l_6$ in $\operatorname{Pic}(\overline{X}_m)$

• \overline{U}_m is simply connected.

 \bullet The canonical divisor $\omega_{\overline{X}_m}$ of \overline{X}_m satisfies

$$\omega_{\overline{X}_m} = -3L + \sum_{i=1}^6 l_i \text{ in } \operatorname{Pic}(\overline{X}_m).$$

• The divisor $D_m = X_m \setminus U_m$ consists of three lines

$$L_1: \{t = x = 0\}, \ L_2: \{t = y = 0\}, \ L_3: \{t = z = 0\}$$

and

$$L_1 = L - l_1 - l_4$$
, $L_2 = L - l_2 - l_5$, $L_3 = L - l_3 - l_6$ in $\operatorname{Pic}(\overline{X}_m)$

• \overline{U}_m is simply connected.

• Basic question: For which m, $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$?

Proposition.

$$\prod_{p}\mathfrak{U}_{m}(\mathbb{Z}_{p})=\emptyset$$

if and only if $m \equiv 3 \mod 4$ or $m \equiv \pm 3 \mod 9$.

Proposition. \mathfrak{U}_m admits an automorphism group Γ generated by (a) The Vieta involution: $(x, y, z) \mapsto (yz - x, y, z)$; (b) The sign change: $(x, y, z) \mapsto (-x, -y, z)$;

(c) The permutations of x, y, z.

• Basic question: For which m, $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$?

Proposition.

$$\prod_p \mathfrak{U}_m(\mathbb{Z}_p) = \emptyset$$

if and only if $m \equiv 3 \mod 4$ or $m \equiv \pm 3 \mod 9$.

Proposition. \mathfrak{U}_m admits an automorphism group Γ generated by

- (a) The Vieta involution: $(x, y, z) \mapsto (yz x, y, z)$;
- (b) The sign change: $(x, y, z) \mapsto (-x, -y, z)$;

(c) The permutations of x, y, z.

• Basic question: For which m, $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$?

Proposition.

$$\prod_p \mathfrak{U}_m(\mathbb{Z}_p) = \emptyset$$

if and only if $m \equiv 3 \mod 4$ or $m \equiv \pm 3 \mod 9$.

Proposition. \mathfrak{U}_m admits an automorphism group Γ generated by

- (a) The Vieta involution: $(x, y, z) \mapsto (yz x, y, z);$
- (b) The sign change: $(x, y, z) \mapsto (-x, -y, z)$;

(c) The permutations of x, y, z.

• Basic question: For which m, $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$?

Proposition.

$$\prod_p \mathfrak{U}_m(\mathbb{Z}_p) = \emptyset$$

if and only if $m \equiv 3 \mod 4$ or $m \equiv \pm 3 \mod 9$.

Proposition. \mathfrak{U}_m admits an automorphism group Γ generated by (a) The Vieta involution: $(x, y, z) \mapsto (yz - x, y, z)$; (b) The sign change: $(x, y, z) \mapsto (-x, -y, z)$;

(c) The permutations of x, y, z.

• Basic question: For which m, $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$?

Proposition.

$$\prod_p \mathfrak{U}_m(\mathbb{Z}_p) = \emptyset$$

if and only if $m \equiv 3 \mod 4$ or $m \equiv \pm 3 \mod 9$.

Proposition. \mathfrak{U}_m admits an automorphism group Γ generated by

- (a) The Vieta involution: $(x, y, z) \mapsto (yz x, y, z)$;
- (b) The sign change: $(x, y, z) \mapsto (-x, -y, z)$;

(c) The permutations of x, y, z.

• Basic question: For which m, $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$?

Proposition.

$$\prod_p \mathfrak{U}_m(\mathbb{Z}_p) = \emptyset$$

if and only if $m \equiv 3 \mod 4$ or $m \equiv \pm 3 \mod 9$.

Proposition. \mathfrak{U}_m admits an automorphism group Γ generated by

- (a) The Vieta involution: $(x, y, z) \mapsto (yz x, y, z)$;
- (b) The sign change: $(x, y, z) \mapsto (-x, -y, z)$;
- (c) The permutations of x, y, z.
- Γ acts on $\mathfrak{U}_m(\mathbb{Z})$ naturally.

• Basic question: For which m, $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$?

Proposition.

$$\prod_p \mathfrak{U}_m(\mathbb{Z}_p) = \emptyset$$

if and only if $m \equiv 3 \mod 4$ or $m \equiv \pm 3 \mod 9$.

Proposition. \mathfrak{U}_m admits an automorphism group Γ generated by

- (a) The Vieta involution: $(x, y, z) \mapsto (yz x, y, z);$
- (b) The sign change: $(x, y, z) \mapsto (-x, -y, z)$;
- (c) The permutations of x, y, z.
- Γ acts on $\mathfrak{U}_m(\mathbb{Z})$ naturally.

Theorem (Markoff, Hurwitz, Mordell, ..., Ghosh-Sarnak)

When m < 0, then each orbit of Γ contains a unique integral solution (x_0, y_0, z_0) such that

$$3 \le x_0 \le y_0 \le z_0 \le \frac{1}{2}x_0y_0$$

and the number of Γ -orbits is finite.

When m > 0, then each orbit of Γ contains an integral solutions (x_0, y_0, z_0) such that

$$3 \le x_0 \le y_0 \le -z_0$$
 or $x_0 = 0, 1, 2.$

Moreover, if m is not form of

(i)
$$u^2 + v^2$$
 ($x_0 = 0$); (ii) $u^2 - uv + v^2 + 1$ ($x_0 = 1$); (iii) $u^2 + 4$ ($x_0 = 2$),

then the integral solution is unique and the number of Forbits is finite.

Theorem (Markoff, Hurwitz, Mordell, ..., Ghosh-Sarnak)

When m < 0, then each orbit of Γ contains a unique integral solution (x_0, y_0, z_0) such that

$$3 \le x_0 \le y_0 \le z_0 \le \frac{1}{2}x_0y_0$$

and the number of Γ -orbits is finite.

When m > 0, then each orbit of Γ contains an integral solutions (x_0, y_0, z_0) such that

$$3 \le x_0 \le y_0 \le -z_0$$
 or $x_0 = 0, 1, 2.$

Moreover, if m is not form of

(i)
$$u^2 + v^2$$
 ($x_0 = 0$); (ii) $u^2 - uv + v^2 + 1$ ($x_0 = 1$); (iii) $u^2 + 4$ ($x_0 = 2$),

then the integral solution is unique and the number of Γ -orbits is finite.

Theorem (Ghosh-Sarnak).

$$\begin{split} & \sharp\{m \in \mathbb{Z}: \ 0 < m \le K, \quad \prod_p \mathfrak{U}_m(\mathbb{Z}_p) \neq \emptyset \text{ but } \mathfrak{U}_m(\mathbb{Z}) = \emptyset\} \\ & \gg \sqrt{K} (\log K)^{-\frac{1}{2}} \end{split}$$

as $K \to \infty$.

as $K \to \infty$.

Theorem (Ghosh-Sarnak).

$$\begin{split} & \sharp\{m \in \mathbb{Z}: \ 0 < m \le K, \quad \prod_p \mathfrak{U}_m(\mathbb{Z}_p) \neq \emptyset \text{ but } \mathfrak{U}_m(\mathbb{Z}) = \emptyset\} \\ & \gg \sqrt{K} (\log K)^{-\frac{1}{2}} \end{split}$$

 $\text{ as } K \to \infty.$

$$\begin{split} & \sharp\{m\in\mathbb{Z}: \ -K\leq m<0, \quad \prod_p\mathfrak{U}_m(\mathbb{Z}_p)\neq\emptyset \ \text{but} \ \mathfrak{U}_m(\mathbb{Z})=\emptyset\} \\ & \gg \sqrt{K}(logK)^{-\frac{1}{2}} \end{split}$$

 $\text{ as } K \to \infty.$

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4.

If $[\mathbb{Q}(\sqrt{m},\sqrt{d}):\mathbb{Q}]=4$, then

 $\operatorname{Br}(X_m)/\operatorname{Br}(\mathbb{Q}) = \operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong \mathbb{Z}/2$

with a generator

$$\{((\frac{x}{t})^2-4,d)=((\frac{y}{t})^2-4,d)=((\frac{z}{t})^2-4,d)\} \quad \text{ over } t\neq 0.$$

If $d \not\in (\mathbb{Q}^{\times})^2$ and $m \in (\mathbb{Q}^{\times})^2$, then

 $\operatorname{Br}(X_m)/\operatorname{Br}(\mathbb{Q}) = \operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^2$

with two generators

$$\{((\frac{x}{t})^2 - 4, d), ((\sqrt{m} - \frac{x}{t})(\frac{x}{t} + 2), d)\}$$
 over $t \neq 0.$

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4. If $[\mathbb{Q}(\sqrt{m}, \sqrt{d}) : \mathbb{Q}] = 4$, then $\operatorname{Br}(X_m)/\operatorname{Br}(\mathbb{Q}) = \operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong \mathbb{Z}/2$

with a generator

$$\{((\frac{x}{t})^2-4,d)=((\frac{y}{t})^2-4,d)=((\frac{z}{t})^2-4,d)\} \quad \text{ over } \quad t\neq 0.$$

If $d
ot\in (\mathbb{Q}^{ imes})^2$ and $m\in (\mathbb{Q}^{ imes})^2$, then ${
m Br}(X_m)/{
m Br}(\mathbb{Q})={
m Br}_1(X_m)/{
m Br}(X_m)/{
m Br}(X_m)$

with two generators

$$\{((\frac{x}{t})^2 - 4, d), ((\sqrt{m} - \frac{x}{t})(\frac{x}{t} + 2), d)\}$$
 over $t \neq 0$.

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4. If $[\mathbb{Q}(\sqrt{m}, \sqrt{d}) : \mathbb{Q}] = 4$, then $\operatorname{Br}(X_m)/\operatorname{Br}(\mathbb{Q}) = \operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong \mathbb{Z}/2$

with a generator

$$\{((\frac{x}{t})^2-4,d)=((\frac{y}{t})^2-4,d)=((\frac{z}{t})^2-4,d)\} \quad \text{ over } \ t\neq 0.$$

If $d \not\in (\mathbb{Q}^{\times})^2$ and $m \in (\mathbb{Q}^{\times})^2$, then

$$\operatorname{Br}(X_m)/\operatorname{Br}(\mathbb{Q}) = \operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^2$$

with two generators

$$\{((\frac{x}{t})^2 - 4, d), \ ((\sqrt{m} - \frac{x}{t})(\frac{x}{t} + 2), d)\} \quad \text{ over } \quad t \neq 0.$$

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4. If $[\mathbb{Q}(\sqrt{m}, \sqrt{d}) : \mathbb{Q}] = 4$, then $\operatorname{Br}(X_m)/\operatorname{Br}(\mathbb{Q}) = \operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong \mathbb{Z}/2$

with a generator

$$\{((\frac{x}{t})^2-4,d)=((\frac{y}{t})^2-4,d)=((\frac{z}{t})^2-4,d)\} \quad \text{ over } \ t\neq 0.$$

If $d \not\in (\mathbb{Q}^{\times})^2$ and $m \in (\mathbb{Q}^{\times})^2$, then

$$\operatorname{Br}(X_m)/\operatorname{Br}(\mathbb{Q}) = \operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^2$$

with two generators

$$\{((\frac{x}{t})^2 - 4, d), ((\sqrt{m} - \frac{x}{t})(\frac{x}{t} + 2), d)\}$$
 over $t \neq 0$.

Sketch of proof. Since \overline{X}_m is rational, one obtains $Br_1(X_m) = Br(X_m)$.

By $H^p(\mathbb{Q}, H^q(\overline{X}_m, \mathbb{G}_m)) \Rightarrow H^{p+q}(X_m, \mathbb{G}_m)$, one has $\operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong H^1(\mathbb{Q}, \operatorname{Pic}(\overline{X}_m))$

$$H^{1}(\mathbb{Q}, \operatorname{Pic}(\overline{X}_{m})) \cong \begin{cases} \mathbb{Z}/2 & m, d \text{ and} \\ 0 & d \in (\mathbb{Q}^{\times}) \\ (\mathbb{Z}/2)^{2} & m \in (\mathbb{Q}^{\times}) \end{cases}$$

 $m, d \text{ and } md \notin (\mathbb{Q}^{\times})^2$ $d \in (\mathbb{Q}^{\times})^2 \text{ or } d \cdot m \in (\mathbb{Q}^{\times})^2$ $m \in (\mathbb{Q}^{\times})^2 \text{ but } d \notin (\mathbb{Q}^{\times})^2$

Sketch of proof. Since \overline{X}_m is rational, one obtains $Br_1(X_m) = Br(X_m)$.

By $H^p(\mathbb{Q}, H^q(\overline{X}_m, \mathbb{G}_m)) \Rightarrow H^{p+q}(X_m, \mathbb{G}_m)$, one has $\operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong H^1(\mathbb{Q}, \operatorname{Pic}(\overline{X}_m))$

$$H^{1}(\mathbb{Q}, \operatorname{Pic}(\overline{X}_{m})) \cong \begin{cases} \mathbb{Z}/2 & m, d \text{ and } md \notin (\mathbb{Q}^{\times})^{2} \\ 0 & d \in (\mathbb{Q}^{\times})^{2} \text{ or } d \cdot m \in (\mathbb{Q}^{\times})^{2} \\ (\mathbb{Z}/2)^{2} & m \in (\mathbb{Q}^{\times})^{2} \text{ but } d \notin (\mathbb{Q}^{\times})^{2} \end{cases}$$

Sketch of proof. Since \overline{X}_m is rational, one obtains $Br_1(X_m) = Br(X_m)$.

By $H^p(\mathbb{Q}, H^q(\overline{X}_m, \mathbb{G}_m)) \Rightarrow H^{p+q}(X_m, \mathbb{G}_m)$, one has $\operatorname{Br}_1(X_m)/\operatorname{Br}(\mathbb{Q}) \cong H^1(\mathbb{Q}, \operatorname{Pic}(\overline{X}_m))$

$$H^{1}(\mathbb{Q}, \operatorname{Pic}(\overline{X}_{m})) \cong \begin{cases} \mathbb{Z}/2 & m, d \text{ and } md \notin (\mathbb{Q}^{\times})^{2} \\ 0 & d \in (\mathbb{Q}^{\times})^{2} \text{ or } d \cdot m \in (\mathbb{Q}^{\times})^{2} \\ (\mathbb{Z}/2)^{2} & m \in (\mathbb{Q}^{\times})^{2} \text{ but } d \notin (\mathbb{Q}^{\times})^{2} \end{cases}$$

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4.

If $[\mathbb{Q}(\sqrt{m},\sqrt{d}):\mathbb{Q}]=4$ then

 $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q})\cong (\mathbb{Z}/2)^3$

with the generators $\{(x-2,d), (y-2,d), (z-2,d)\}$.

If $d \notin \mathbb{Q}^{ imes 2}$ and $dm \in \mathbb{Q}^{ imes 2}$ then

 $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^2$

with the generators $\{(x-2,d), (y-2,d)\}$.

If $d \notin \mathbb{Q}^{\times 2}$ and $m \in \mathbb{Q}^{\times 2}$, then

 $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^4$

with the generators $\{(x-2,d), (y-2,d), (z-2,d), (x-\sqrt{m},d)\}$.

If $d \in \mathbb{Q}^{\times 2}$, then $\operatorname{Br}_1(U_m) = \operatorname{Br}(\mathbb{Q})$.

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4. If $[\mathbb{Q}(\sqrt{m},\sqrt{d}):\mathbb{Q}]=4$ then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^3$ with the generators $\{(x - 2, d), (y - 2, d), (z - 2, d)\}$. < 由 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > July 9, 2023

20 / 34

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4. If $[\mathbb{Q}(\sqrt{m},\sqrt{d}):\mathbb{Q}]=4$ then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^3$ with the generators $\{(x - 2, d), (y - 2, d), (z - 2, d)\}$. If $d \notin \mathbb{Q}^{\times 2}$ and $dm \in \mathbb{Q}^{\times 2}$ then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^2$ with the generators $\{(x-2,d), (y-2,d)\}$. < 由 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > July 9, 2023

20 / 34

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4. If $[\mathbb{Q}(\sqrt{m},\sqrt{d}):\mathbb{Q}]=4$ then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^3$ with the generators $\{(x - 2, d), (y - 2, d), (z - 2, d)\}$. If $d \notin \mathbb{Q}^{\times 2}$ and $dm \in \mathbb{Q}^{\times 2}$ then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{O}) \cong (\mathbb{Z}/2)^2$ with the generators $\{(x-2,d), (y-2,d)\}$. If $d \notin \mathbb{Q}^{\times 2}$ and $m \in \mathbb{Q}^{\times 2}$, then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{O}) \cong (\mathbb{Z}/2)^4$ with the generators $\{(x - 2, d), (y - 2, d), (z - 2, d), (x - \sqrt{m}, d)\}$. イロト 不得 トイヨト イヨト 二日

Theorem (Colliot-Thelene, Wei and X.; Loughran and Mitankin). Let $m \neq 0, 4$ and d = m - 4. If $[\mathbb{Q}(\sqrt{m},\sqrt{d}):\mathbb{Q}]=4$ then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong (\mathbb{Z}/2)^3$ with the generators $\{(x - 2, d), (y - 2, d), (z - 2, d)\}$. If $d \notin \mathbb{Q}^{\times 2}$ and $dm \in \mathbb{Q}^{\times 2}$ then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{O}) \cong (\mathbb{Z}/2)^2$ with the generators $\{(x-2, d), (y-2, d)\}$. If $d \notin \mathbb{Q}^{\times 2}$ and $m \in \mathbb{Q}^{\times 2}$, then $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{O}) \cong (\mathbb{Z}/2)^4$ with the generators $\{(x - 2, d), (y - 2, d), (z - 2, d), (x - \sqrt{m}, d)\}$. If $d \in \mathbb{Q}^{\times 2}$, then $\operatorname{Br}_1(U_m) = \operatorname{Br}(\mathbb{Q})$. イロト 不得 トイヨト イヨト 二日 July 9, 2023

20 / 34

Sketch of proof. By the exact sequence of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\text{-modules}$

$$0 \to \overline{\mathbb{Q}}^{\times} \to \overline{\mathbb{Q}}[U_m]^{\times} \to \operatorname{Div}_{\overline{X}_m \setminus \overline{U}_m}(\overline{X}_m) \xrightarrow{\phi} \operatorname{Pic}(\overline{X}_m) \to \operatorname{Pic}(\overline{U}_m) \to 0$$

and $\operatorname{Div}_{\overline{X}_m \setminus \overline{U}_m}(\overline{X}_m) = \bigoplus_{i=1}^3 \mathbb{Z}L_i$, one can show ϕ is injective. Indeed, if
 $aL_1 + bL_2 + cL_3 = a(L - l_1 - l_4) + b(L - l_2 - l_5) + c(L - l_3 - l_6) = 0$,
then $a = b = c = 0$. This implies that $\overline{\mathbb{Q}}^{\times} = \overline{\mathbb{Q}}[U_m]^{\times}$ and the sub-lattice
 $\operatorname{Div}_{\overline{X}_m \setminus \overline{U}_m}(\overline{X}_m) = \bigoplus_{i=1}^3 \mathbb{Z}L_i$

is primitive in $\operatorname{Pic}(\overline{X}_m)$. Therefore $\operatorname{Pic}(\overline{U}_m)$ is torsion free.

By
$$H^p(\mathbb{Q}, H^q(\overline{U}_m, \mathbb{G}_m)) \Rightarrow H^{p+q}(U_m, \mathbb{G}_m)$$
, one has
 $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong H^1(\mathbb{Q}, \operatorname{Pic}(\overline{U}_m))$

which is finite.

$$H^{1}(\mathbb{Q}, \operatorname{Pic}(\overline{U}_{m})) \cong \begin{cases} (\mathbb{Z}/2)^{3} & m, d \text{ and } md \notin (\mathbb{Q}^{\times})^{2} \\ (\mathbb{Z}/2)^{2} & d \notin (\mathbb{Q}^{\times})^{2} \text{ and } md \in (\mathbb{Q}^{\times})^{2} \\ (\mathbb{Z}/2)^{4} & d \notin (\mathbb{Q}^{\times})^{2} \text{ and } m \in (\mathbb{Q}^{\times})^{2} \\ 0 & d \in (\mathbb{Q}^{\times})^{2} \end{cases}$$

July 9, 2023 22 / 34

・ロト ・日下 ・ 日下
By
$$H^p(\mathbb{Q}, H^q(\overline{U}_m, \mathbb{G}_m)) \Rightarrow H^{p+q}(U_m, \mathbb{G}_m)$$
, one has
 $\operatorname{Br}_1(U_m)/\operatorname{Br}(\mathbb{Q}) \cong H^1(\mathbb{Q}, \operatorname{Pic}(\overline{U}_m))$

which is finite.

$$H^{1}(\mathbb{Q}, \operatorname{Pic}(\overline{U}_{m})) \cong \begin{cases} (\mathbb{Z}/2)^{3} & m, d \text{ and } md \notin (\mathbb{Q}^{\times})^{2} \\ (\mathbb{Z}/2)^{2} & d \notin (\mathbb{Q}^{\times})^{2} \text{ and } md \in (\mathbb{Q}^{\times})^{2} \\ (\mathbb{Z}/2)^{4} & d \notin (\mathbb{Q}^{\times})^{2} \text{ and } m \in (\mathbb{Q}^{\times})^{2} \\ 0 & d \in (\mathbb{Q}^{\times})^{2} \end{cases}$$

Image: Image:

Theorem (Colliot-Thelene, Wei and X.).

Let $m \neq 0,4$; d = m-4 and $K = \mathbb{Q}(\sqrt{d},\sqrt{m})$.

If -1 and $\frac{\sqrt{d}-\sqrt{m}}{2}$ are in $(K^{\times})^2$, then $\operatorname{Br}(U_m)/\operatorname{Br}_1(U_m) \cong \mathbb{Z}/2$. Otherwise $\operatorname{Br}(U_m) = \operatorname{Br}_1(U_m)$.

Sketch of proof. Recall $\pi: \overline{X}_m \to \mathbb{P}^2$ is a contraction of $\{l_1, \cdots, l_6\}$ to \mathbb{P}^2 and

$$\overline{X}_m = \overline{U}_m \cup \{L_1, L_2, L_3\}.$$

This implies that π induces an isomorphism

 $\overline{U}_m \setminus \{l_1, \cdots, l_6\} \cong \mathbb{P}^2 \setminus \{\pi(L_1), \pi(L_2), \pi(L_3)\} \cong \mathbb{G}_m \times_{\overline{\mathbb{Q}}} \mathbb{G}_m$

over $\overline{\mathbb{Q}}$.

Theorem (Colliot-Thelene, Wei and X.).

Let $m \neq 0, 4$; d = m - 4 and $K = \mathbb{Q}(\sqrt{d}, \sqrt{m})$.

If -1 and $\frac{\sqrt{d}-\sqrt{m}}{2}$ are in $(K^{\times})^2$, then $\operatorname{Br}(U_m)/\operatorname{Br}_1(U_m) \cong \mathbb{Z}/2$. Otherwise $\operatorname{Br}(U_m) = \operatorname{Br}_1(U_m)$.

Sketch of proof. Recall $\pi: \overline{X}_m \to \mathbb{P}^2$ is a contraction of $\{l_1, \cdots, l_6\}$ to \mathbb{P}^2 and

$$\overline{X}_m = \overline{U}_m \cup \{L_1, L_2, L_3\}.$$

This implies that π induces an isomorphism

 $\overline{U}_m \setminus \{l_1, \cdots, l_6\} \cong \mathbb{P}^2 \setminus \{\pi(L_1), \pi(L_2), \pi(L_3)\} \cong \mathbb{G}_m \times_{\overline{\mathbb{Q}}} \mathbb{G}_m$

over $\overline{\mathbb{Q}}$.

Theorem (Colliot-Thelene, Wei and X.).

- Let $m \neq 0,4; \ d=m-4$ and $K=\mathbb{Q}(\sqrt{d},\sqrt{m})$.
- If -1 and $\frac{\sqrt{d}-\sqrt{m}}{2}$ are in $(K^{\times})^2$, then $\operatorname{Br}(U_m)/\operatorname{Br}_1(U_m) \cong \mathbb{Z}/2$. Otherwise $\operatorname{Br}(U_m) = \operatorname{Br}_1(U_m)$.

Sketch of proof. Recall $\pi: \overline{X}_m \to \mathbb{P}^2$ is a contraction of $\{l_1, \cdots, l_6\}$ to \mathbb{P}^2 and

$$\overline{X}_m = \overline{U}_m \cup \{L_1, L_2, L_3\}.$$

This implies that π induces an isomorphism

 $\overline{U}_m \setminus \{l_1, \cdots, l_6\} \cong \mathbb{P}^2 \setminus \{\pi(L_1), \pi(L_2), \pi(L_3)\} \cong \mathbb{G}_m \times_{\overline{\mathbb{Q}}} \mathbb{G}_m$

over $\overline{\mathbb{Q}}$.

(日) (周) (三) (三)

Theorem (Colliot-Thelene, Wei and X.). Let $m \neq 0, 4$; d = m - 4 and $K = \mathbb{Q}(\sqrt{d}, \sqrt{m})$.

If -1 and $\frac{\sqrt{d}-\sqrt{m}}{2}$ are in $(K^{\times})^2$, then $\operatorname{Br}(U_m)/\operatorname{Br}_1(U_m) \cong \mathbb{Z}/2$. Otherwise $\operatorname{Br}(U_m) = \operatorname{Br}_1(U_m)$.

Sketch of proof. Recall $\pi: \overline{X}_m \to \mathbb{P}^2$ is a contraction of $\{l_1, \cdots, l_6\}$ to \mathbb{P}^2 and

$$\overline{X}_m = \overline{U}_m \cup \{L_1, L_2, L_3\}.$$

This implies that π induces an isomorphism

 $\overline{U}_m \setminus \{l_1, \cdots, l_6\} \cong \mathbb{P}^2 \setminus \{\pi(L_1), \pi(L_2), \pi(L_3)\} \cong \mathbb{G}_m \times_{\overline{\mathbb{Q}}} \mathbb{G}_m$

over $\overline{\mathbb{Q}}$.

(日) (周) (三) (三)

Theorem (Colliot-Thelene, Wei and X.).

Let $m \neq 0,4$; d = m - 4 and $K = \mathbb{Q}(\sqrt{d},\sqrt{m})$.

If -1 and $\frac{\sqrt{d}-\sqrt{m}}{2}$ are in $(K^{\times})^2$, then $\operatorname{Br}(U_m)/\operatorname{Br}_1(U_m) \cong \mathbb{Z}/2$. Otherwise $\operatorname{Br}(U_m) = \operatorname{Br}_1(U_m)$.

Sketch of proof. Recall $\pi: \overline{X}_m \to \mathbb{P}^2$ is a contraction of $\{l_1, \cdots, l_6\}$ to \mathbb{P}^2 and

$$\overline{X}_m = \overline{U}_m \cup \{L_1, L_2, L_3\}.$$

This implies that π induces an isomorphism

$$\overline{U}_m \setminus \{l_1, \cdots, l_6\} \cong \mathbb{P}^2 \setminus \{\pi(L_1), \pi(L_2), \pi(L_3)\} \cong \mathbb{G}_m \times_{\overline{\mathbb{Q}}} \mathbb{G}_m$$

over $\overline{\mathbb{Q}}$.

Let
$$V = \overline{U}_m \setminus \{l_1, \cdots, l_6\} \cong \mathbb{G}_m \times_{\overline{\mathbb{Q}}} \mathbb{G}_m$$
. Then
 $0 \to \operatorname{Br}(\overline{U}_m) \to \operatorname{Br}(V) \xrightarrow{res} \bigoplus_{i=1}^6 H^1_{et}(D_i, \mathbb{Q}/\mathbb{Z})$

where

 $D_i = l_i \setminus \{$ the intersection point of l_i with $L_1, L_2, L_3 \} \cong \mathbb{A}^1$

over $\overline{\mathbb{Q}}$. Since $H^1_{et}(\mathbb{A}^1_{\overline{\mathbb{Q}}}, \mathbb{Q}/\mathbb{Z}) = 0$, one concludes that

 $\operatorname{Br}(\overline{U}_m) \cong \operatorname{Br}(V) \cong \operatorname{Br}(\mathbb{G}_m \times_{\overline{\mathbb{O}}} \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}.$

イロト イ団ト イヨト イヨ

Example. If $\sqrt{-1} \notin \mathbb{Q}(\sqrt{d})$, then $\operatorname{Br}(U_m) = \operatorname{Br}_1(U_m)$.

Proof. Suppose that -1 and $\frac{\sqrt{d}-\sqrt{m}}{2}$ are in $(K^{\times})^2$. Since $\sqrt{-1} \notin \mathbb{Q}(\sqrt{d})$, one has $K \neq \mathbb{Q}(\sqrt{d})$ and $\sqrt{m} \notin \mathbb{Q}(\sqrt{d})$. Then

$$Norm_{K/\mathbb{Q}(\sqrt{d})}(\frac{\sqrt{d}-\sqrt{m}}{2}) = (\frac{\sqrt{d}-\sqrt{m}}{2})(\frac{\sqrt{d}+\sqrt{m}}{2}) = -1$$

On the other hand, $\frac{\sqrt{d}-\sqrt{m}}{2} \in (K^{\times})^2$. This implies that $\sqrt{-1} \in \mathbb{Q}(\sqrt{d})$. A contradiction is derived.

Example. If $\sqrt{-1} \notin \mathbb{Q}(\sqrt{d})$, then $\operatorname{Br}(U_m) = \operatorname{Br}_1(U_m)$.

Proof. Suppose that -1 and $\frac{\sqrt{d}-\sqrt{m}}{2}$ are in $(K^{\times})^2$. Since $\sqrt{-1} \notin \mathbb{Q}(\sqrt{d})$, one has $K \neq \mathbb{Q}(\sqrt{d})$ and $\sqrt{m} \notin \mathbb{Q}(\sqrt{d})$. Then

$$Norm_{K/\mathbb{Q}(\sqrt{d})}(\frac{\sqrt{d}-\sqrt{m}}{2}) = (\frac{\sqrt{d}-\sqrt{m}}{2})(\frac{\sqrt{d}+\sqrt{m}}{2}) = -1$$

On the other hand, $\frac{\sqrt{d}-\sqrt{m}}{2} \in (K^{\times})^2$. This implies that $\sqrt{-1} \in \mathbb{Q}(\sqrt{d})$. A contradiction is derived.

Example. If $\sqrt{-1} \notin \mathbb{Q}(\sqrt{d})$, then $\operatorname{Br}(U_m) = \operatorname{Br}_1(U_m)$.

Proof. Suppose that -1 and $\frac{\sqrt{d}-\sqrt{m}}{2}$ are in $(K^{\times})^2$. Since $\sqrt{-1} \notin \mathbb{Q}(\sqrt{d})$, one has $K \neq \mathbb{Q}(\sqrt{d})$ and $\sqrt{m} \notin \mathbb{Q}(\sqrt{d})$. Then

$$Norm_{K/\mathbb{Q}(\sqrt{d})}(\frac{\sqrt{d}-\sqrt{m}}{2}) = (\frac{\sqrt{d}-\sqrt{m}}{2})(\frac{\sqrt{d}+\sqrt{m}}{2}) = -1$$

On the other hand, $\frac{\sqrt{d}-\sqrt{m}}{2} \in (K^{\times})^2$. This implies that $\sqrt{-1} \in \mathbb{Q}(\sqrt{d})$. A contradiction is derived.

Example. If $m = 4 + rv^2$ where $r \in \mathbb{Z}$ is one of 2, -2, -3, 12, -12 and all prime factors of v are congruent to

 $\begin{cases} \pm 1 \mod 8 & \text{when } r = 2 \\ \pm 1 \mod 12 \text{ and } v^2 \equiv 25 \mod 32 & \text{when } r = 12 \\ 1 \text{ or } 3 \mod 8 & \text{when } r = -2 \text{ and } m < 0 \\ 1 \mod 3 & \text{when } r = -3 \text{ and } m < 0 \\ 1 \mod 3 & \text{when } r = -12, \end{cases}$

then

$$(\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\mathrm{Br}_1(U_m)}=\emptyset$$

In particular, $\mathfrak{U}_m(\mathbb{Z}) = \emptyset$.

Example. If $m = 4 + 20v^2$ where all prime factors of v are congruent to $\pm 1 \mod 5$, then

$$(\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\mathrm{Br}_1(U_m)}=\emptyset$$

In particular, $\mathfrak{U}_m(\mathbb{Z}) = \emptyset$.

Theorem (Loughran and Mitankin). Let d = m - 4. If

$$(\prod_{p \le \infty} \mathfrak{U}_m(\mathbb{Z}_p)) \neq \emptyset \quad \mathsf{but} \quad (\prod_{p \le \infty} \mathfrak{U}_m(\mathbb{Z}_p))^{\mathrm{Br}_1(U_m)} = \emptyset$$

then d belongs to a finite subgroup of $\mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2$ generated by

 $\{\pm 1, 2, 3, 5\}.$

Example. If $m = 4 + 20v^2$ where all prime factors of v are congruent to $\pm 1 \mod 5$, then

$$(\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\mathrm{Br}_1(U_m)}=\emptyset$$

In particular, $\mathfrak{U}_m(\mathbb{Z}) = \emptyset$.

Theorem (Loughran and Mitankin). Let d = m - 4. If

$$(\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))\neq \emptyset \quad \text{but} \quad (\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\mathrm{Br}_1(U_m)}=\emptyset$$

then d belongs to a finite subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ generated by

 $\{\pm 1, 2, 3, 5\}.$

Theorem (Loughran and Mitankin).

$$\begin{split} & \sharp\{m\in\mathbb{Z}:\ |m|\leq K,\ \prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p)\neq\emptyset\ \text{but}\ (\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\mathrm{Br}(U_m)}=\emptyset\}\\ & \asymp\sqrt{K}(\log K)^{-\frac{1}{2}}\\ & \text{as }K\to\infty. \end{split}$$

Theorem (Loughran and Mitankin).

$$\sharp \{ m \in \mathbb{Z} : |m| \le K, \ (\prod_{p \le \infty} \mathfrak{U}_m(\mathbb{Z}_p))^{\operatorname{Br}(U_m)} \neq \emptyset \text{ but } \mathfrak{U}_m(\mathbb{Z}) = \emptyset \}$$
$$\gg \sqrt{K} (\log K)^{-1}$$

as $K \to \infty$.

Theorem (Loughran and Mitankin).

$$\begin{split} & \sharp\{m\in\mathbb{Z}:\ |m|\leq K,\quad \prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p)\neq\emptyset \quad \text{but} \quad (\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\operatorname{Br}(U_m)}=\emptyset\}\\ & \asymp\sqrt{K}(\log K)^{-\frac{1}{2}}\\ & \text{as }K\to\infty. \end{split}$$

Theorem (Loughran and Mitankin).

$$\sharp \{ m \in \mathbb{Z} : |m| \le K, \ (\prod_{p \le \infty} \mathfrak{U}_m(\mathbb{Z}_p))^{\operatorname{Br}(U_m)} \neq \emptyset \text{ but } \mathfrak{U}_m(\mathbb{Z}) = \emptyset \}$$
$$\gg \sqrt{K} (\log K)^{-1}$$

as $K \to \infty$.

Proposition (Ghosh-Sarnak).

If $m = 4 + 2l^2$ where $l \ge 13$ is a prime with $l \equiv \pm 4 \mod 9$, then

$$\prod_{p \leq \infty} \mathfrak{U}_m(\mathbb{Z}_p) \neq \emptyset \quad \text{but} \quad \mathfrak{U}_m(\mathbb{Z}) = \emptyset.$$

Proposition (Colliot-Thelene, Wei and X.).

Let $m = 4 + 2l^2w^2$ where w is an odd integer and l is a prime with $l \equiv \pm 3 \mod 8$.

If $lw \equiv \pm 4 \mod 9$, then

$$(\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\mathrm{Br}(U_m)}\neq\emptyset.$$

Proposition (Ghosh-Sarnak).

If $m = 4 + 2l^2$ where $l \ge 13$ is a prime with $l \equiv \pm 4 \mod 9$, then

$$\prod_{p \leq \infty} \mathfrak{U}_m(\mathbb{Z}_p) \neq \emptyset \quad \text{but} \quad \mathfrak{U}_m(\mathbb{Z}) = \emptyset.$$

Proposition (Colliot-Thelene, Wei and X.).

Let $m = 4 + 2l^2w^2$ where w is an odd integer and l is a prime with $l \equiv \pm 3 \mod 8$.

If $lw \equiv \pm 4 \mod 9$, then

$$(\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\mathrm{Br}(U_m)}\neq\emptyset.$$

Proposition (Colliot-Thelene, Wei and X.).

If $m = 4 + rl^2$ such that one of the following conditions holds

i) r=2 and $l\geq 13$ is a prime with $l\equiv \pm 4 \mod 9$,

ii) r = 12 and $l \ge 37$ is a prime, $l^2 \equiv 25 \mod 32$ and $1 + 3l^2$ is not a sum of two squares (e.g. l = 37, 43, ...),

iii) r=-2 and $l\geq 13$ is a prime,

iv) r = -3 and $l \ge 17$ is a prime,

v) r = -12 and $l \ge 37$ is a prime,

then

 $\mathfrak{U}_m(\mathbb{Z})=\emptyset.$

If $m = 4 + rl^2$ such that one of the following conditions holds

i) r = 2 and $l \ge 13$ is a prime with $l \equiv \pm 4 \mod 9$,

ii) r = 12 and $l \ge 37$ is a prime, $l^2 \equiv 25 \mod 32$ and $1 + 3l^2$ is not a sum of two squares (e.g. l = 37, 43, ...),

iii) r = -2 and $l \ge 13$ is a prime,

iv) r = -3 and $l \ge 17$ is a prime,

v) r = -12 and $l \ge 37$ is a prime,

then

 $\mathfrak{U}_m(\mathbb{Z})=\emptyset.$

If $m = 4 + rl^2$ such that one of the following conditions holds i) r = 2 and $l \ge 13$ is a prime with $l \equiv \pm 4 \mod 9$, ii) r = 12 and $l \ge 37$ is a prime, $l^2 \equiv 25 \mod 32$ and $1 + 3l^2$ is not a sum of two squares (e.g. l = 37, 43, ...),

 $\mathfrak{U}_m(\mathbb{Z}) = \emptyset.$

If $m = 4 + rl^2$ such that one of the following conditions holds i) r = 2 and $l \ge 13$ is a prime with $l \equiv \pm 4 \mod 9$, ii) r = 12 and $l \ge 37$ is a prime, $l^2 \equiv 25 \mod 32$ and $1 + 3l^2$ is not a sum of two squares (e.g. l = 37, 43, ...), iii) r = -2 and $l \ge 13$ is a prime,

 $\mathfrak{U}_m(\mathbb{Z}) = \emptyset.$

If $m = 4 + rl^2$ such that one of the following conditions holds i) r = 2 and $l \ge 13$ is a prime with $l \equiv \pm 4 \mod 9$, ii) r = 12 and $l \ge 37$ is a prime, $l^2 \equiv 25 \mod 32$ and $1 + 3l^2$ is not a sum of two squares (e.g. l = 37, 43, ...), iii) r = -2 and $l \ge 13$ is a prime, iv) r = -3 and $l \ge 17$ is a prime,

If $m = 4 + rl^2$ such that one of the following conditions holds i) r = 2 and $l \ge 13$ is a prime with $l \equiv \pm 4 \mod 9$, ii) r = 12 and l > 37 is a prime, $l^2 \equiv 25 \mod 32$ and $1 + 3l^2$ is not a sum of two squares (e.g. l = 37, 43, ...), iii) r = -2 and $l \ge 13$ is a prime, iv) r = -3 and l > 17 is a prime. v) r = -12 and $l \ge 37$ is a prime,

 $\mathfrak{U}_m(\mathbb{Z}) = \emptyset.$

If $m = 4 + rl^2$ such that one of the following conditions holds i) r = 2 and $l \ge 13$ is a prime with $l \equiv \pm 4 \mod 9$, ii) r = 12 and l > 37 is a prime, $l^2 \equiv 25 \mod 32$ and $1 + 3l^2$ is not a sum of two squares (e.g. l = 37, 43, ...), iii) r = -2 and $l \ge 13$ is a prime, iv) r = -3 and l > 17 is a prime. v) r = -12 and $l \ge 37$ is a prime, then

$$\mathfrak{U}_m(\mathbb{Z})=\emptyset.$$

Sketch of proof for case i).

Suppose $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$. By the reduction theory, there is $(x_0, y_0, z_0) \in \mathfrak{U}_m(\mathbb{Z})$ such that

 $3 \le x_0 \le y_0 \le -z_0$ or $x_0 = 0, 1, 2$ (which can be excluded)

This implies that $x_0 \leq (4+2l^2)^{\frac{1}{3}}$. Then $x_0 < l-2$.

One concludes $(l, x_0^2 - 4) = 1$ and the Hilbert symbol $(x_0^2 - 4, 2)_l = 1$. Therefore

$$(x_0^2 - 4, 2)_p = \begin{cases} 1 & p \neq 2 \\ -1 & p = 2 \end{cases}$$

This contradicts to the Hilbert (quadratic) reciprocity law.

Sketch of proof for case i).

Suppose $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$. By the reduction theory, there is $(x_0, y_0, z_0) \in \mathfrak{U}_m(\mathbb{Z})$ such that

 $3 \le x_0 \le y_0 \le -z_0$ or $x_0 = 0, 1, 2$ (which can be excluded)

This implies that $x_0 \le (4+2l^2)^{\frac{1}{3}}$. Then $x_0 < l-2$.

One concludes $(l, x_0^2 - 4) = 1$ and the Hilbert symbol $(x_0^2 - 4, 2)_l = 1$. Therefore

$$(x_0^2 - 4, 2)_p = \begin{cases} 1 & p \neq 2 \\ -1 & p = 2 \end{cases}$$

This contradicts to the Hilbert (quadratic) reciprocity law.

Sketch of proof for case i).

Suppose $\mathfrak{U}_m(\mathbb{Z}) \neq \emptyset$. By the reduction theory, there is $(x_0, y_0, z_0) \in \mathfrak{U}_m(\mathbb{Z})$ such that

 $3 \leq x_0 \leq y_0 \leq -z_0$ or $x_0 = 0, 1, 2$ (which can be excluded)

This implies that $x_0 \le (4+2l^2)^{\frac{1}{3}}$. Then $x_0 < l-2$.

One concludes $(l, x_0^2 - 4) = 1$ and the Hilbert symbol $(x_0^2 - 4, 2)_l = 1$. Therefore

$$(x_0^2 - 4, 2)_p = \begin{cases} 1 & p \neq 2 \\ -1 & p = 2 \end{cases}$$

This contradicts to the Hilbert (quadratic) reciprocity law.

イロト 不得下 イヨト イヨト 二日

By applying this idea, we can also improve the result of Loughran and Mitankin as follows

Theorem (Colliot-Thelene, Wei and X.).

$$\sharp \{ m \in \mathbb{Z} : |m| \le K, \quad (\prod_{p \le \infty} \mathfrak{U}_m(\mathbb{Z}_p))^{\operatorname{Br}(U_m)} \neq \emptyset \text{ but } \mathfrak{U}_m(\mathbb{Z}) = \emptyset \}$$
$$\gg \sqrt{K} (\log K)^{-\frac{1}{2}}$$

 $\text{ as } K \to \infty.$

VII. Failure of strong approximation

Theorem (Colliot-Thelene, Wei and X.).

For any finite set ${\boldsymbol{S}}$ of primes, the image of the natural map

$$\mathfrak{U}_m(\mathbb{Z}) \to \prod_{p \notin S} \mathfrak{U}_m(\mathbb{Z}_p)$$

is not dense.

Corollary. $\mathfrak{U}_m(\mathbb{Z})$ is not dense in $pr^f((\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\operatorname{Br}(U_m)})$. On the other hand, $\mathfrak{U}_m(\mathbb{Z})$ is Zariski dense in \mathfrak{U}_m if

 $\begin{cases} m > 4 \text{ is not a square} \\ m \text{ is a square with a prime } p | m \text{ and } p \equiv 1 \mod 4 \\ m < 0 \end{cases}$

VII. Failure of strong approximation

Theorem (Colliot-Thelene, Wei and X.).

For any finite set ${\boldsymbol{S}}$ of primes, the image of the natural map

$$\mathfrak{U}_m(\mathbb{Z}) \to \prod_{p \notin S} \mathfrak{U}_m(\mathbb{Z}_p)$$

is not dense.

Corollary. $\mathfrak{U}_m(\mathbb{Z})$ is not dense in $pr^f((\prod_{p\leq\infty}\mathfrak{U}_m(\mathbb{Z}_p))^{\operatorname{Br}(U_m)})$. On the other hand, $\mathfrak{U}_m(\mathbb{Z})$ is Zariski dense in \mathfrak{U}_m if

$$\left\{ \begin{array}{ll} m>4 \text{ is not a square} \\ m \text{ is a square with a prime } p|m \text{ and } p\equiv 1 \mod 4 \\ m<0 \end{array} \right.$$

Thank you for your attention !

→ < ∃ >

July 9, 2023

34 / 34