

# Quadratic diophantine equations over function fields

Chang Lv

State Key Laboratory of Information Security (SKLOIS),  
Institute of Information Engineering (IIE),  
Chinese Academy of Sciences (CAS)

May 18, 2021

# Outline

1 **Problem:** is  $ax^2 + bxy + cy^2 + g = 0$  solvable over  $\mathbb{F}_q[t]$  ?

2 **Solution:** torsors under norm-one tori + class field theory

3 **Application:** primes of the form  $x^2 + Dy^2$  in  $\mathbb{F}_q[t]$

## Binary quad. forms over $\mathbb{F}_q[t]$

- Let  $k = \mathbb{F}_q$ ,  $F = k(t)$  rational func. field,  $\mathfrak{o}_F = k[t]$  the poly. ring.
- Fix  $a, b, c$  and  $d$  in  $\mathfrak{o}_F$ , and consider the diophantine eq. def. by the bin. quad. form

$$ax^2 + bxy + cy^2 + g = 0.$$

- Problem: when does it solvable over  $\mathfrak{o}_F$  ?

## Binary quad. forms over $\mathbb{F}_q[t]$

- Let  $k = \mathbb{F}_q$ ,  $F = k(t)$  rational func. field,  $\mathfrak{o}_F = k[t]$  the poly. ring.
- Fix  $a, b, c$  and  $d$  in  $\mathfrak{o}_F$ , and consider the diophantine eq. def. by the bin. quad. form

$$ax^2 + bxy + cy^2 + g = 0.$$

- Problem: when does it solvable over  $\mathfrak{o}_F$  ?

## Binary quad. forms over $\mathbb{F}_q[t]$

- Let  $k = \mathbb{F}_q$ ,  $F = k(t)$  rational func. field,  $\mathfrak{o}_F = k[t]$  the poly. ring.
- Fix  $a, b, c$  and  $d$  in  $\mathfrak{o}_F$ , and consider the diophantine eq. def. by the bin. quad. form

$$ax^2 + bxy + cy^2 + g = 0.$$

- Problem: when does it solvable over  $\mathfrak{o}_F$  ?

## An example

### Example 1.1

- Consider the eq. over  $k[t] = \mathbb{F}_3[t]$

$$-x^2 + txy - (t^3 - t^2 + 1)y^2 + g = 0. \quad (1.2)$$

Write  $g = u \times (t-1)^{s_1} \times (t^2 - t - 1)^{s_2} \times \prod_{j=1}^r p_j^{m_j}$ , where  $u \in k^\times$ ,  $p_r$  distinct monic irr. poly. in  $k[t]$ .

- Then (1.2) is solvable over  $k[t]$  if and only if

- $\left(\frac{g \times p^{-v_p(g)}}{p}\right) = (-1)^{v_p(g)}$ , for  $p = t-1$  or  $t^2 - t - 1$ ,
- $\left(\frac{-(t-1)(t^2-t-1)}{p}\right) = 1$ , for  $p \nmid (t-1)(t^2-t-1)$ ,  $v_p(g)$  odd.

## An example

### Example 1.1

- Consider the eq. over  $k[t] = \mathbb{F}_3[t]$

$$-x^2 + txy - (t^3 - t^2 + 1)y^2 + g = 0. \quad (1.2)$$

Write  $g = u \times (t-1)^{s_1} \times (t^2 - t - 1)^{s_2} \times \prod_{j=1}^r p_j^{m_j}$ , where  $u \in k^\times$ ,  $p_r$  distinct monic irr. poly. in  $k[t]$ .

- Then (1.2) is solvable over  $k[t]$  if and only if

- $\left(\frac{g \times p^{-v_p(g)}}{p}\right) = (-1)^{v_p(g)}$ , for  $p = t-1$  or  $t^2 - t - 1$ ,
- $\left(\frac{-(t-1)(t^2-t-1)}{p}\right) = 1$ , for  $p \nmid (t-1)(t^2-t-1)$ ,  $v_p(g)$  odd.

## An example

### Example 1.1

- Consider the eq. over  $k[t] = \mathbb{F}_3[t]$

$$-x^2 + txy - (t^3 - t^2 + 1)y^2 + g = 0. \quad (1.2)$$

Write  $g = u \times (t-1)^{s_1} \times (t^2 - t - 1)^{s_2} \times \prod_{j=1}^r p_j^{m_j}$ , where  $u \in k^\times$ ,  $p_r$  distinct monic irr. poly. in  $k[t]$ .

- Then (1.2) is solvable over  $k[t]$  if and only if

- $\left(\frac{g \times p^{-v_p(g)}}{p}\right) = (-1)^{v_p(g)}$ , for  $p = t-1$  or  $t^2 - t - 1$ ,
- $\left(\frac{-(t-1)(t^2-t-1)}{p}\right) = 1$ , for  $p \nmid (t-1)(t^2-t-1)$ ,  $v_p(g)$  odd.



## Another example

### Example 1.3

- The eq. over  $k[t] = \mathbb{F}_3[t]$

$$(t-1)x^2 + (t^2 + t - 1)y^2 + g = 0. \quad (1.4)$$

Write  $q_1 = t-1$ ,  $q_2 = t^2 + t - 1$  and  $-d = -q_1q_2$  and define

$$\theta(X) = X^4 - (t^2 - t)X^2 - t^3 + 1 \in k[t][X]$$

(generates certain Galois extension),

$$D_1 = \{p \mid \left(\frac{-d}{p}\right) = 1, \theta(X) \bmod p \text{ factors into two irr. polys.}\},$$

$$D_2 = \{p \mid \left(\frac{-d}{p}\right) = 1, \theta(X) \bmod p \text{ is irr.}\}$$

(reflex the splittings of places)

## Another example

### Example 1.3

- The eq. over  $k[t] = \mathbb{F}_3[t]$

$$(t-1)x^2 + (t^2+t-1)y^2 + g = 0. \quad (1.4)$$

Write  $q_1 = t-1$ ,  $q_2 = t^2+t-1$  and  $-d = -q_1q_2$  and define

$$\theta(X) = X^4 - (t^2-t)X^2 - t^3 + 1 \in k[t][X]$$

(generates certain Galois extension),

$$D_1 = \{p \mid \left(\frac{-d}{p}\right) = 1, \theta(X) \text{ mod } p \text{ factors into two irr. polys.}\},$$

$$D_2 = \{p \mid \left(\frac{-d}{p}\right) = 1, \theta(X) \text{ mod } p \text{ is irr.}\}$$

(reflex the splittings of places)

## Another example

### Example 1.3

- The eq. over  $k[t] = \mathbb{F}_3[t]$

$$(t-1)x^2 + (t^2 + t - 1)y^2 + g = 0. \quad (1.4)$$

Write  $q_1 = t - 1$ ,  $q_2 = t^2 + t - 1$  and  $-d = -q_1q_2$  and define

$$\theta(X) = X^4 - (t^2 - t)X^2 - t^3 + 1 \in k[t][X]$$

(generates certain Galois extension),

$$D_1 = \{p \mid \left(\frac{-d}{p}\right) = 1, \theta(X) \text{ mod } p \text{ factors into two irr. polys.}\},$$

$$D_2 = \{p \mid \left(\frac{-d}{p}\right) = 1, \theta(X) \text{ mod } p \text{ is irr.}\}$$

(reflex the splittings of places)

## Another example (count.)

### Example (1.3, count.)

- Then (1.4) is solvable over  $k[t]$  if and only if

(1)  $\left(\frac{g \times p^{-v_p(g)}}{p}\right) = (-1)^{\deg(p)}$ , for  $q_1$  or  $q_2$ ,

(2)  $\left(\frac{-d}{p}\right) = 1$ , for  $p \nmid d$  with odd  $v_p(g)$ ,

(3) either

- $D_2 = \emptyset$  and  $\sum_{p \in \{q_1, q_2\} \cup D_1} v_p(g) \equiv 1 \pmod{2}$ , or
- $D_2 \neq \emptyset$  and  $\sum_{p \in D_2} v_p(g) \equiv 0 \pmod{2}$ .

- The conditions (1) and (2) are **local**,
- and (3) is called the **Artin condition**.

## Another example (count.)

### Example (1.3, count.)

- Then (1.4) is solvable over  $k[t]$  if and only if

(1)  $\left(\frac{g \times p^{-v_p(g)}}{p}\right) = (-1)^{\deg(p)}$ , for  $q_1$  or  $q_2$ ,

(2)  $\left(\frac{-d}{p}\right) = 1$ , for  $p \nmid d$  with odd  $v_p(g)$ ,

(3) either

- $D_2 = \emptyset$  and  $\sum_{p \in \{q_1, q_2\} \cup D_1} v_p(g) \equiv 1 \pmod{2}$ , or
- $D_2 \neq \emptyset$  and  $\sum_{p \in D_2} v_p(g) \equiv 0 \pmod{2}$ .

- The conditions (1) and (2) are **local**,
- and (3) is called the **Artin condition**.

## Another example (count.)

### Example (1.3, count.)

- Then (1.4) is solvable over  $k[t]$  if and only if

(1)  $\left(\frac{g \times p^{-v_p(g)}}{p}\right) = (-1)^{\deg(p)}$ , for  $q_1$  or  $q_2$ ,

(2)  $\left(\frac{-d}{p}\right) = 1$ , for  $p \nmid d$  with odd  $v_p(g)$ ,

(3) either

- $D_2 = \emptyset$  and  $\sum_{p \in \{q_1, q_2\} \cup D_1} v_p(g) \equiv 1 \pmod{2}$ , or
- $D_2 \neq \emptyset$  and  $\sum_{p \in D_2} v_p(g) \equiv 0 \pmod{2}$ .

- The conditions (1) and (2) are **local**,
- and (3) is called the **Artin condition**.

## Another example (count.)

### Example (1.3, count.)

- Then (1.4) is solvable over  $k[t]$  if and only if

(1)  $\left(\frac{g \times p^{-v_p(g)}}{p}\right) = (-1)^{\deg(p)}$ , for  $q_1$  or  $q_2$ ,

(2)  $\left(\frac{-d}{p}\right) = 1$ , for  $p \nmid d$  with odd  $v_p(g)$ ,

(3) either

- $D_2 = \emptyset$  and  $\sum_{p \in \{q_1, q_2\} \cup D_1} v_p(g) \equiv 1 \pmod{2}$ , or
- $D_2 \neq \emptyset$  and  $\sum_{p \in D_2} v_p(g) \equiv 0 \pmod{2}$ .

- The conditions (1) and (2) are **local**,
- and (3) is called the **Artin condition**.

# Outline

1 **Problem:** is  $ax^2 + bxy + cy^2 + g = 0$  solvable over  $\mathbb{F}_q[t]$  ?

2 **Solution:** torsors under norm-one tori + class field theory

3 **Application:** primes of the form  $x^2 + Dy^2$  in  $\mathbb{F}_q[t]$



# The reformulation in arith. geometry

## ■ Restrictions:

- $k$  with char. not 2,  $-d = (b/2)^2 - ac$  not square,
- the quad. ext.  $E = F(\sqrt{-d})/F$  is **imaginary**, i.e., there is a **unique place lying over  $1/t$** .
- The question is to ask the existence of integral points of the affine scheme  $\mathbf{X} = \text{Spec}(\mathfrak{o}_F[x, y]/(a(ax^2 + bxy + cy^2 + g)))$  over  $\mathfrak{o}_F$ .
  - General tool: (int.) obstructions to local-global principal.
  - Observation:  $\tilde{x} = ax + \frac{b}{2}y, \tilde{y} = y, n = -ag, \mathbf{X} : \tilde{x}^2 + d\tilde{y}^2 = n$ , whose generic fiber admits the structure of **a torsor of a torus**.
  - Bonus: we can make use of class field theory.

# The reformulation in arith. geometry

- Restrictions:
  - $k$  with char. not 2,  $-d = (b/2)^2 - ac$  not square,
  - the quad. ext.  $E = F(\sqrt{-d})/F$  is **imaginary**, i.e., there is a **unique place lying over  $1/t$** .
- The question is to ask the existence of integral points of the affine scheme  $\mathbf{X} = \text{Spec}(\mathfrak{o}_F[x, y]/(a(ax^2 + bxy + cy^2 + g)))$  over  $\mathfrak{o}_F$ .
  - General tool: (int.) obstructions to local-global principal.
  - Observation:  $\tilde{x} = ax + \frac{b}{2}y, \tilde{y} = y, n = -ag, \mathbf{X} : \tilde{x}^2 + d\tilde{y}^2 = n$ , whose generic fiber admits the structure of **a torsor of a torus**.
  - Bonus: we can make use of class field theory.

# The reformulation in arith. geometry

- Restrictions:
  - $k$  with char. not 2,  $-d = (b/2)^2 - ac$  not square,
  - the quad. ext.  $E = F(\sqrt{-d})/F$  is **imaginary**, i.e., there is a **unique place lying over  $1/t$** .
- The question is to ask the existence of integral points of the affine scheme  $\mathbf{X} = \text{Spec}(\mathfrak{o}_F[x, y]/(a(ax^2 + bxy + cy^2 + g)))$  over  $\mathfrak{o}_F$ .
  - General tool: (int.) obstructions to local-global principal.
  - Observation:  $\tilde{x} = ax + \frac{b}{2}y, \tilde{y} = y, n = -ag, \mathbf{X} : \tilde{x}^2 + d\tilde{y}^2 = n$ , whose generic fiber admits the structure of **a torsor of a torus**.
  - Bonus: we can make use of class field theory.

# The reformulation in arith. geometry

- Restrictions:
  - $k$  with char. not 2,  $-d = (b/2)^2 - ac$  not square,
  - the quad. ext.  $E = F(\sqrt{-d})/F$  is **imaginary**, i.e., there is a **unique place lying over  $1/t$** .
  
- The question is to ask the existence of integral points of the affine scheme  $\mathbf{X} = \text{Spec}(\mathfrak{o}_F[x, y]/(a(ax^2 + bxy + cy^2 + g)))$  over  $\mathfrak{o}_F$ .
  - General tool: (int.) obstructions to local-global principal.
  - Observation:  $\tilde{x} = ax + \frac{b}{2}y, \tilde{y} = y, n = -ag, \mathbf{X} : \tilde{x}^2 + d\tilde{y}^2 = n$ , whose generic fiber admits the structure of **a torsor of a torus**.
  - Bonus: we can make use of class field theory.

# The reformulation in arith. geometry

- Restrictions:
  - $k$  with char. not 2,  $-d = (b/2)^2 - ac$  not square,
  - the quad. ext.  $E = F(\sqrt{-d})/F$  is **imaginary**, i.e., there is a **unique place lying over  $1/t$** .
  
- The question is to ask the existence of integral points of the affine scheme  $\mathbf{X} = \text{Spec}(\mathfrak{o}_F[x, y]/(a(ax^2 + bxy + cy^2 + g)))$  over  $\mathfrak{o}_F$ .
  - General tool: (int.) obstructions to local-global principal.
  - Observation:  $\tilde{x} = ax + \frac{b}{2}y, \tilde{y} = y, n = -ag, \mathbf{X} : \tilde{x}^2 + d\tilde{y}^2 = n$ , whose generic fiber admits the structure of **a torsor of a torus**.
  - Bonus: we can make use of class field theory.

# Torsors under norm-one tori

- Let  $T = \ker(R_{E/F}(\mathbb{G}_{m,E}) \xrightarrow{N_{E/F}} \mathbb{G}_{m,F})$  (called **norm-one torus**), and  $X_F = X \times_{o_F} F$  the generic fiber.
- Intuition: if  $N(t) = 1$  and  $N(x) = n$  then  $N(tx) = n$ .  
 $\rightsquigarrow T \times X_F \rightarrow X_F$ , making  $X_F$  a  $T$ -torsor.
- Fix a rat. pt.  $P \in X_F(F)$  to obtain  $\phi_P : X_F \xrightarrow{\sim} T$ , whose restriction to  $\mathbf{X}(o_{F_p})$  (int. local pts.) has image in  $\mathbb{I}_E$  (idèle group).
- The composition  $\tilde{f}_E : \prod_{\mathfrak{p}} \mathbf{X}(o_{F_p}) \rightarrow \mathbb{I}_E \xrightarrow{\times P} \mathbb{I}_E$  whose  $\mathfrak{p}$ -component is

$$\tilde{f}_E[(x_p, y_p)] = \begin{cases} (\tilde{x}_p + \sqrt{-d}\tilde{y}_p, \tilde{x}_p - \sqrt{-d}\tilde{y}_p) \in E_{\mathfrak{q}\mathfrak{p}} \times E_{\mathfrak{q}\mathfrak{p}} & , \text{ if } \mathfrak{p} = \mathfrak{q}\mathfrak{p} \text{ splits in } E/F, \\ \tilde{x}_p + \sqrt{-d}\tilde{y}_p \in E_{\mathfrak{q}\mathfrak{p}} & , \text{ otherwise,} \end{cases}$$

where  $\mathfrak{q}$  and  $\mathfrak{p}$  (resp.  $\mathfrak{q}$ ) are places of  $E$  above  $\mathfrak{p}$  and  $\tilde{x}_p = ax_p + \frac{b}{2}y_p$ ,  $\tilde{y}_p = y_p$ .

# Torsors under norm-one tori

- Let  $T = \ker(R_{E/F}(\mathbb{G}_{m,E}) \xrightarrow{N_{E/F}} \mathbb{G}_{m,F})$  (called **norm-one torus**), and  $X_F = X \times_{o_F} F$  the generic fiber.
- Intuition: if  $N(t) = 1$  and  $N(x) = n$  then  $N(tx) = n$ .  
 $\rightsquigarrow T \times X_F \rightarrow X_F$ , making  $X_F$  a  $T$ -torsor.
- Fix a rat. pt.  $P \in X_F(F)$  to obtain  $\phi_P : X_F \xrightarrow{\sim} T$ , whose restriction to  $\mathbf{X}(o_{F_p})$  (int. local pts.) has image in  $\mathbb{I}_E$  (idèle group).
- The composition  $\tilde{f}_E : \prod_{\mathfrak{p}} \mathbf{X}(o_{F_p}) \rightarrow \mathbb{I}_E \xrightarrow{\times P} \mathbb{I}_E$  whose  $\mathfrak{p}$ -component is

$$\tilde{f}_E[(x_p, y_p)] = \begin{cases} (\tilde{x}_p + \sqrt{-d}\tilde{y}_p, \tilde{x}_p - \sqrt{-d}\tilde{y}_p) \in E_{\mathfrak{q}\mathfrak{p}} \times E_{\mathfrak{q}\mathfrak{p}} & , \text{ if } \mathfrak{p} = \mathfrak{q}\mathfrak{p} \text{ splits in } E/F, \\ \tilde{x}_p + \sqrt{-d}\tilde{y}_p \in E_{\mathfrak{q}\mathfrak{p}} & , \text{ otherwise,} \end{cases}$$

where  $\mathfrak{q}$  and  $\mathfrak{p}$  (resp.  $\mathfrak{q}$ ) are places of  $E$  above  $\mathfrak{p}$  and  $\tilde{x}_p = ax_p + \frac{b}{2}y_p$ ,  $\tilde{y}_p = y_p$ .

# Torsors under norm-one tori

- Let  $T = \ker(R_{E/F}(\mathbb{G}_{m,E}) \xrightarrow{N_{E/F}} \mathbb{G}_{m,F})$  (called **norm-one torus**), and  $X_F = X \times_{o_F} F$  the generic fiber.
- Intuition: if  $N(t) = 1$  and  $N(x) = n$  then  $N(tx) = n$ .  
 $\rightsquigarrow T \times X_F \rightarrow X_F$ , making  $X_F$  a  $T$ -torsor.
- Fix a rat. pt.  $P \in X_F(F)$  to obtain  $\phi_P : X_F \xrightarrow{\sim} T$ , whose restriction to  $\mathbf{X}(o_{F_p})$  (int. local pts.) has image in  $\mathbb{I}_E$  (**idèle group**).
- The composition  $\tilde{f}_E : \prod_{\mathfrak{p}} \mathbf{X}(o_{F_p}) \rightarrow \mathbb{I}_E \xrightarrow{\times^P} \mathbb{I}_E$  whose  $\mathfrak{p}$ -component is

$$\tilde{f}_E[(x_p, y_p)] = \begin{cases} (\tilde{x}_p + \sqrt{-d}\tilde{y}_p, \tilde{x}_p - \sqrt{-d}\tilde{y}_p) \in E_{\mathfrak{q}\mathfrak{p}} \times E_{\mathfrak{q}\mathfrak{p}} & , \text{ if } \mathfrak{p} = \mathfrak{q}\mathfrak{p} \text{ splits in } E/F, \\ \tilde{x}_p + \sqrt{-d}\tilde{y}_p \in E_{\mathfrak{q}\mathfrak{p}} & , \text{ otherwise,} \end{cases}$$

where  $\mathfrak{q}$  and  $\mathfrak{p}$  (resp.  $\mathfrak{q}$ ) are places of  $E$  above  $\mathfrak{p}$  and  $\tilde{x}_p = ax_p + \frac{b}{2}y_p$ ,  $\tilde{y}_p = y_p$ .



# Torsors under norm-one tori

- Let  $T = \ker(R_{E/F}(\mathbb{G}_{m,E}) \xrightarrow{N_{E/F}} \mathbb{G}_{m,F})$  (called **norm-one torus**), and  $X_F = X \times_{o_F} F$  the generic fiber.
- Intuition: if  $N(t) = 1$  and  $N(x) = n$  then  $N(tx) = n$ .  
 $\rightsquigarrow T \times X_F \rightarrow X_F$ , making  $X_F$  a  $T$ -torsor.
- Fix a rat. pt.  $P \in X_F(F)$  to obtain  $\phi_P : X_F \xrightarrow{\sim} T$ , whose restriction to  $\mathbf{X}(o_{F_p})$  (int. local pts.) has image in  $\mathbb{I}_E$  (idèle group).
- The composition  $\tilde{f}_E : \prod_{\mathfrak{p}} \mathbf{X}(o_{F_p}) \rightarrow \mathbb{I}_E \xrightarrow{\times P} \mathbb{I}_E$  whose  $\mathfrak{p}$ -component is

$$\tilde{f}_E[(x_p, y_p)] = \begin{cases} (\tilde{x}_p + \sqrt{-d}\tilde{y}_p, \tilde{x}_p - \sqrt{-d}\tilde{y}_p) \in E_{\mathfrak{q}_3} \times E_{\mathfrak{q}_3} & , \text{ if } \mathfrak{p} = \mathfrak{q}_3\bar{\mathfrak{q}}_3 \text{ splits in } E/F, \\ \tilde{x}_p + \sqrt{-d}\tilde{y}_p \in E_{\mathfrak{q}_3} & , \text{ otherwise,} \end{cases}$$

where  $\mathfrak{q}_3$  and  $\bar{\mathfrak{q}}_3$  (resp.  $\mathfrak{q}_3$ ) are places of  $E$  above  $\mathfrak{p}$  and  $\tilde{x}_p = ax_p + \frac{b}{2}y_p$ ,  $\tilde{y}_p = y_p$ .

# The sign func. and the positive open subgroup

- Let  $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d} \subseteq \mathfrak{o}_E$  an order, with completion  $L_{\mathfrak{p}} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_{\mathfrak{p}}}$  at  $\mathfrak{p}$ .
- Let  $\mathfrak{p}_{\infty} = 1/t$  be the place of  $k(t)$  at  $\infty$  and  $\mathfrak{P}_{\infty}$  the unique place in  $E$  above  $\mathfrak{p}_{\infty}$ .
- Fix a **sign function**  $\text{sgn} : E_{\mathfrak{P}_{\infty}} \rightarrow \mathfrak{o}_{E_{\mathfrak{P}_{\infty}}}/\mathfrak{P}_{\infty}$  (taking the first non-zero coeff. of the Laurent expansion), and take all the **positive** elements  $E_{\mathfrak{P}_{\infty}}^+ = \{\alpha \in E_{\mathfrak{P}_{\infty}}^{\times} \mid \text{sgn}(\alpha) = 1\} \subseteq E_{\mathfrak{P}_{\infty}}^{\times}$ .
- $\rightsquigarrow$  an open subgp.  $\Xi_{\mathfrak{P}_{\infty}}^+ = E_{\mathfrak{P}_{\infty}}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{P}_{\infty}} L_{\mathfrak{p}}^{\times} \subseteq \mathbb{I}_E$ .

# The sign func. and the positive open subgroup

- Let  $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d} \subseteq \mathfrak{o}_E$  an order, with completion  $L_{\mathfrak{p}} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_{\mathfrak{p}}}$  at  $\mathfrak{p}$ .
- Let  $\mathfrak{p}_{\infty} = 1/t$  be the place of  $k(t)$  at  $\infty$  and  $\mathfrak{P}_{\infty}$  the unique place in  $E$  above  $\mathfrak{p}_{\infty}$ .
- Fix a **sign function**  $\text{sgn} : E_{\mathfrak{P}_{\infty}} \rightarrow \mathfrak{o}_{E_{\mathfrak{P}_{\infty}}}/\mathfrak{P}_{\infty}$  (taking the first non-zero coeff. of the Laurent expansion), and take all the **positive** elements  $E_{\mathfrak{P}_{\infty}}^+ = \{\alpha \in E_{\mathfrak{P}_{\infty}}^{\times} \mid \text{sgn}(\alpha) = 1\} \subseteq E_{\mathfrak{P}_{\infty}}^{\times}$ .
- $\rightsquigarrow$  an open subgp.  $\Xi_{\mathfrak{P}_{\infty}}^+ = E_{\mathfrak{P}_{\infty}}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{P}_{\infty}} L_{\mathfrak{p}}^{\times} \subseteq \mathbb{I}_E$ .

# The sign func. and the positive open subgroup

- Let  $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d} \subseteq \mathfrak{o}_E$  an order, with completion  $L_{\mathfrak{p}} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_{\mathfrak{p}}}$  at  $\mathfrak{p}$ .
- Let  $\mathfrak{p}_{\infty} = 1/t$  be the place of  $k(t)$  at  $\infty$  and  $\mathfrak{P}_{\infty}$  the unique place in  $E$  above  $\mathfrak{p}_{\infty}$ .
- Fix a **sign function**  $\text{sgn} : E_{\mathfrak{P}_{\infty}} \rightarrow \mathfrak{o}_{E_{\mathfrak{P}_{\infty}}}/\mathfrak{P}_{\infty}$  (taking the first non-zero coeff. of the Laurent expansion), and take all the **positive** elements  $E_{\mathfrak{P}_{\infty}}^+ = \{\alpha \in E_{\mathfrak{P}_{\infty}}^{\times} \mid \text{sgn}(\alpha) = 1\} \subseteq E_{\mathfrak{P}_{\infty}}^{\times}$ .
- $\rightsquigarrow$  an open subgp.  $\Xi_{\mathfrak{P}_{\infty}}^+ = E_{\mathfrak{P}_{\infty}}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{P}_{\infty}} L_{\mathfrak{p}}^{\times} \subseteq \mathbb{I}_E$ .

# The sign func. and the positive open subgroup

- Let  $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d} \subseteq \mathfrak{o}_E$  an order, with completion  $L_{\mathfrak{p}} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_{\mathfrak{p}}}$  at  $\mathfrak{p}$ .
- Let  $\mathfrak{p}_{\infty} = 1/t$  be the place of  $k(t)$  at  $\infty$  and  $\mathfrak{P}_{\infty}$  the unique place in  $E$  above  $\mathfrak{p}_{\infty}$ .
- Fix a **sign function**  $\text{sgn} : E_{\mathfrak{P}_{\infty}} \rightarrow \mathfrak{o}_{E_{\mathfrak{P}_{\infty}}}/\mathfrak{P}_{\infty}$  (taking the first non-zero coeff. of the Laurent expansion), and take all the **positive** elements  $E_{\mathfrak{P}_{\infty}}^+ = \{\alpha \in E_{\mathfrak{P}_{\infty}}^{\times} \mid \text{sgn}(\alpha) = 1\} \subseteq E_{\mathfrak{P}_{\infty}}^{\times}$ .
- $\rightsquigarrow$  an open subgp.  $\Xi_{\mathfrak{P}_{\infty}}^+ = E_{\mathfrak{P}_{\infty}}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{p}_{\infty}} L_{\mathfrak{p}}^{\times} \subseteq \mathbb{I}_E$ .

# Existence of int. pts. of $\mathbf{X}$ (main result)

Theorem 2.1 ([Lv, 2020], **func. field analog** to [Lv et al., 2018])

Notations above, we have

- (a) The open subgrp.  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  is of finite index in  $\mathbb{I}_E$ .
- (b) Let  $K_{\mathfrak{p}_\infty}^+$  be the class field corresp. to  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  (called the **narrow ring class field**) and  $\psi_{K_{\mathfrak{p}_\infty}^+/E} : \mathbb{I}_E \rightarrow \text{Gal}(K_{\mathfrak{p}_\infty}^+/E)$  the Artin map. Then  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$  if and only if
- there exists a local solution  $\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  (**local condition**) s.t.
  - $\psi_{K_{\mathfrak{p}_\infty}^+/E}(\tilde{r}_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1$  (**Artin condition**).

- Calculate to obtain Examples 1.1 and 1.3.

# Existence of int. pts. of $\mathbf{X}$ (main result)

Theorem 2.1 ([Lv, 2020], **func. field analog** to [Lv et al., 2018])

Notations above, we have

- (a) The open subgrp.  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  is of finite index in  $\mathbb{I}_E$ .
- (b) Let  $K_{\mathfrak{p}_\infty}^+$  be the class field corresp. to  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  (called the **narrow ring class field**) and  $\psi_{K_{\mathfrak{p}_\infty}^+/E} : \mathbb{I}_E \rightarrow \text{Gal}(K_{\mathfrak{p}_\infty}^+/E)$  the Artin map. Then  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$  if and only if
- there exists a local solution  $\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  (**local condition**) s.t.
  - $\psi_{K_{\mathfrak{p}_\infty}^+/E}(\tilde{f}_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1$  (**Artin condition**).

- Calculate to obtain Examples 1.1 and 1.3.

# Existence of int. pts. of $\mathbf{X}$ (main result)

Theorem 2.1 ([Lv, 2020], **func. field analog** to [Lv et al., 2018])

Notations above, we have

- (a) The open subgrp.  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  is of finite index in  $\mathbb{I}_E$ .
- (b) Let  $K_{\mathfrak{p}_\infty}^+$  be the class field corresp. to  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  (called the **narrow ring class field**) and  $\psi_{K_{\mathfrak{p}_\infty}^+/E} : \mathbb{I}_E \rightarrow \text{Gal}(K_{\mathfrak{p}_\infty}^+/E)$  the Artin map. Then  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$  if and only if
- there exists a local solution  $\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  (**local condition**) s.t.
  - $\psi_{K_{\mathfrak{p}_\infty}^+/E}(\tilde{f}_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1$  (**Artin condition**).

- Calculate to obtain Examples 1.1 and 1.3.



# Existence of int. pts. of $\mathbf{X}$ (main result)

Theorem 2.1 ([Lv, 2020], **func. field analog** to [Lv et al., 2018])

Notations above, we have

- (a) The open subgrp.  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  is of finite index in  $\mathbb{I}_E$ .
- (b) Let  $K_{\mathfrak{p}_\infty}^+$  be the class field corresp. to  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  (called the **narrow ring class field**) and  $\psi_{K_{\mathfrak{p}_\infty}^+/E} : \mathbb{I}_E \rightarrow \text{Gal}(K_{\mathfrak{p}_\infty}^+/E)$  the Artin map. Then  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$  if and only if
- there exists a local solution  $\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  (**local condition**) s.t.
  - $\psi_{K_{\mathfrak{p}_\infty}^+/E}(\tilde{f}_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1$  (**Artin condition**).

- Calculate to obtain Examples 1.1 and 1.3.

# Existence of int. pts. of $\mathbf{X}$ (main result)

Theorem 2.1 ([Lv, 2020], **func. field analog** to [Lv et al., 2018])

Notations above, we have

- (a) The open subgrp.  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  is of finite index in  $\mathbb{I}_E$ .
- (b) Let  $K_{\mathfrak{p}_\infty}^+$  be the class field corresp. to  $E^\times \Xi_{\mathfrak{p}_\infty}^+$  (called the **narrow ring class field**) and  $\psi_{K_{\mathfrak{p}_\infty}^+/E} : \mathbb{I}_E \rightarrow \text{Gal}(K_{\mathfrak{p}_\infty}^+/E)$  the Artin map. Then  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$  if and only if
- there exists a local solution  $\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  (**local condition**) s.t.
  - $\psi_{K_{\mathfrak{p}_\infty}^+/E}(\tilde{f}_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1$  (**Artin condition**).

- Calculate to obtain Examples 1.1 and 1.3.

# Ideas of the proof

- Replace  $L$  by  $\mathfrak{o}_E \rightsquigarrow \Xi_{\mathfrak{p}_\infty}^+$  by  $\tilde{\Xi}_{\mathfrak{p}_\infty}^+ = E_{\mathfrak{p}_\infty}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$   
 $\Rightarrow E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite.
- But  $\mathbb{I}_E / E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ \cong Cl^+(\mathfrak{o}_E)$  is the **narrow class gp.**, which is finite [Goss, 1996]  $\Rightarrow \mathbb{I}_E / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite (**shows (a)**).
- Replace  $E_{\mathfrak{p}_\infty}^+$  by  $E_{\mathfrak{p}_\infty}^\times \rightsquigarrow \tilde{\Xi}_{\mathfrak{p}_\infty}^+$  by  $\Xi_{\mathfrak{p}_\infty} = E_{\mathfrak{p}_\infty}^\times \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$ .  
 Call the corresp.  $K_{\mathfrak{p}_\infty}$  **Hilbert class field**.
- The int. model  $\mathbf{T} = \text{Spec}(\mathfrak{o}_F[x, y]/(x^2 + dy^2 - 1))$  of  $T$  is so that  $\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$  acts stably on  $\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  for all  $\mathfrak{p}$ .
- Use [Wei and Xu, 2012] and exploit the properties of  $\text{sgn}$  and the def. of  $E_{\mathfrak{p}_\infty}^+$  (**shows (b)**).

# Ideas of the proof

- Replace  $L$  by  $\mathfrak{o}_E \rightsquigarrow \Xi_{\mathfrak{p}_\infty}^+$  by  $\tilde{\Xi}_{\mathfrak{p}_\infty}^+ = E_{\mathfrak{p}_\infty}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$   
 $\Rightarrow E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite.
- But  $\mathbb{I}_E / E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ \cong CI^+(\mathfrak{o}_E)$  is the **narrow class gp.**, which is finite [Goss, 1996]  $\Rightarrow \mathbb{I}_E / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite (**shows (a)**).
- Replace  $E_{\mathfrak{p}_\infty}^+$  by  $E_{\mathfrak{p}_\infty}^\times \rightsquigarrow \tilde{\Xi}_{\mathfrak{p}_\infty}^+$  by  $\Xi_{\mathfrak{p}_\infty}^\times = E_{\mathfrak{p}_\infty}^\times \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$ .  
 Call the corresp.  $K_{\mathfrak{p}_\infty}$  **Hilbert class field**.
- The int. model  $\mathbf{T} = \text{Spec}(\mathfrak{o}_F[x, y]/(x^2 + dy^2 - 1))$  of  $T$  is so that  $\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$  acts stably on  $\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  for all  $\mathfrak{p}$ .
- Use [Wei and Xu, 2012] and exploit the properties of  $\text{sgn}$  and the def. of  $E_{\mathfrak{p}_\infty}^+$  (**shows (b)**).

# Ideas of the proof

- Replace  $L$  by  $\mathfrak{o}_E \rightsquigarrow \Xi_{\mathfrak{p}_\infty}^+$  by  $\tilde{\Xi}_{\mathfrak{p}_\infty}^+ = E_{\mathfrak{p}_\infty}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$   
 $\Rightarrow E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite.
- But  $\mathbb{I}_E / E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ \cong CI^+(\mathfrak{o}_E)$  is the **narrow class gp.**, which is finite [Goss, 1996]  $\Rightarrow \mathbb{I}_E / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite (**shows (a)**).
- Replace  $E_{\mathfrak{p}_\infty}^+$  by  $E_{\mathfrak{p}_\infty}^\times \rightsquigarrow \tilde{\Xi}_{\mathfrak{p}_\infty}^+$  by  $\Xi_{\mathfrak{p}_\infty}^\times = E_{\mathfrak{p}_\infty}^\times \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$ .  
 Call the corresp.  $K_{\mathfrak{p}_\infty}$  **Hilbert class field**.
- The int. model  $\mathbf{T} = \text{Spec}(\mathfrak{o}_F[x, y]/(x^2 + dy^2 - 1))$  of  $T$  is so that  $\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$  acts stably on  $\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  for all  $\mathfrak{p}$ .
- Use [Wei and Xu, 2012] and exploit the properties of  $\text{sgn}$  and the def. of  $E_{\mathfrak{p}_\infty}^+$  (**shows (b)**).

# Ideas of the proof

- Replace  $L$  by  $\mathfrak{o}_E \rightsquigarrow \Xi_{\mathfrak{p}_\infty}^+$  by  $\tilde{\Xi}_{\mathfrak{p}_\infty}^+ = E_{\mathfrak{p}_\infty}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$   
 $\Rightarrow E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite.
- But  $\mathbb{I}_E / E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ \cong CI^+(\mathfrak{o}_E)$  is the **narrow class gp.**, which is finite [Goss, 1996]  $\Rightarrow \mathbb{I}_E / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite (**shows (a)**).
- Replace  $E_{\mathfrak{p}_\infty}^+$  by  $E_{\mathfrak{p}_\infty}^\times \rightsquigarrow \tilde{\Xi}_{\mathfrak{p}_\infty}^+$  by  $\Xi_{\mathfrak{p}_\infty}^\times = E_{\mathfrak{p}_\infty}^\times \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$ .  
 Call the corresp.  $K_{\mathfrak{p}_\infty}$  **Hilbert class field**.
- The int. model  $\mathbf{T} = \text{Spec}(\mathfrak{o}_F[x, y]/(x^2 + dy^2 - 1))$  of  $T$  is so that  $\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$  acts stably on  $\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  for all  $\mathfrak{p}$ .
- Use [Wei and Xu, 2012] and exploit the properties of  $\text{sgn}$  and the def. of  $E_{\mathfrak{p}_\infty}^+$  (**shows (b)**).

# Ideas of the proof

- Replace  $L$  by  $\mathfrak{o}_E \rightsquigarrow \Xi_{\mathfrak{p}_\infty}^+$  by  $\tilde{\Xi}_{\mathfrak{p}_\infty}^+ = E_{\mathfrak{p}_\infty}^+ \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$   
 $\Rightarrow E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite.
- But  $\mathbb{I}_E / E^\times \tilde{\Xi}_{\mathfrak{p}_\infty}^+ \cong Cl^+(\mathfrak{o}_E)$  is the **narrow class gp.**, which is finite [Goss, 1996]  $\Rightarrow \mathbb{I}_E / E^\times \Xi_{\mathfrak{p}_\infty}^+$  is finite (**shows (a)**).
- Replace  $E_{\mathfrak{p}_\infty}^+$  by  $E_{\mathfrak{p}_\infty}^\times \rightsquigarrow \tilde{\Xi}_{\mathfrak{p}_\infty}^+$  by  $\Xi_{\mathfrak{p}_\infty} = E_{\mathfrak{p}_\infty}^\times \times \prod_{\mathfrak{p} \neq \mathfrak{p}_\infty} \mathfrak{o}_{E_{\mathfrak{p}}}^\times$ .  
 Call the corresp.  $K_{\mathfrak{p}_\infty}$  **Hilbert class field**.
- The int. model  $\mathbf{T} = \text{Spec}(\mathfrak{o}_F[x, y]/(x^2 + dy^2 - 1))$  of  $T$  is so that  $\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$  acts stably on  $\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  for all  $\mathfrak{p}$ .
- Use [Wei and Xu, 2012] and exploit the properties of  $\text{sgn}$  and the def. of  $E_{\mathfrak{p}_\infty}^+$  (**shows (b)**).

# Outline

- 1 **Problem:** is  $ax^2 + bxy + cy^2 + g = 0$  solvable over  $\mathbb{F}_q[t]$  ?
- 2 **Solution:** torsors under norm-one tori + class field theory
- 3 **Application:** primes of the form  $x^2 + Dy^2$  in  $\mathbb{F}_q[t]$



Primes of the form  $x^2 + Dy^2$  in  $k[t]$ 

- Let  $D \in k[t]$  be sqr. free with positive deg.,  $l \nmid D$  irr., and consider  $l = x^2 + Dy^2$  over  $k[t]$ .
- Suppose that  $\deg D$  is odd or  $\text{lc}(-D) \notin k^{\times 2}$ , which is to say  $E = F(\sqrt{-D})/F$  is imaginary [Rosen, 2013].
- Then a necessary cond. for int. solvability is

$\deg l$  is even if  $\deg D$  is,

which we will always assume.

- Let  $d_\infty$  be the relative deg. of  $\mathfrak{P}_\infty \mid \mathfrak{p}_\infty$ ,  $\deg^* l = \frac{\deg l}{d_\infty} \in \mathbb{Z}_{>0}$  and choose  $\text{sgn}$  w.r.t the uniformizer  $t^g / \sqrt{-D}$  ( $g$  the genus of  $E$ ).

Primes of the form  $x^2 + Dy^2$  in  $k[t]$ 

- Let  $D \in k[t]$  be sqr. free with positive deg.,  $l \nmid D$  irr., and consider  $l = x^2 + Dy^2$  over  $k[t]$ .
- Suppose that  $\deg D$  is odd or  $\text{lc}(-D) \notin k^{\times 2}$ , which is to say  $E = F(\sqrt{-D})/F$  is imaginary [Rosen, 2013].
- Then a necessary cond. for int. solvability is

$\deg l$  is even if  $\deg D$  is,

which we will always assume.

- Let  $d_\infty$  be the relative deg. of  $\mathfrak{P}_\infty \mid \mathfrak{p}_\infty$ ,  $\deg^* l = \frac{\deg l}{d_\infty} \in \mathbb{Z}_{>0}$  and choose  $\text{sgn}$  w.r.t the uniformizer  $t^g/\sqrt{-D}$  ( $g$  the genus of  $E$ ).

Primes of the form  $x^2 + Dy^2$  in  $k[t]$ 

- Let  $D \in k[t]$  be sqr. free with positive deg.,  $l \nmid D$  irr., and consider  $l = x^2 + Dy^2$  over  $k[t]$ .
- Suppose that  $\deg D$  is odd or  $\text{lc}(-D) \notin k^{\times 2}$ , which is to say  $E = F(\sqrt{-D})/F$  is imaginary [Rosen, 2013].
- Then a necessary cond. for int. solvability is

$\deg l$  is even if  $\deg D$  is,

which we will always assume.

- Let  $d_\infty$  be the relative deg. of  $\mathfrak{P}_\infty \mid \mathfrak{p}_\infty$ ,  $\deg^* l = \frac{\deg l}{d_\infty} \in \mathbb{Z}_{>0}$  and choose  $\text{sgn}$  w.r.t the uniformizer  $t^g/\sqrt{-D}$  ( $g$  the genus of  $E$ ).

Primes of the form  $x^2 + Dy^2$  in  $k[t]$ 

- Let  $D \in k[t]$  be sqr. free with positive deg.,  $l \nmid D$  irr., and consider  $l = x^2 + Dy^2$  over  $k[t]$ .
- Suppose that  $\deg D$  is odd or  $\text{lc}(-D) \notin k^{\times 2}$ , which is to say  $E = F(\sqrt{-D})/F$  is imaginary [Rosen, 2013].
- Then a necessary cond. for int. solvability is

$\deg l$  is even if  $\deg D$  is,

which we will always assume.

- Let  $d_\infty$  be the relative deg. of  $\mathfrak{P}_\infty \mid \mathfrak{p}_\infty$ ,  $\deg^* l = \frac{\deg l}{d_\infty} \in \mathbb{Z}_{>0}$  and choose  $\text{sgn}$  w.r.t the uniformizer  $t^g/\sqrt{-D}$  ( $g$  the genus of  $E$ ).

# Extending a result of Maciak

Corollary ([Lv, 2020], **extends** [Maciak, 2011])

Notations and assumptions above, we have

(a) if  $\text{sgn}(l)(-1)^{\deg^* l} \in k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if

- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$  and
- $l$  splits completely in  $K_{\mathfrak{p}_\infty}^+$ ;

(b) if  $\text{sgn}(l)(-1)^{\deg^* l} \notin k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if

- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$ ,
- $l$  splits completely in  $K_{\mathfrak{p}_\infty}$  and
- the relative deg. of  $l$  in  $K_{\mathfrak{p}_\infty}^+$  is 2.

- To show it, use the Thm. 2.1 and calculate the Artin cond.

# Extending a result of Maciak

Corollary ([Lv, 2020], **extends** [Maciak, 2011])

Notations and assumptions above, we have

(a) if  $\text{sgn}(l)(-1)^{\deg^* l} \in k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if

- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$  and
- $l$  splits completely in  $K_{\mathfrak{p}_\infty}^+$ ;

(b) if  $\text{sgn}(l)(-1)^{\deg^* l} \notin k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if

- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$ ,
- $l$  splits completely in  $K_{\mathfrak{p}_\infty}$  and
- the relative deg. of  $l$  in  $K_{\mathfrak{p}_\infty}^+$  is 2.

- To show it, use the Thm. 2.1 and calculate the Artin cond.

# Extending a result of Maciak

Corollary ([Lv, 2020], **extends** [Maciak, 2011])

Notations and assumptions above, we have

(a) if  $\text{sgn}(l)(-1)^{\deg^* l} \in k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if

- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$  and
- $l$  splits completely in  $K_{\mathfrak{p}_\infty}^+$ ;

(b) if  $\text{sgn}(l)(-1)^{\deg^* l} \notin k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if

- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$ ,
- $l$  splits completely in  $K_{\mathfrak{p}_\infty}$  and
- the relative deg. of  $l$  in  $K_{\mathfrak{p}_\infty}^+$  is 2.

- To show it, use the Thm. 2.1 and calculate the Artin cond.

# Extending a result of Maciak

Corollary ([Lv, 2020], **extends** [Maciak, 2011])

Notations and assumptions above, we have

- (a) if  $\text{sgn}(l)(-1)^{\deg^* l} \in k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if
- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$  and
  - $l$  splits completely in  $K_{\mathfrak{p}_\infty}^+$ ;
- (b) if  $\text{sgn}(l)(-1)^{\deg^* l} \notin k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if
- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$ ,
  - $l$  splits completely in  $K_{\mathfrak{p}_\infty}$  and
  - the relative deg. of  $l$  in  $K_{\mathfrak{p}_\infty}^+$  is 2.

- To show it, use the Thm. 2.1 and calculate the Artin cond.



# Extending a result of Maciak

Corollary ([Lv, 2020], **extends** [Maciak, 2011])

Notations and assumptions above, we have

- (a) if  $\text{sgn}(l)(-1)^{\deg^* l} \in k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if
- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$  and
  - $l$  splits completely in  $K_{\mathfrak{p}_\infty}^+$ ;
- (b) if  $\text{sgn}(l)(-1)^{\deg^* l} \notin k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if
- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$ ,
  - $l$  splits completely in  $K_{\mathfrak{p}_\infty}$  and
  - the relative deg. of  $l$  in  $K_{\mathfrak{p}_\infty}^+$  is 2.

- To show it, use the Thm. 2.1 and calculate the Artin cond.

# Extending a result of Maciak

Corollary ([Lv, 2020], **extends** [Maciak, 2011])

Notations and assumptions above, we have

- (a) if  $\text{sgn}(l)(-1)^{\deg^* l} \in k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if
- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$  and
  - $l$  splits completely in  $K_{\mathfrak{p}_\infty}^+$ ;
- (b) if  $\text{sgn}(l)(-1)^{\deg^* l} \notin k^{\times 2}$ , then  $l = x^2 + Dy^2$  is solvable over  $k[t]$  if and only if
- $\left(\frac{l}{r}\right) = 1$  for each monic irr. factor  $r \mid D$ ,
  - $l$  splits completely in  $K_{\mathfrak{p}_\infty}$  and
  - the relative deg. of  $l$  in  $K_{\mathfrak{p}_\infty}^+$  is 2.

- To show it, use the Thm. 2.1 and calculate the Artin cond.

# Outline revisited

Thanks for your attention.

- 1 Problem:** is  $ax^2 + bxy + cy^2 + g = 0$  solvable over  $\mathbb{F}_q[t]$  ?
- 2 Solution:** torsors under norm-one tori + class field theory
- 3 Application:** primes of the form  $x^2 + Dy^2$  in  $\mathbb{F}_q[t]$