# Elliptic curves and number fields

$$E : y^2 = x^3 + x + 745$$

**Theorem.**

*Let $nf$ be a number field. The set of rational points $E(nf)$ is an abelian group*

**Theorem.**

*Let* $nf$ *be a number field. The set of rational points* $E(nf)$ *is an abelian group*

finitely generated

**Theorem.**

*Let* $nf$ *be a number field. The set of rational points* $E(nf)$ *is an abelian group*

finitely generated

*of the form*

$$\mathbf{E}(\mathbf{nf}) = (\mathbb{Z}/\mathbf{m}\mathbb{Z}) \times (\mathbb{Z}/\mathbf{n}\mathbb{Z}) \times \mathbb{Z}^{\mathbf{r}}$$

$$\mathbf{E}(\mathbf{nf}) = (\mathbb{Z}/\mathbf{m}\mathbb{Z}) \times (\mathbb{Z}/\mathbf{n}\mathbb{Z}) \times \mathbb{Z}^{\mathbf{r}}$$

elltors($\mathbf{E}$): $\quad \mathbf{nf} = \mathbb{Q} : \mathbf{m} = \mathbf{n} = \mathbf{1}$

$$\mathbf{E(nf)} = (\mathbb{Z}/\mathbf{m}\mathbb{Z}) \times (\mathbb{Z}/\mathbf{n}\mathbb{Z}) \times \mathbb{Z}^{\mathbf{r}}$$

elltors($\mathbf{E}$): $\mathbf{nf} = \mathbb{Q} : \mathbf{m} = \mathbf{n} = \mathbf{1}$

elltorsnf($\mathbf{E}$): missing

$$\mathbf{E}(\mathbf{nf}) = (\mathbb{Z}/\mathbf{m}\mathbb{Z}) \times (\mathbb{Z}/\mathbf{n}\mathbb{Z}) \times \mathbb{Z}^{\mathbf{r}}$$

elltors($\mathbf{E}$): $\quad \mathbf{nf} = \mathbb{Q} : \mathbf{m} = \mathbf{n} = \mathbf{1}$

elltorsnf($\mathbf{E}$): missing

Algo :

- Reduce modulo a few degree 1 primes $\mathfrak{p}_i$
- Compute the number of points mod $\mathfrak{p}_i =$ mod $p$.
- Find a small bound on $mn \mid B$
- `nffactor(nf,elldivpol(E,b))` for prime powers $b \mid B$.

By brute force, we find $\mathbf{P(-8, 15)} \in \mathbf{E}(\mathbb{Q})$

By brute force, we find $\mathbf{P(-8,15)} \in \mathbf{E}(\mathbb{Q})$

Given a polynomial $pol(x,y)$, need a function `bruteforce(pol,B)` that finds (rational) solutions of $pol(x,y)=0$ with height $\leqslant B$.

By brute force, we find $\mathbf{P}(-\mathbf{8}, \mathbf{15}) \in \mathbf{E}(\mathbb{Q})$

Given a polynomial $pol(x, y)$, need a function `bruteforce(pol,B)` that finds (rational) solutions of $pol(x, y) = 0$ with height $\leqslant B$. Similarly `nfbruteforce(nf,pol,B)`.

By brute force, we find $\mathbf{P}(-\mathbf{8}, \mathbf{15}) \in \mathbf{E}(\mathbb{Q})$

Given a polynomial $pol(x, y)$, need a function `bruteforce(pol,B)` that finds (rational) solutions of $pol(x, y) = 0$ with height $\leqslant B$.
Similarly `nfbruteforce(nf,pol,B)`.

The hyperelliptic case is of specific interest: $pol(x, y) = y^2 - F(x)$
$\rightarrow$ `hyperbruteforce(F,B)`.

By brute force, we find $\mathbf{P(-8, 15)} \in \mathbf{E}(\mathbb{Q})$

Given a polynomial $pol(x, y)$, need a function `bruteforce(pol,B)` that finds (rational) solutions of $pol(x, y) = 0$ with height $\leqslant B$.
Similarly `nfbruteforce(nf,pol,B)`.

The hyperelliptic case is of specific interest: $pol(x, y) = y^2 - F(x)$
$\rightarrow$ `hyperbruteforce(F,B)`.
Similarly `nfhyperbruteforce(nf,F,B)`.

# 2-DESCENT

Let $\theta$ be a root of $x^3 + x + 745$ and $K = \mathbb{Q}(\theta)$.

# 2-DESCENT

Let $\theta$ be a root of $x^3 + x + 745$ and $K = \mathbb{Q}(\theta)$.

If $P(x, y) \in E(\mathbb{Q})$, then

$$\begin{aligned} y^2 &= x^3 + x + 745 \\ &= (x - \theta)\left(F'(\theta) + \tfrac{1}{2}F''(\theta)(x - \theta) + (x - \theta)^2\right) \\ &= \mathcal{N}_{K/\mathbb{Q}}(x - \theta) \end{aligned}$$

# 2-DESCENT

Let $\theta$ be a root of $x^3 + x + 745$ and $K = \mathbb{Q}(\theta)$.

If $P(x, y) \in E(\mathbb{Q})$, then

$$\begin{aligned} y^2 &= x^3 + x + 745 \\ &= (x - \theta)\left(F'(\theta) + \tfrac{1}{2}F''(\theta)(x - \theta) + (x - \theta)^2\right) \\ &= \mathcal{N}_{K/\mathbb{Q}}(x - \theta) \end{aligned}$$

Hence

$$(x - \theta)\mathbb{Z}_K = D \cdot J^2$$

where $J$ isi an ideal and $D$ is in a finite set:

$x - \theta$ is almost a square.

# UNITS AND CLASS GROUPS

$S$ a small finite set of primes.

We need to consider

$$K_{S,2} = \{\delta \in K^*/(K^*)^2 \mid \delta\mathbb{Z}_{K,S} = J^2\}$$

# UNITS AND CLASS GROUPS

$S$ a small finite set of primes.

We need to consider

$$K_{S,2} = \{\delta \in K^*/(K^*)^2 \mid \delta\mathbb{Z}_{K,S} = J^2\}$$

**Property.**

*$K_{S,2}$ satisfies*

$$1 \longrightarrow \mathbb{U}_{K,S}/(\mathbb{U}_{K,S})^2 \longrightarrow K_{S,2} \longrightarrow Cl_S(K)[2] \longrightarrow 1$$

# UNITS AND CLASS GROUPS

$S$ a small finite set of primes.

We need to consider

$$K_{S,2} = \{\delta \in K^*/(K^*)^2 \mid \delta \mathbb{Z}_{K,S} = J^2\}$$

**Property.**

*$K_{S,2}$ satisfies*

$$1 \longrightarrow \mathbb{U}_{K,S}/(\mathbb{U}_{K,S})^2 \longrightarrow K_{S,2} \longrightarrow Cl_S(K)[2] \longrightarrow 1$$

$\rightarrow$ `bnfsunit(bnf,S)`

# 2-DESCENT

For each $\delta \in K_{S,2}$, we need to solve

$$\begin{cases} \mathcal{N}_{K/\mathbb{Q}}(\delta) = \square \\ \delta z^2 = (x - \theta) \end{cases}$$

# 2-DESCENT

For each $\delta \in K_{S,2}$, we need to solve

$$\begin{cases} \mathcal{N}_{K/\mathbb{Q}}(\delta) = \square \\ \delta z^2 = (x - \theta) \end{cases}$$

Some elements of $K_{S,2}$ have to be discarded because of local conditions : $\rightarrow$ `nfsign()`

# QUADRATIC EQUATIONS

The equation becomes

$$\begin{aligned} x - \theta &= v(z_0 + z_1\theta + z_2\theta^2)^2 \\ &= q_0(z_0, z_1, z_2) + q_1(z_0, z_1, z_2)\theta + q_2(z_0, z_1, z_2)\theta^2 \end{aligned}$$

ie

$$\begin{cases} q_2(z_0, z_1, z_2) & = 0 \\ q_1(z_0, z_1, z_2) & = -1 \end{cases}$$

# QUADRATIC EQUATIONS

The equation becomes

$$\begin{aligned} x - \theta &= v(z_0 + z_1\theta + z_2\theta^2)^2 \\ &= q_0(z_0, z_1, z_2) + q_1(z_0, z_1, z_2)\theta + q_2(z_0, z_1, z_2)\theta^2 \end{aligned}$$

ie

$$\begin{cases} q_2(z_0, z_1, z_2) &= 0 \\ q_1(z_0, z_1, z_2) &= -1 \end{cases}$$

Find 1 solution of $q_2 = 0$: $\rightarrow$ `qfsolve(q2)`

Need `bnfqfsolve(bnf,q2)` (see `bnfisnorm()`)

# QUADRATIC EQUATIONS

The equation becomes

$$\begin{aligned} x - \theta &= v(z_0 + z_1\theta + z_2\theta^2)^2 \\ &= q_0(z_0, z_1, z_2) + q_1(z_0, z_1, z_2)\theta + q_2(z_0, z_1, z_2)\theta^2 \end{aligned}$$

ie

$$\begin{cases} q_2(z_0, z_1, z_2) & = 0 \\ q_1(z_0, z_1, z_2) & = -1 \end{cases}$$

Find 1 solution of $q_2 = 0$: $\rightarrow$ `qfsolve(q2)`

Need `bnfqfsolve(bnf,q2)` (see `bnfisnorm()`)

Parametrizing all solutions: $\rightarrow$ `qfparam(q2,sol)`

# QUADRATIC EQUATIONS

End : solve $q_1(param(U,V)) = -1$ ie

$$-Y^2 = aU^4 + bU^3V + cU^2V^2 + dUV^3 + eV^4$$

→ `hyperbruteforce(F,B)`.

→ `nfhyperbruteforce(nf,F,B)`.

# OTHER ell- FUNCTIONS

- ellreducepoints(ell,list_of_points)
- ellrelations(ell,list_of_points)
- elldivide(ell,point,p)