Individual Discrete Logarithm with Sublattice Reduction

Haetham AL ASWAD
and
Cécile PIERROT

Journées C2, Hendaye, 11 April 2022

A reduction problem

- $\log(T) \mod \ell$?

A reduction problem

- $\log(T) \mod \ell$?
- Let's find R such that:

A reduction problem

- $\log(T) \mod \ell$?
- Let's find R such that:
  - $\log(R) \equiv \log(T) \mod \ell$.

A reduction problem

- $\log(T) \mod \ell$?
- Let's find R such that:
  - $\log(R) \equiv \log(T) \mod \ell$.
  - $\log(R)$ easier to calculate.

Discrete logarithm in finite fields

Definition

Let $\mathbb{F}_{p^n}^*$ be the multiplicative groupe of a finite field with g a generator. For $T \in \mathbb{F}_{p^n}^*$, $T = g^k$,

Discrete logarithm in finite fields

Definition

Let $\mathbb{F}_{p^n}^*$ be the multiplicative groupe of a finite field with g a generator. For $T \in \mathbb{F}_{p^n}^*$, $T = g^k$,

$$\log_g(T) := k$$

Discrete logarithm in finite fields

Definition

Let $\mathbb{F}_{p^n}^*$ be the multiplicative groupe of a finite field with g a generator. For $T \in \mathbb{F}_{p^n}^*$, $T = g^k$,

$$\log_g(T) := k$$

Alice

Private key: $a \in [\![1, p^n - 1]\!]$
$K = B^a = g^{ab}$

$A = g^a$ →

← $B = g^b$

Bob

Private key : $b \in [\![1, p^n - 1]\!]$
$K = A^b = g^{ab}$

- Naive algorithm, Baby step Giant step, and Pollard-Rho are exponentiel in the input size: $\log(p^n)$.

- Naive algorithm, Baby step Giant step, and Pollard-Rho are exponentiel in the input size: $\log(p^n)$.
- The number field sieve (NFS) has a subexponential complexity.

$$L_{p^n}\left(\frac{1}{3}\right)$$

$$L_{p^n}(\alpha, c) = e^{(c+o(1))\log(p^n)^{\alpha}\log\log(p^n)^{1-\alpha}}$$

Steps of the Number Field Sieve

Steps of the Number Field Sieve

1. Polynomial selection.

Steps of the Number Field Sieve

1. Polynomial selection.
2. Sieving.

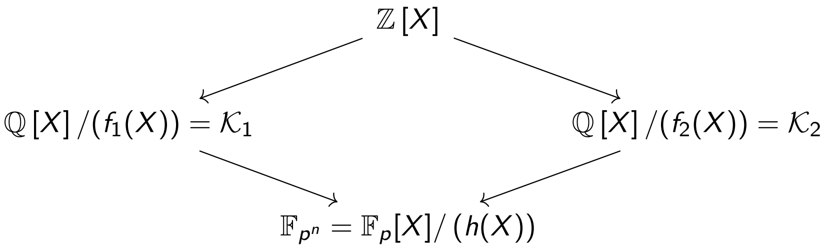
Steps of the Number Field Sieve

1. Polynomial selection.
2. Sieving.
3. Linear algebra.

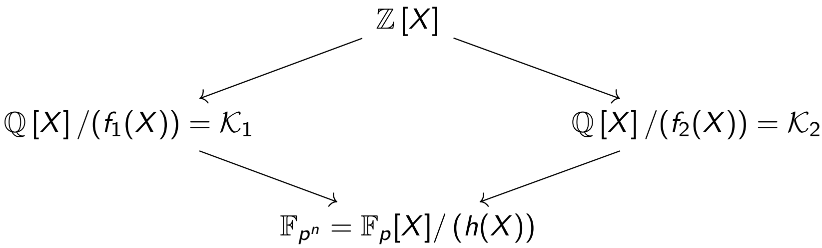
Steps of the Number Field Sieve

1. Polynomial selection.
2. Sieving.
3. Linear algebra.
4. **Individual Logarithm**.

1) Polynomial selection.



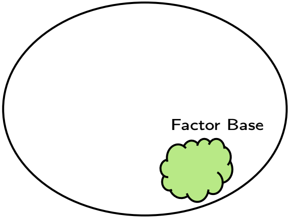
1) Polynomial selection.



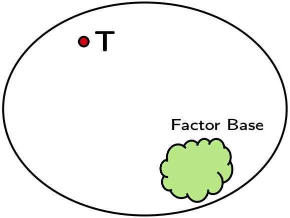
Why number fields?

In $\mathcal{K}_1$ we have

- A norm: $\mathcal{N} : \phi \mapsto |\text{resultant}(f_1, \phi)|$.
- Unique decomposition of ideals into prime ideals.

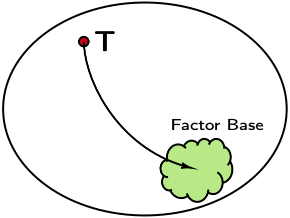


2), 3) **Sieve and linear algebra:** We know the logarithms of the factor base. .



2), 3) **Sieve and linear algebra:** We know the logarithms of the factor base. .

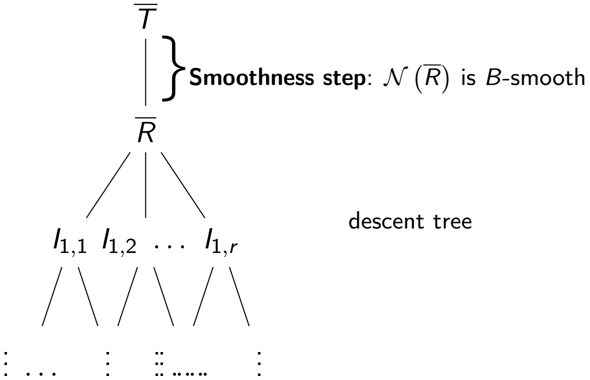
4) **Individual logarithm:**



2), 3) **Sieve and linear algebra:** We know the logarithms of the factor base. .

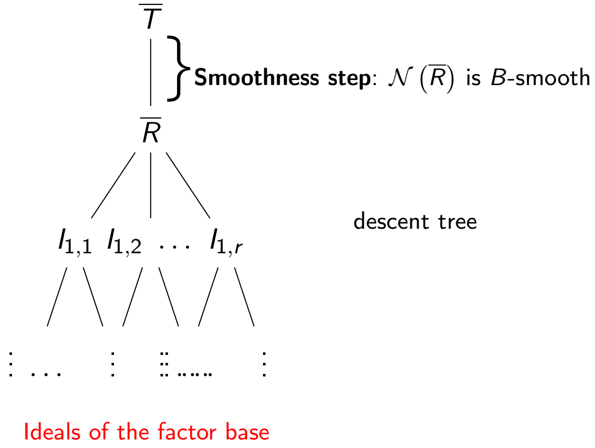
4) **Individual logarithm:** We decompose T into product of elements of the factor base.

Individual logarithm



descent tree

Individual logarithm



Our problem

Definition: B-smoothness

An integer is B-smooth if all its prime factors are below B.

Our problem

Definition: B-smoothness

An integer is B-smooth if all its prime factors are below B.

This work

- **Given:** $\mathbb{F}_{p^n}$ with n composite, d its greater proper divisor, B a smoothness bound, and a target $T \in \mathbb{F}_{p^n}^*$.

Our problem

Definition: B-smoothness

An integer is B-smooth if all its prime factors are below B.

This work

- **Given:** $\mathbb{F}_{p^n}$ with n composite, d its greater proper divisor, B a smoothness bound, and a target $T \in \mathbb{F}_{p^n}^*$.
- **Aim:** Find $\overline{R} \in \mathcal{K}_f$ such that:
  - $\log(R) \equiv \log(T) \mod \ell$. with ℓ a large prime divisor of the group order.
  - $\mathcal{N}(\overline{R})$ B-smooth.

Crucial lemma and [Guillevic 19]'s algorithm

Lemma

Let $U \in \mathbb{F}_{p^n}^{\times}$ *in a proper subfield of* $\mathbb{F}_{p^n}$*. Then* $\log(U) \equiv 0 \mod \ell$*.*

Crucial lemma and [Guillevic 19]'s algorithm

Lemma

Let $U \in \mathbb{F}_{p^n}^{\times}$ *in a proper subfield of* $\mathbb{F}_{p^n}$. *Then* $\log(U) \equiv 0 \mod \ell$.

Algorithm

- Compute $U = g^{\frac{p^n-1}{p^d-1}}$. Hence $\{1, U, \ldots, U^{d-1}\}$ is an $\mathbb{F}_p$ base of $\mathbb{F}_{p^d}$.

Crucial lemma and [Guillevic 19]'s algorithm

Lemma

Let $U \in \mathbb{F}_{p^n}^{\times}$ *in a proper subfield of* $\mathbb{F}_{p^n}$. *Then* $\log(U) \equiv 0 \mod \ell$.

Algorithm

- Compute $U = g^{\frac{p^n-1}{p^d-1}}$. Hence $\{1, U, \ldots, U^{d-1}\}$ is an $\mathbb{F}_p$ base of $\mathbb{F}_{p^d}$.
- $R \leftarrow LLL\left(\{T, UT, \ldots, U^{d-1}T\}\right)$.

Crucial lemma and [Guillevic 19]'s algorithm

Lemma

Let $U \in \mathbb{F}_{p^n}^{\times}$ *in a proper subfield of* $\mathbb{F}_{p^n}$*. Then* $\log(U) \equiv 0 \mod \ell$*.*

Algorithm

- Compute $U = g^{\frac{p^n-1}{p^d-1}}$. Hence $\{1, U, \ldots, U^{d-1}\}$ is an $\mathbb{F}_p$ base of $\mathbb{F}_{p^d}$.
- $R \leftarrow LLL\left(\{T, UT, \ldots, U^{d-1}T\}\right)$.
  - $\|R\|_\infty \leq 2^{\frac{n-1}{4}} p^{\frac{n-d}{n}}$
  - $\deg(R) = n - 1$.

Crucial lemma and [Guillevic 19]'s algorithm

Lemma

Let $U \in \mathbb{F}_{p^n}^{\times}$ in a proper subfield of $\mathbb{F}_{p^n}$. Then $\log(U) \equiv 0 \mod \ell$.

Algorithm

- Compute $U = g^{\frac{p^n-1}{p^d-1}}$. Hence $\{1, U, \ldots, U^{d-1}\}$ is an $\mathbb{F}_p$ base of $\mathbb{F}_{p^d}$.
- $R \leftarrow LLL\left(\{T, UT, \ldots, U^{d-1}T\}\right)$.
  - $\|R\|_\infty \leq 2^{\frac{n-1}{4}} p^{\frac{n-d}{n}}$
  - $\deg(R) = n - 1$.
- $\mathcal{N}\left(\overline{R}\right) = O\left(2^{n\frac{n-1}{4}} p^{(1+\zeta)n-d-\zeta}\right)$. Where $\zeta \in [0, 1]$ fixed by the polynomial selection.

The degree counts for $\mathcal{N}$

$$P = 1 + X + 3X^2 \in \mathcal{K}_f \qquad Q = 1 + X + 3X^{50} \in \mathcal{K}_f$$

The degree counts for $\mathcal{N}$

$$P = 1 + X + 3X^2 \in \mathcal{K}_f \qquad Q = 1 + X + 3X^{50} \in \mathcal{K}_f$$

- $\|P\|_\infty = \|Q\|_\infty$.
- $\|P\|_2 = \|Q\|_2$.

The degree counts for $\mathcal{N}$

$$P = 1 + X + 3X^2 \in \mathcal{K}_f \qquad Q = 1 + X + 3X^{50} \in \mathcal{K}_f$$

- $\|P\|_\infty = \|Q\|_\infty$.
- $\|P\|_2 = \|Q\|_2$.
- $\mathcal{N}(P) << \mathcal{N}(Q)$.

The degree counts for $\mathcal{N}$

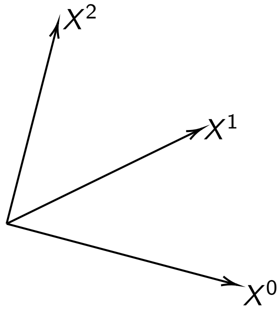
$$P = 1 + X + 3X^2 \in \mathcal{K}_f \qquad Q = 1 + X + 3X^{50} \in \mathcal{K}_f$$

- $\|P\|_\infty = \|Q\|_\infty$.
- $\|P\|_2 = \|Q\|_2$.
- $\mathcal{N}(P) << \mathcal{N}(Q)$.

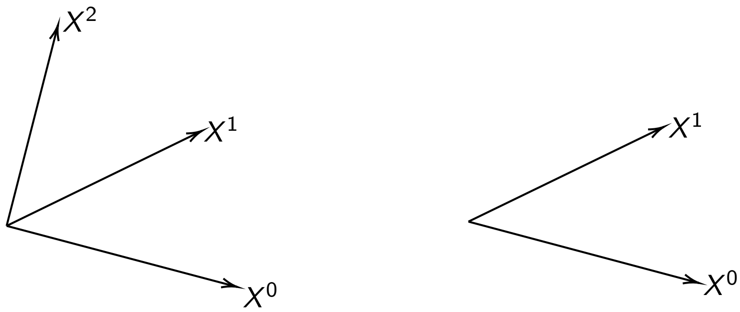
Lemma

Let $R \in \mathcal{K}_f$, *then:* $\mathcal{N}(R) = O\left(\|f\|_\infty^{\deg(R)} \|R\|_\infty^{\deg(f)}\right)$

Smaller dimension = Smaller degree



Smaller dimension = Smaller degree



Our algorithm

~~$R \leftarrow LLL(\{T, UT, \ldots, U^{d-1}T\}$ of dimension n $)$~~

Our algorithm

~~$R \leftarrow LLL\left(\{T, UT, \ldots, U^{d-1}T\}\text{ of dimension n }\right)$~~

$R \leftarrow LLL\left(\underline{\text{sublattice}}\text{ of }\{T, UT, \ldots, U^{d-1}T\}\text{ of dimension } n-s\right)$

where $0 \leq s \leq d-2$.

Our algorithm

~~$R \leftarrow LLL\left(\{T, UT, \ldots, U^{d-1}T\} \text{ of dimension n }\right)$~~

$R \leftarrow LLL\left(\underline{\text{sublattice}} \text{ of } \{T, UT, \ldots, U^{d-1}T\} \text{ of dimension } n-s\right)$

where $0 \leq s \leq d-2$.

- Coefficients of $R \leq 2^{\frac{n-s-1}{4}} p^{\frac{n-d}{n-s}}$
- $\deg(R) = n - s - 1$.

Our algorithm

~~$R \leftarrow LLL(\{T, UT, \ldots, U^{d-1}T\}$ of dimension n $)$~~

$R \leftarrow LLL\left(\underline{\text{sublattice}} \text{ of } \{T, UT, \ldots, U^{d-1}T\} \text{ of dimension } n-s\right)$

where $0 \leq s \leq d-2$.

- Coefficients of $R \leq 2^{\frac{n-s-1}{4}} p^{\frac{n-d}{n-s}}$
- $\deg(R) = n-s-1$.

New bound on $\mathcal{N}(\overline{R})$

$\mathcal{N}\left(\overline{R}\right) = O\left(2^{n\frac{n-s-1}{4}} p^{n\frac{n-d}{n-s}+\zeta(n-s-1)}\right)$.

Where $\zeta \in [0,1]$ is fixed by the polynomial selection.

Our algorithm

~~$R \leftarrow LLL(\{T, UT, \dots, U^{d-1}T\}$ of dimension n $)$~~

$$R \leftarrow LLL\left(\underline{\text{sublattice}} \text{ of } \{T, UT, \dots, U^{d-1}T\} \text{ of dimension } n-s\right)$$

where $0 \leq s \leq d-2$.

- Coefficients of $R \leq 2^{\frac{n-s-1}{4}} p^{\frac{n-d}{n-s}}$
- $\deg(R) = n - s - 1$.

New bound on $\mathcal{N}(\overline{R})$

$\mathcal{N}\left(\overline{R}\right) = O\left(2^{n\frac{n-s-1}{4}} p^{n\frac{n-d}{n-s}+\zeta(n-s-1)}\right)$. We minimize it in s

Where $\zeta \in [0, 1]$ is fixed by the polynomial selection.

Our algorithm

~~$R \leftarrow LLL\left(\{T, UT, \ldots, U^{d-1}T\} \text{ of dimension n }\right)$~~

$R \leftarrow LLL\left(\underline{\text{sublattice}} \text{ of } \{T, UT, \ldots, U^{d-1}T\} \text{ of dimension } n-s\right)$

where $0 \leq s \leq d-2$.

- Coefficients of $R \leq 2^{\frac{n-s-1}{4}} p^{\frac{n-d}{n-s}}$
- $\deg(R) = n - s - 1$.

New bound on $\mathcal{N}(\overline{R})$

$\mathcal{N}\left(\overline{R}\right) = O\left(2^{n\frac{n-s-1}{4}} p^{n\frac{n-d}{n-s}+\zeta(n-s-1)}\right)$. We minimize it in s

Where $\zeta \in [0,1]$ is fixed by the polynomial selection.

Remark

$s = 0 \Rightarrow$ *Initial algorithm [Guillevic 19]*

Finite fields of 500 bits

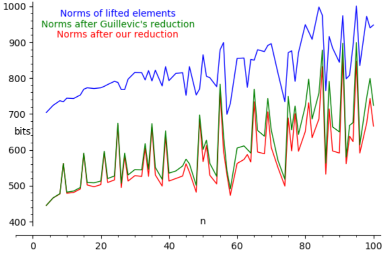


Figure: Norms in finite fields

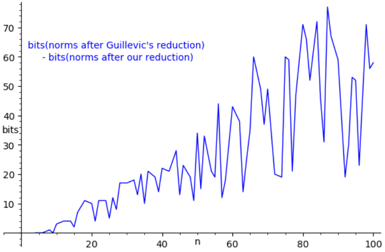
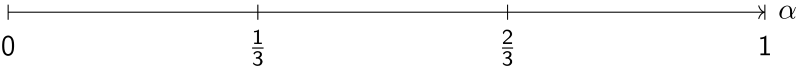


Figure: Difference in bits between [Guillevic 19] and our results as a function of n

Finite fields classification

$$p = L_{p^n}(\alpha, c) = e^{(c+o(1))\log(p^n)^{\alpha}\log\log(p^n)^{1-\alpha}}.$$

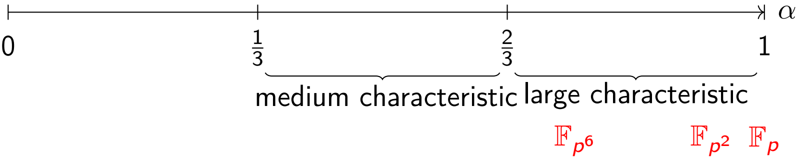


Finite fields classification

$$p = L_{p^n}(\alpha, c) = e^{(c+o(1))\log(p^n)^{\alpha}\log\log(p^n)^{1-\alpha}}.$$

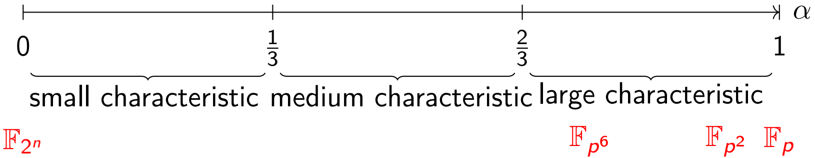
Finite fields classification

$$p = L_{p^n}(\alpha, c) = e^{(c+o(1))\log(p^n)^{\alpha}\log\log(p^n)^{1-\alpha}}.$$



Finite fields classification

$$p = L_{p^n}(\alpha, c) = e^{(c+o(1))\log(p^n)^\alpha \log\log(p^n)^{1-\alpha}}.$$



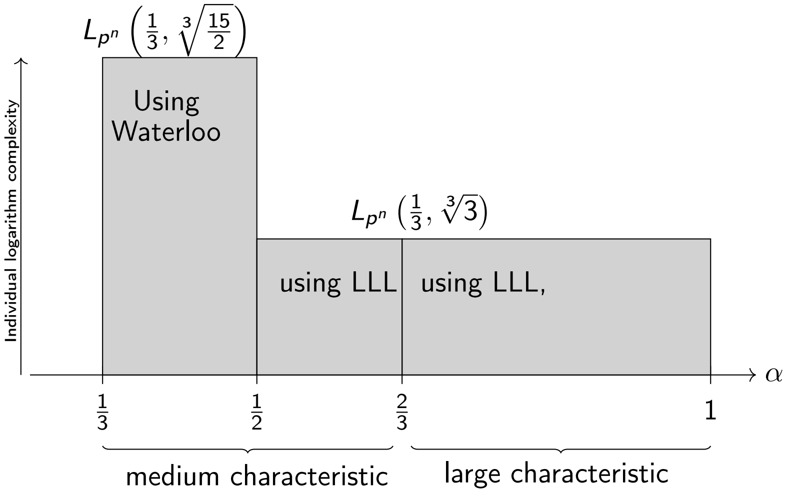


Figure: Even extension degress with JLSV1 polynomial selection

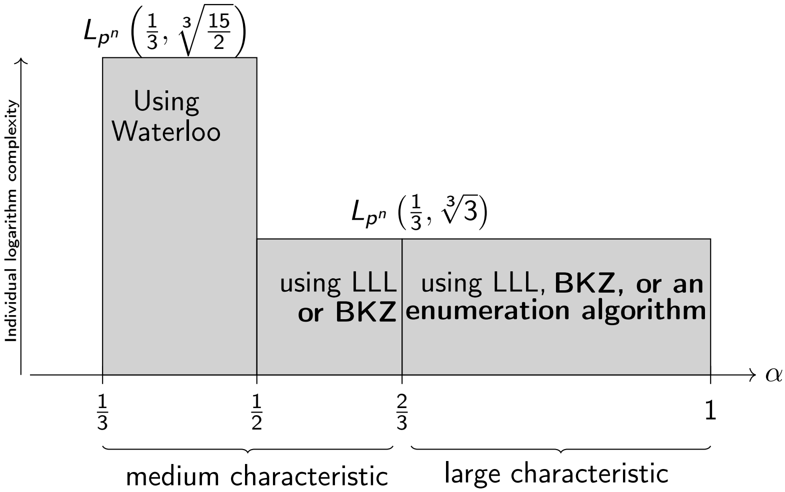


Figure: Even extension degress with JLSV1 polynomial selection

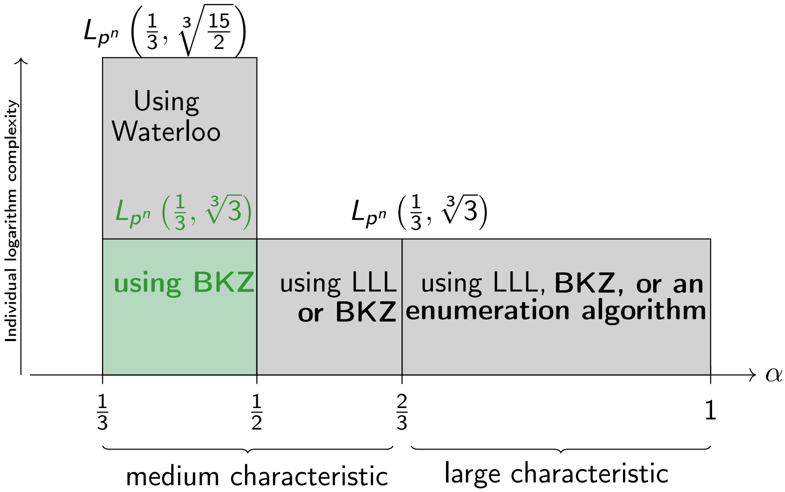
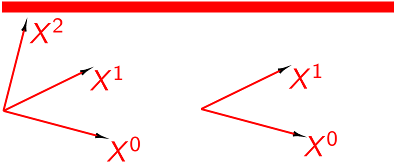


Figure: Even extension degress with JLSV1 polynomial selection

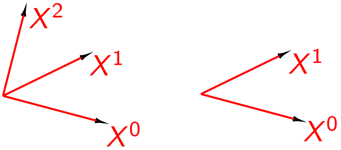
Takeaway

In practice: Use sublattices for large composite extensions.

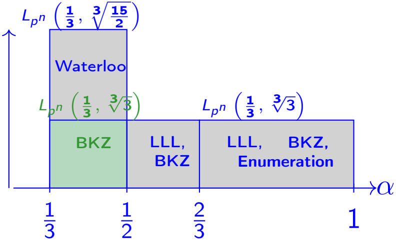


Takeaway

In practice: Use sublattices for large composite extensions.

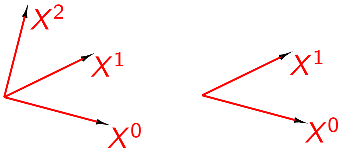


In theory: Use BKZ instead of LLL.

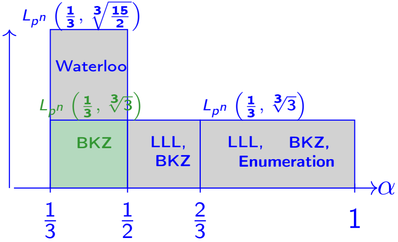


Takeaway

In practice: Use sublattices for large composite extensions.



In theory: Use BKZ instead of LLL.



Thank you !