Division and Slope Factorization of p-Adic Polynomials

Xavier Caruso, David Roe **Tristan Vaccon**

Univ.Rennes 1, Univ. Pittsburgh, 立教大学

July 22nd, 2016

RIKKYO UNIVERSITY

Why should one work with p-adic numbers ?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;

Why should one work with p-adic numbers ?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- *e.g.* Dixon's method (used in F4), Polynomial factorization via Hensel's lemma.

Why should one work with p-adic numbers ?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- *e.g.* Dixon's method (used in F4), Polynomial factorization via Hensel's lemma.

p-adic algorithms

- Going from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$ and then back to $\mathbb{Z}/p\mathbb{Z}$ enables more computation,

Why should one work with p-adic numbers ?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- *e.g.* Dixon's method (used in F4), Polynomial factorization via Hensel's lemma.

p-adic algorithms

- Going from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$ and then back to $\mathbb{Z}/p\mathbb{Z}$ enables more computation, *e.g.* the algorithms of Bostan et al. and Lercier et al. using p-adic differential equations ;

Why should one work with p-adic numbers ?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- *e.g.* Dixon's method (used in F4), Polynomial factorization via Hensel's lemma.

p-adic algorithms

- Going from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$ and then back to $\mathbb{Z}/p\mathbb{Z}$ enables more computation, *e.g.* the algorithms of Bostan et al. and Lercier et al. using p-adic differential equations ;
- Kedlaya's and Lauder's counting-point algorithms via p-adic cohomology ;

Why should one work with p-adic numbers ?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- *e.g.* Dixon's method (used in F4), Polynomial factorization via Hensel's lemma.

p-adic algorithms

- Going from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$ and then back to $\mathbb{Z}/p\mathbb{Z}$ enables more computation, *e.g.* the algorithms of Bostan et al. and Lercier et al. using p-adic differential equations ;
- Kedlaya's and Lauder's counting-point algorithms via p-adic cohomology ;

My personal (long-term) motivation

Computing (some) moduli spaces of p-adic Galois representations.

Studying polynomial computations over p-adics

A building block

At ISSAC 2015, we have studied the p-adic stability of some computations in **linear algebra**.

Studying polynomial computations over p-adics

A building block

At ISSAC 2015, we have studied the p-adic stability of some computations in **linear algebra**. This year, we study basic operations related to **polynomial computations**.

Studying polynomial computations over p-adics

A building block

At ISSAC 2015, we have studied the p-adic stability of some computations in **linear algebra**. This year, we study basic operations related to **polynomial computations**.

More motivations

- Understanding basic operations related to field extensions, in particular division and quotients.

Studying polynomial computations over p-adics

A building block

At ISSAC 2015, we have studied the p-adic stability of some computations in **linear algebra**. This year, we study basic operations related to **polynomial computations**.

More motivations

- Understanding basic operations related to field extensions, in particular division and quotients.
- Understanding the behaviour of precision during factorisation: over $\mathbb{Q}_p$ or $k[\![T]\!]$, or as an intermediate to factorisation over $\mathbb{Q}$.

Studying polynomial computations over p-adics

A building block

At ISSAC 2015, we have studied the p-adic stability of some computations in **linear algebra**. This year, we study basic operations related to **polynomial computations**.

More motivations

- Understanding basic operations related to field extensions, in particular division and quotients.
- Understanding the behaviour of precision during factorisation: over $\mathbb{Q}_p$ or $k[\![T]\!]$, or as an intermediate to factorisation over $\mathbb{Q}$.

Today's highlights

- Optimal tracking of precision for **modular multiplication** and **diffused digits**.

Studying polynomial computations over p-adics

A building block

At ISSAC 2015, we have studied the p-adic stability of some computations in **linear algebra**. This year, we study basic operations related to **polynomial computations**.

More motivations

- Understanding basic operations related to field extensions, in particular division and quotients.
- Understanding the behaviour of precision during factorisation: over $\mathbb{Q}_p$ or $k[\![T]\!]$, or as an intermediate to factorisation over $\mathbb{Q}$.

Today's highlights

- Optimal tracking of precision for **modular multiplication** and **diffused digits**.
- Precision for **slope factorization** algorithms.

What are p-adic numbers?

What are p-adic numbers?

p refers to a prime number

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \ldots a_i \ldots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \ldots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \ldots a_i \ldots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \ldots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \dots a_i \dots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \dots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

The valuation $v_p(a)$ of a is the smallest v such that $a_v \neq 0$.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \dots a_i \dots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \dots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

The valuation $v_p(a)$ of a is the smallest v such that $a_v \neq 0$.

The p-adic numbers form the field $\mathbb{Q}_p$.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \dots a_i \dots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \dots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

The valuation $v_p(a)$ of a is the smallest v such that $a_v \neq 0$.

The p-adic numbers form the field $\mathbb{Q}_p$.

A p-adic number with no digit after the comma is a p-adic integer.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \dots a_i \dots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \dots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

The valuation $v_p(a)$ of a is the smallest v such that $a_v \neq 0$.

The p-adic numbers form the field $\mathbb{Q}_p$.

A p-adic number with no digit after the comma is a p-adic integer.

The p-adic integers form a subring $\mathbb{Z}_p$ of $\mathbb{Q}_p$.

Summary on p-adics

Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

Summary on p-adics

Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\forall k \in \mathbb{N}, \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

Summary on p-adics

Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\forall k \in \mathbb{N}, \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

A first idea

- $\mathbb{Q}_p$ is an extension of $\mathbb{Q}$ where one can perform **calculus**, as simply as over $\mathbb{R}$.

Summary on p-adics

Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\forall k \in \mathbb{N}, \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

A first idea

- $\mathbb{Q}_p$ is an extension of $\mathbb{Q}$ where one can perform **calculus**, as simply as over $\mathbb{R}$.
- We are **closer to arithmetic** : we can reduce modulo p.

Summary on p-adics

Proposition

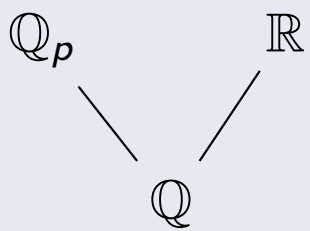
$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\forall k \in \mathbb{N}, \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

A first idea

- $\mathbb{Q}_p$ is an extension of $\mathbb{Q}$ where one can perform **calculus**, as simply as over $\mathbb{R}$.
- We are **closer to arithmetic** : we can reduce modulo p.

Remark



$$\begin{array}{ccc} \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ \downarrow & & \downarrow \\ \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \end{array}$$

Definition of the precision

Finite-precision p-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=k}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $k \in \mathbb{Z}$ and p a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Definition of the precision

Finite-precision p-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=k}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $k \in \mathbb{Z}$ and p a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Definition of the precision

Finite-precision p-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=k}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $k \in \mathbb{Z}$ and p a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Definition

The **order**, or the **absolute precision** of $\sum_{i=k}^{d-1} a_i p^i + O(p^d)$ is d.

Definition of the precision

Finite-precision p-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=k}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $k \in \mathbb{Z}$ and p a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Definition

The **order**, or the **absolute precision** of $\sum_{i=k}^{d-1} a_i p^i + O(p^d)$ is d.

Example

The order of $3 * 7^{-1} + 4 * 7^0 + 5 * 7^1 + 6 * 7^2 + O(7^3)$ is 3.

p-adic precion *vs* real precision

The quintessential idea of the step-by-step analysis is the following :

Proposition (p-adic errors don't add)

Indeed,

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

That is to say, if a and b are known up to precision $O(p^k)$, then so is $a + b$.

p-adic precion *vs* real precision

The quintessential idea of the step-by-step analysis is the following :

Proposition (p-adic errors don't add)

Indeed,

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

That is to say, if a and b are known up to precision $O(p^k)$, then so is $a + b$.

p-adic precion *vs* real precision

The quintessential idea of the step-by-step analysis is the following :

Proposition (p-adic errors don't add)

Indeed,

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

That is to say, if a and b are known up to precision $O(p^k)$, then so is $a + b$.

Remark

It is quite the opposite to when dealing with real numbers, because of **Round-off error** :

$$(1 + 5 * 10^{-2}) + (2 + 6 * 10^{-2}) = 3 + 1 * 10^{-1} + 1 * 10^{-2}.$$

That is to say, if a and b are known up to precision 10^{-n}, then $a + b$ is known up to $10^{(-n+1)}$.

p-adic precion *vs* real precision

The quintessential idea of the step-by-step analysis is the following :

Proposition (p-adic errors don't add)

Indeed,

$$(a + O(p^{k})) + (b + O(p^{k})) = a + b + O(p^{k}).$$

That is to say, if a and b are known up to precision $O(p^k)$, then so is $a + b$.

Remark

It is quite the opposite to when dealing with real numbers, because of **Round-off error** :

$$(1 + 5 * 10^{-2}) + (2 + 6 * 10^{-2}) = 3 + 1 * 10^{-1} + 1 * 10^{-2}.$$

That is to say, if a and b are known up to precision 10^{-n}, then $a + b$ is known up to $10^{(-n+1)}$.

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Proposition (multiplication)

$$(x_0 + O(p^{k_0})) * (x_1 + O(p^{k_1})) = x_0 * x_1 + O(p^{min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Proposition (multiplication)

$$(x_0 + O(p^{k_0})) * (x_1 + O(p^{k_1})) = x_0 * x_1 + O(p^{min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

Proposition (division)

$$\frac{xp^a + O(p^b)}{yp^c + O(p^d)} = x * y^{-1}p^{a-c} + O(p^{min(d+a-2c,b-c)})$$

In particular,

$$\frac{1}{p^c y + O(p^d)} = y^{-1}p^{-c} + O(p^{d-2c})$$

Interesting behaviour

Large modular multiplication

- Setting: 10 significant digits in $\mathbb{Q}_2$.

Interesting behaviour

Large modular multiplication

- Setting: 10 significant digits in $\mathbb{Q}_2$.
- Modulus $P = X^2 + 2$.
- $A = 5 - 2X + 4X^2$.

Interesting behaviour

Large modular multiplication

- Setting: 10 significant digits in $\mathbb{Q}_2$.
- Modulus $P = X^2 + 2$.
- $A = 5 - 2X + 4X^2$.
- Compute **iteratively** (**naively**) $A_n = A^n \mod P$.

Interesting behaviour

Large modular multiplication

- Setting: 10 significant digits in $\mathbb{Q}_2$.
- Modulus $P = X^2 + 2$.
- $A = 5 - 2X + 4X^2$.
- Compute **iteratively** (**naively**) $A_n = A^n \mod P$.

Behaviour of significant digits

Interesting behaviour

Large modular multiplication

- Setting: 10 significant digits in $\mathbb{Q}_2$.
- Modulus $P = X^2 + 2$.
- $A = 5 - 2X + 4X^2$.
- Compute **iteratively** (**naively**) $A_n = A^n \mod P$.

Behaviour of significant digits

n	10^0	10^1	10^2	10^3	10^4	10^5	10^6
relative precision of $lc(A_n)$	10	9	8	7	6	5	4

Interesting behaviour

Large modular multiplication

- Setting: 10 significant digits in $\mathbb{Q}_2$.
- Modulus $P = X^2 + 2$.
- $A = 5 - 2X + 4X^2$.
- Compute **iteratively** (**naively**) $A_n = A^n \mod P$.

Behaviour of significant digits

n	10^0	10^1	10^2	10^3	10^4	10^5	10^6
relative precision of $lc(A_n)$	10	9	8	7	6	5	4

Question:

How can we obtain **satisfying** / **optimal** behaviour regarding to precision?

Table of contents

The Main lemma of p-adic differential precision

Lemma (CRV14)

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) **differentiable** mapping.*

The Main lemma of p-adic differential precision

Lemma (CRV14)

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*

The Main lemma of p-adic differential precision

Lemma (CRV14)

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****,*

The Main lemma of p-adic differential precision

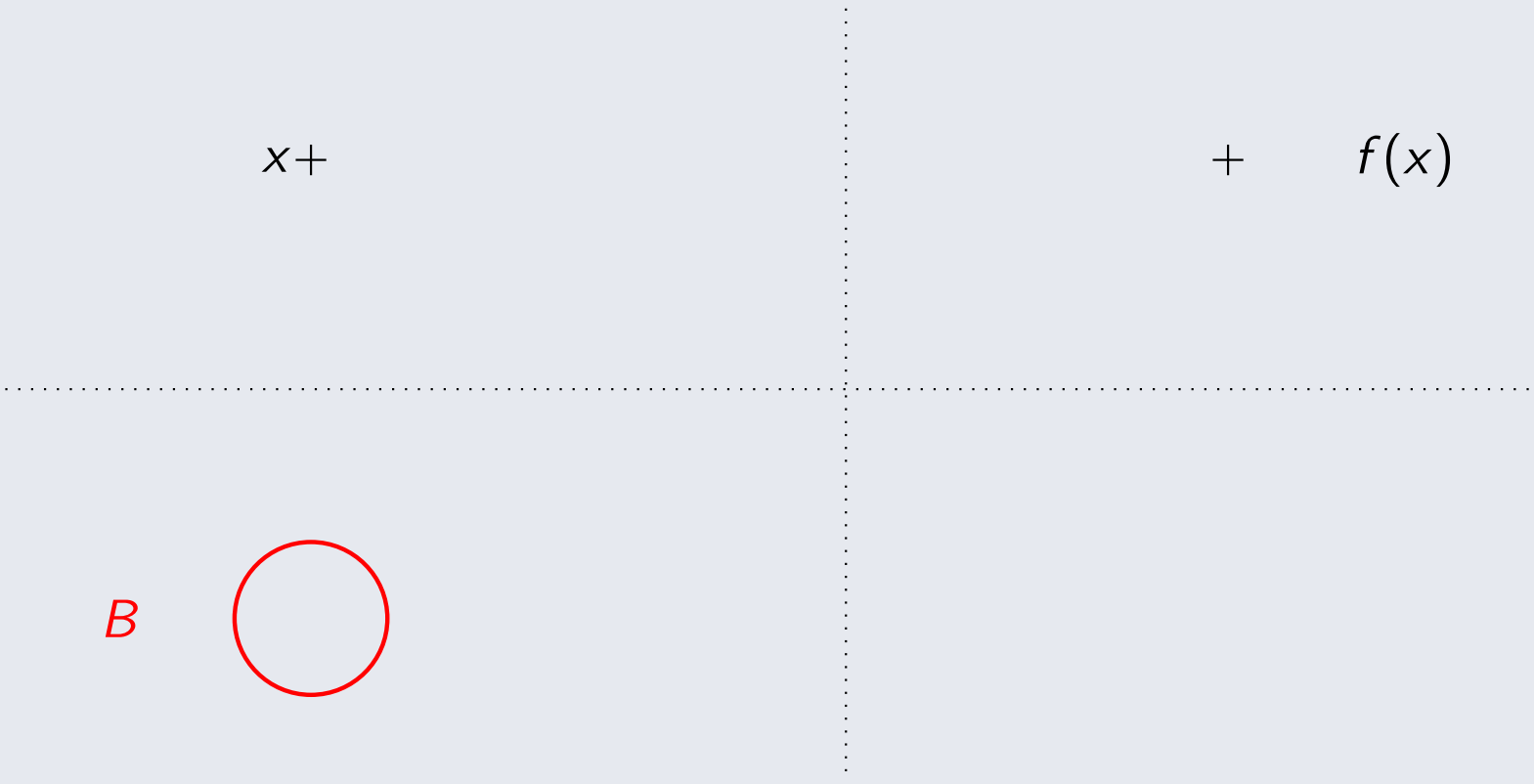
Lemma (CRV14)

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****,*

$$f(x + B) = f(x) + f'(x) \cdot B.$$

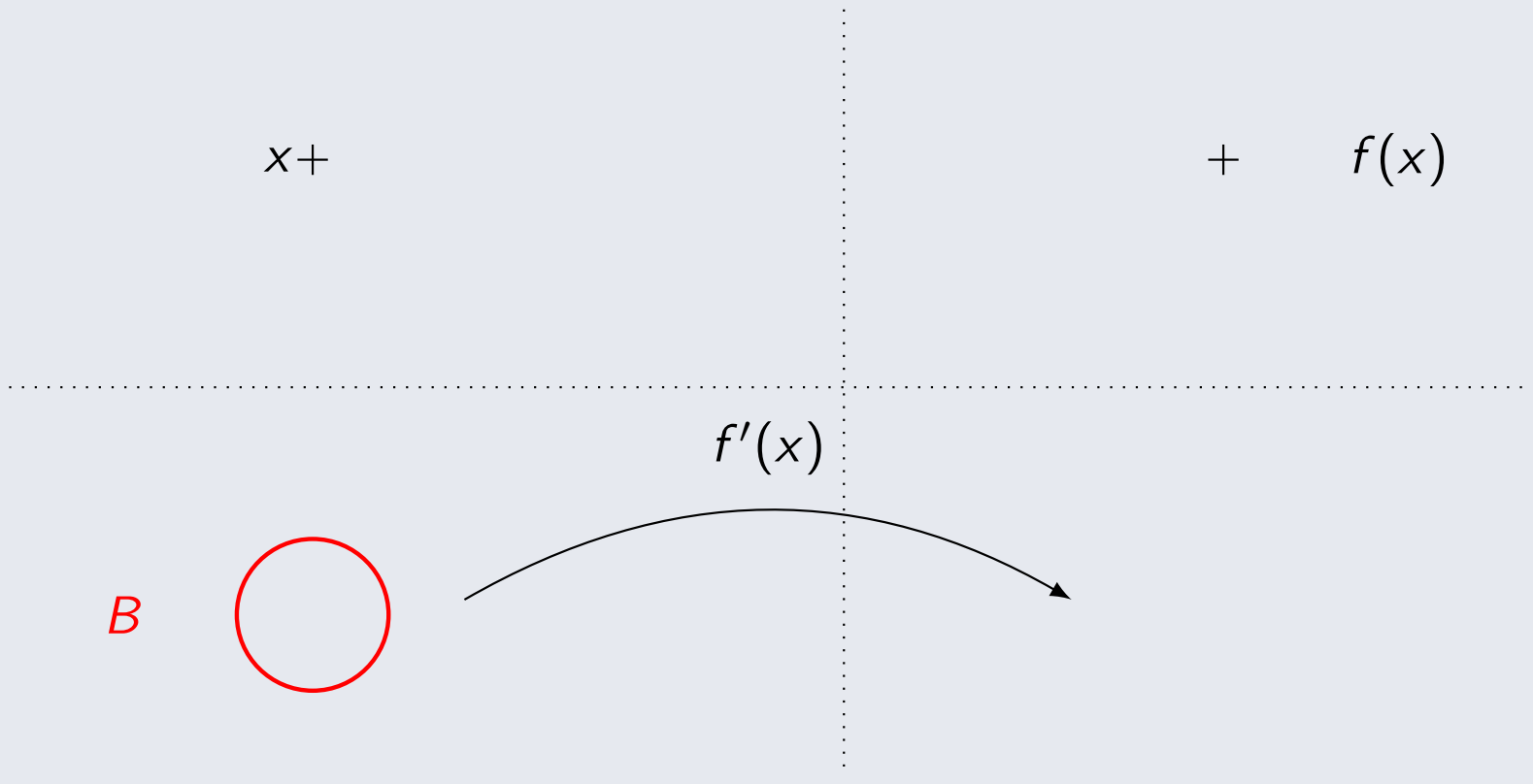
Geometrical meaning

Interpretation



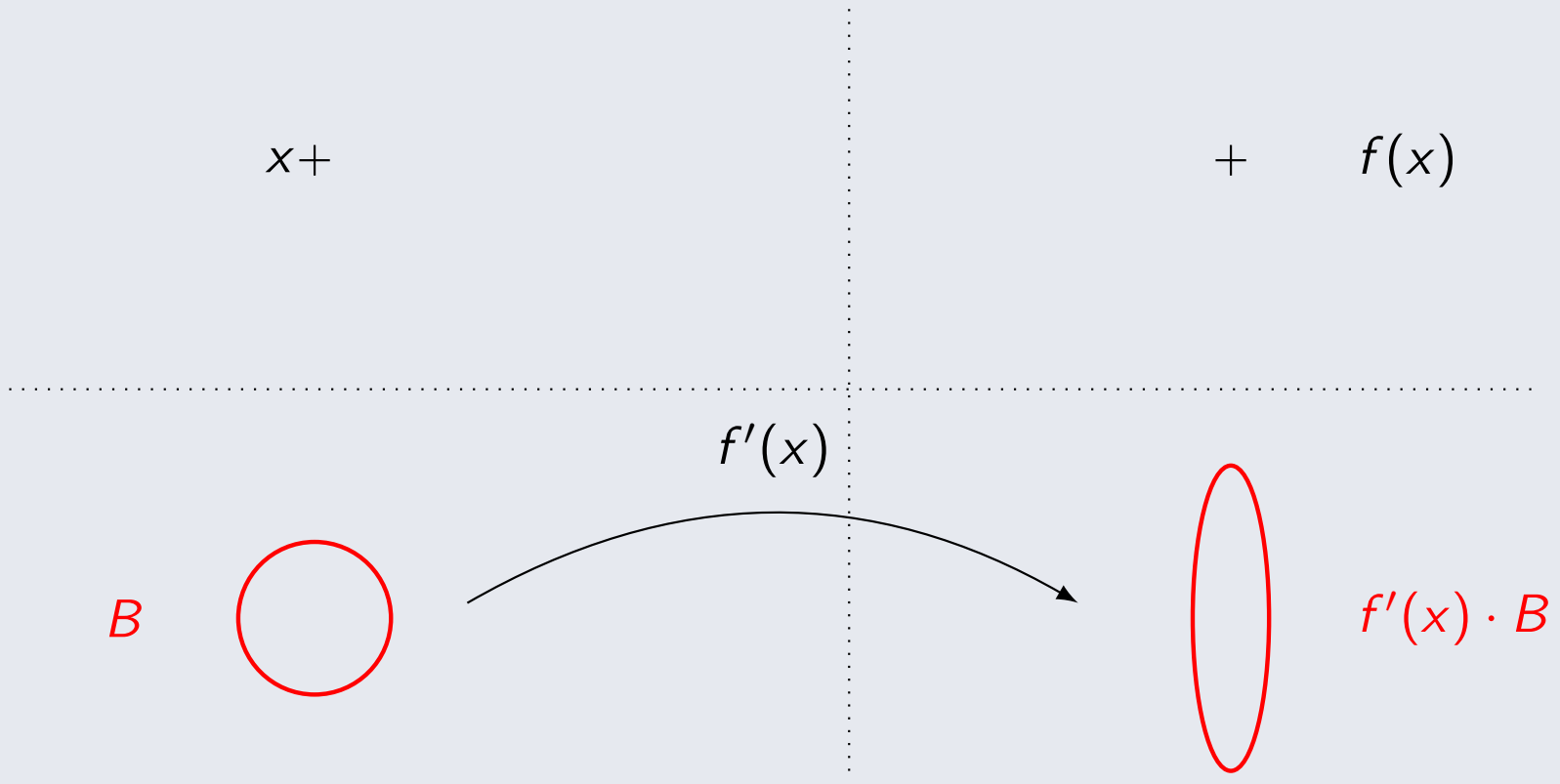
Geometrical meaning

Interpretation



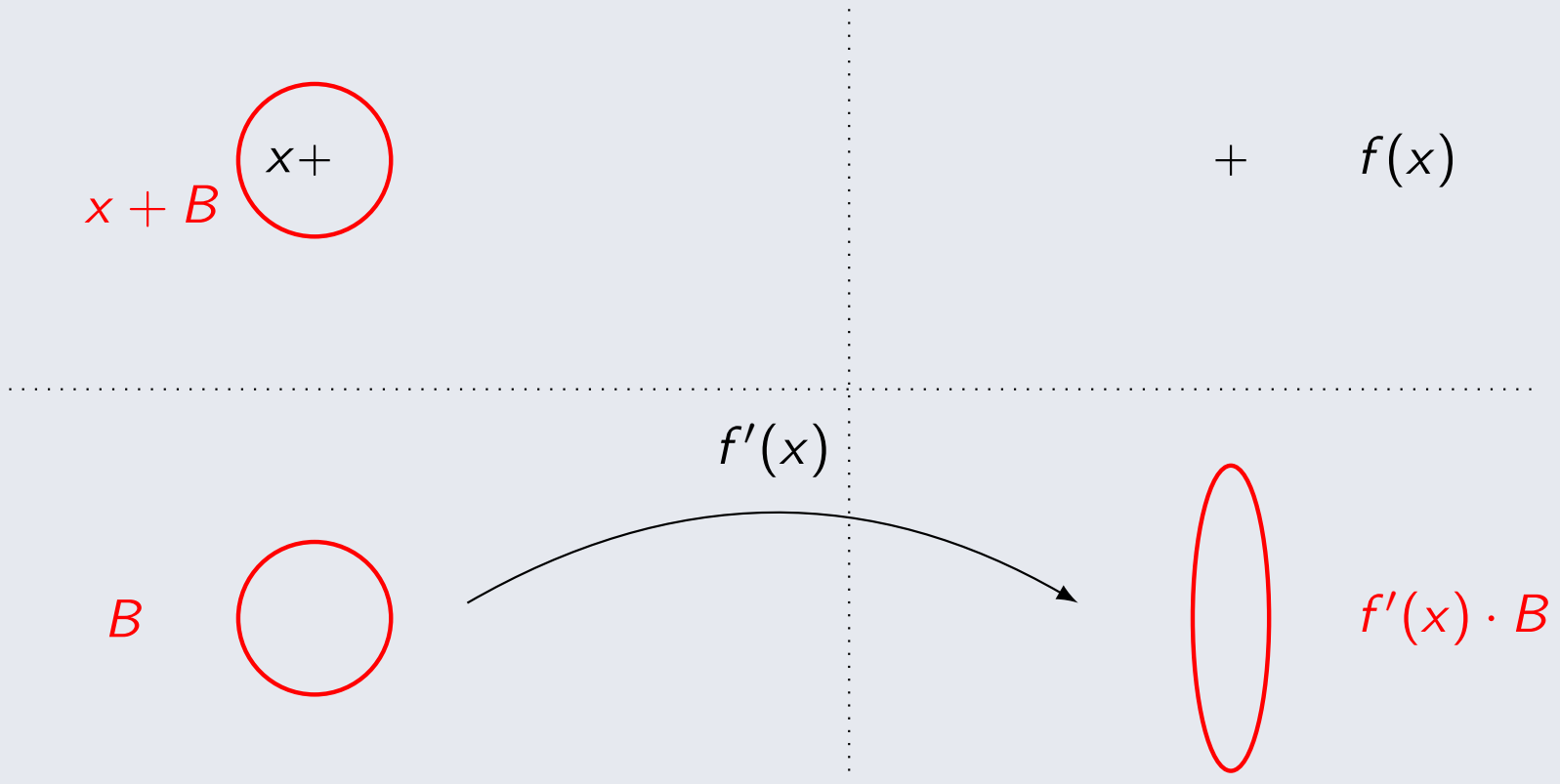
Geometrical meaning

Interpretation



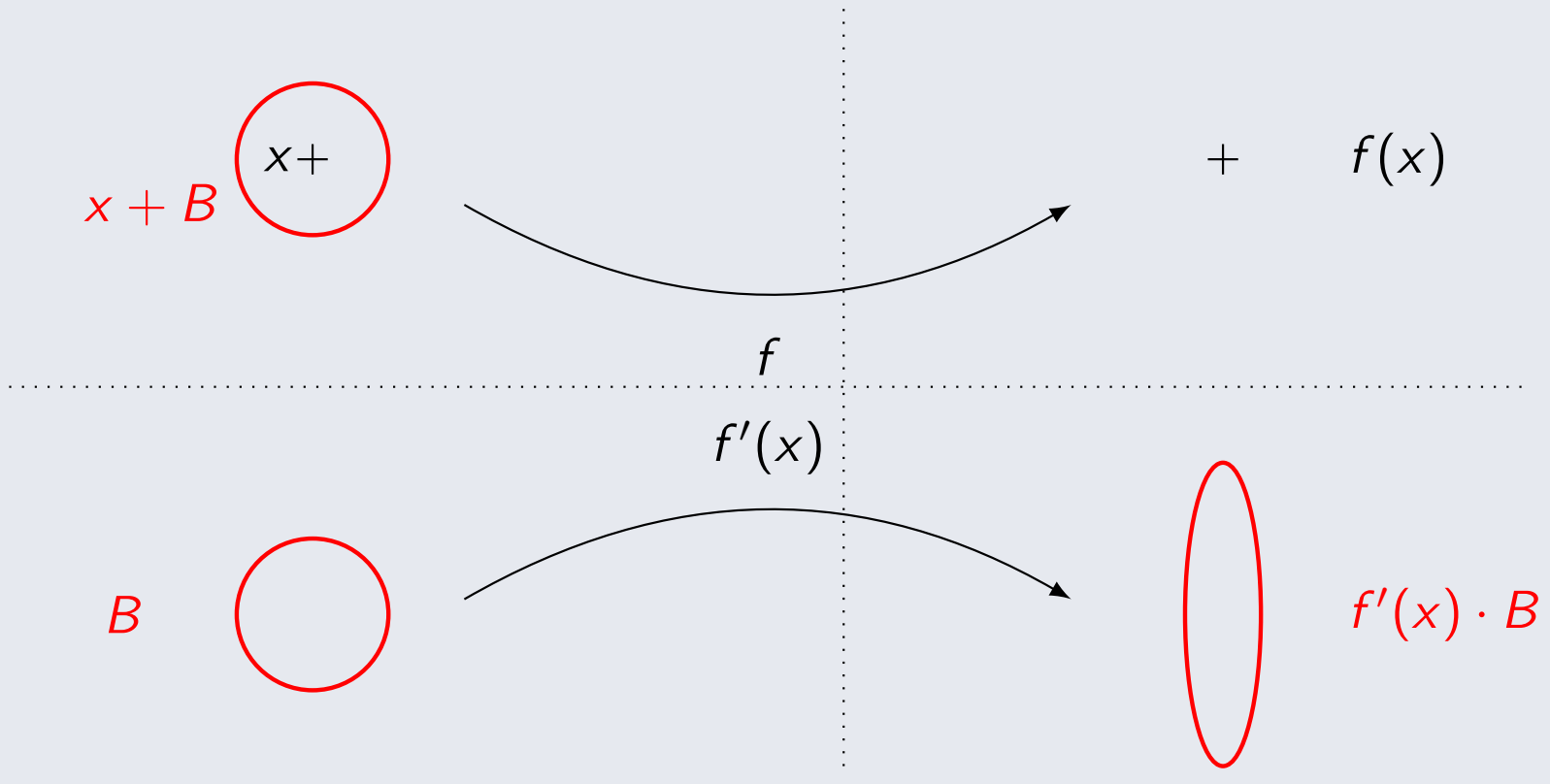
Geometrical meaning

Interpretation



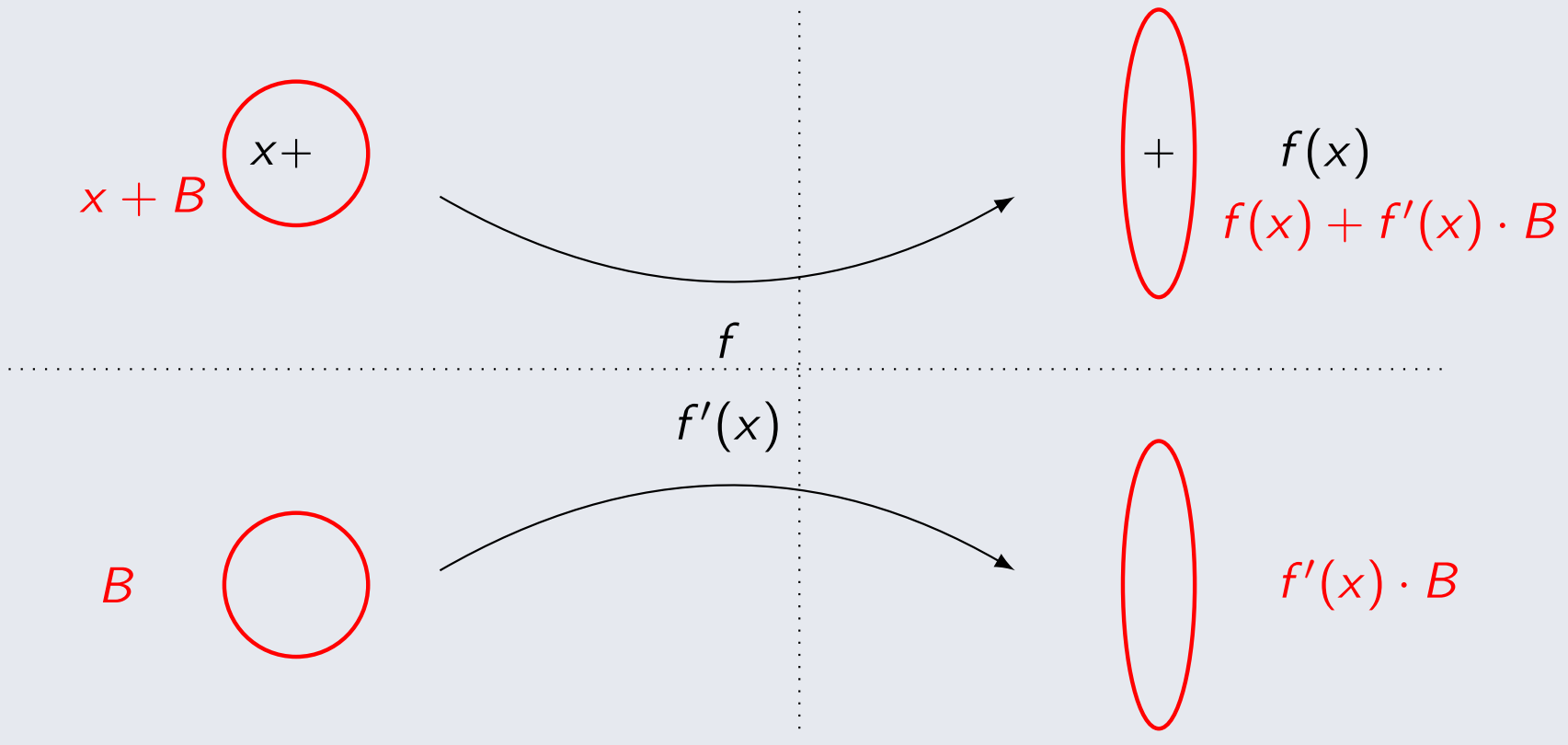
Geometrical meaning

Interpretation



Geometrical meaning

Interpretation



Lattices

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****,*

$$f(x + B) = f(x) + f'(x) \cdot B.$$

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****, for any open $\mathbb{Z}_p$-**lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****, for any open $\mathbb{Z}_p$-**lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

Remark

This allows more models of precision, like

$$(x, y) = (1 + O(p^{10}), 1 + O(p)).$$

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****, for any open $\mathbb{Z}_p$-**lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

Remark

This allows more models of precision, like

$$(x, y) = (1 + O(p^{10}), 1 + O(p)).$$

Remark

Our framework can be extended to **(complete) ultrametric K-vector spaces** (*e.g.* being $\mathbb{F}_p((X))^n$, $\mathbb{Q}((X))^m$, $\mathbb{R}((\varepsilon))^s$).

Higher differentials

Higher differentials

What is **small enough** ?

How can we determine when the lemma applies ?

Higher differentials

What is **small enough** ?

How can we determine when the lemma applies ?
When f is locally analytic, it essentially corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

Higher differentials

What is **small enough** ?

How can we determine when the lemma applies ?
When f is locally analytic, it essentially corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

This can be determined with **Newton-polygon** techniques.

Table of contents

Handling the precision

Lattice precision

To each polynomial, **we attach a $\mathbb{Z}_p$-lattice** (given by a basis of this lattice).

Handling the precision

Lattice precision

To each polynomial, **we attach a $\mathbb{Z}_p$-lattice** (given by a basis of this lattice).

Lattice and division

A and B are known with precision lattice H_A and H_B. Then (H_Q, H_R) are given by the Euclidean division of $H_A - QH_B$ by B.

Handling the precision

Lattice precision

To each polynomial, **we attach a $\mathbb{Z}_p$-lattice** (given by a basis of this lattice).

Lattice and division

A and B are known with precision lattice H_A and H_B. Then (H_Q, H_R) are given by the Euclidean division of $H_A - QH_B$ by B.

Proof.

$$\begin{aligned} A &= BQ + R, \\ A + \delta A &= (B + \delta B)(Q + \delta Q) + (R + \delta R), \end{aligned}$$

Handling the precision

Lattice precision

To each polynomial, **we attach a $\mathbb{Z}_p$-lattice** (given by a basis of this lattice).

Lattice and division

A and B are known with precision lattice H_A and H_B. Then (H_Q, H_R) are given by the Euclidean division of $H_A - QH_B$ by B.

Proof.

$$\begin{aligned} A &= BQ + R, \\ A + \delta A &= (B + \delta B)(Q + \delta Q) + (R + \delta R), \\ \delta A &= Q\delta B + B\delta Q + \delta R \text{ (at first order)}, \end{aligned}$$

Handling the precision

Lattice precision

To each polynomial, **we attach a $\mathbb{Z}_p$-lattice** (given by a basis of this lattice).

Lattice and division

A and B are known with precision lattice H_A and H_B. Then (H_Q, H_R) are given by the Euclidean division of $H_A - QH_B$ by B.

Proof.

$$\begin{aligned} A &= BQ + R, \\ A + \delta A &= (B + \delta B)(Q + \delta Q) + (R + \delta R), \\ \delta A &= Q\delta B + B\delta Q + \delta R \text{ (at first order)}, \\ \delta A - Q\delta B &= B\delta Q + \delta R. \end{aligned}$$

Table of contents

Lattice precision and modular multiplication

Composed derivatives

It is easy to handle in an optimal way the modular multiplication by applying:

Lattice precision and modular multiplication

Composed derivatives

It is easy to handle in an optimal way the modular multiplication by applying:

- For $A \times B$,

Lattice precision and modular multiplication

Composed derivatives

It is easy to handle in an optimal way the modular multiplication by applying:

- For $A \times B$,

$$\delta(A \times B) = A\delta B + B\delta A.$$

Lattice precision and modular multiplication

Composed derivatives

It is easy to handle in an optimal way the modular multiplication by applying:

- For $A \times B$,
$$\delta(A \times B) = A\delta B + B\delta A.$$
- For remainder R in $A = BQ + R$,

Lattice precision and modular multiplication

Composed derivatives

It is easy to handle in an optimal way the modular multiplication by applying:

- For $A \times B$,
$$\delta(A \times B) = A\delta B + B\delta A.$$
- For remainder R in $A = BQ + R$,
$$\delta(R) = \delta A - Q\delta B \mod B.$$

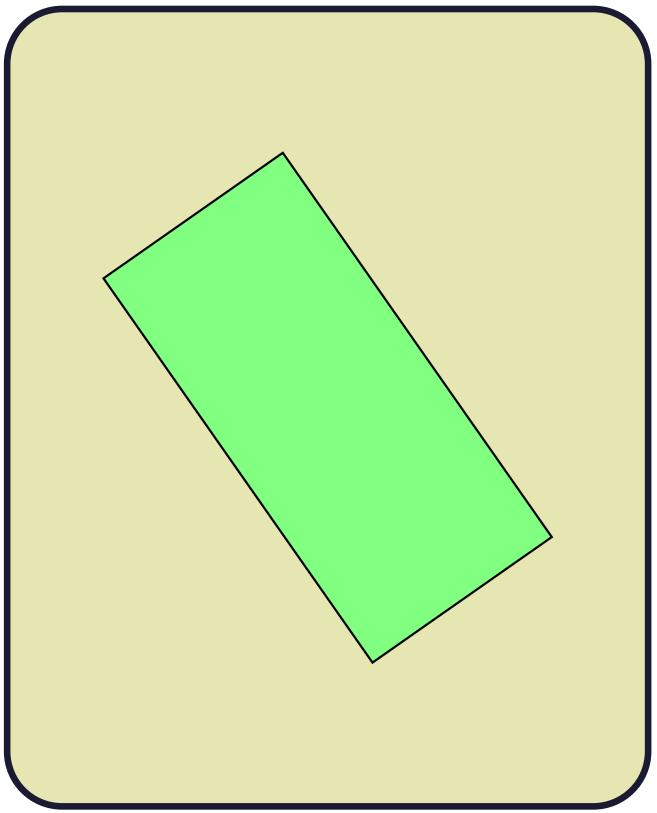
Toward numerical understanding

Displaying precision

Toward numerical understanding

Displaying precision

Let $H \subset \mathbb{Q}_p^n$ be a lattice.



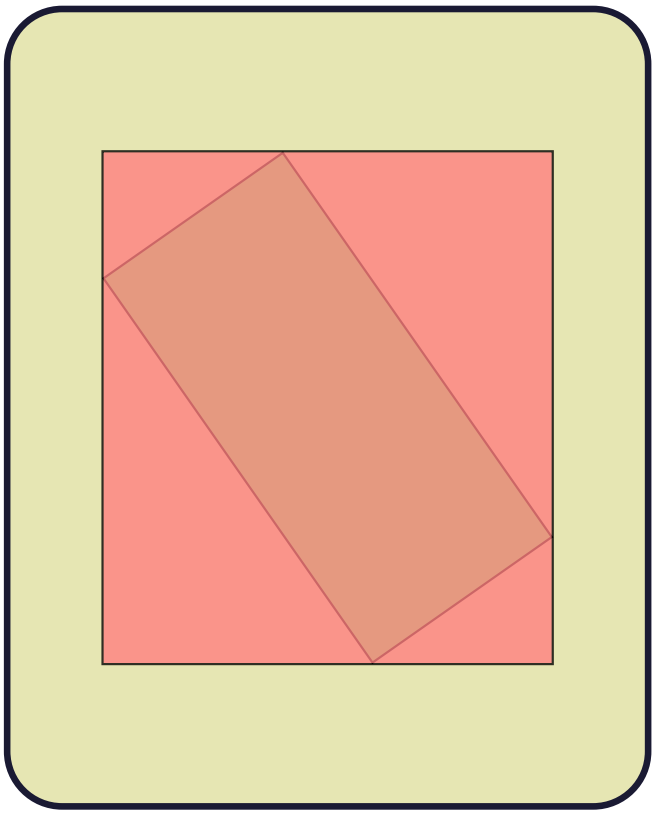
Toward numerical understanding

Displaying precision

Let $H \subset \mathbb{Q}_p^n$ be a lattice.

$$H_0 = \pi_1(H) \oplus \cdots \oplus \pi_n(H)$$

provides the **best precision on coordinates**.
It is the **smallest diagonal lattice** containing H.



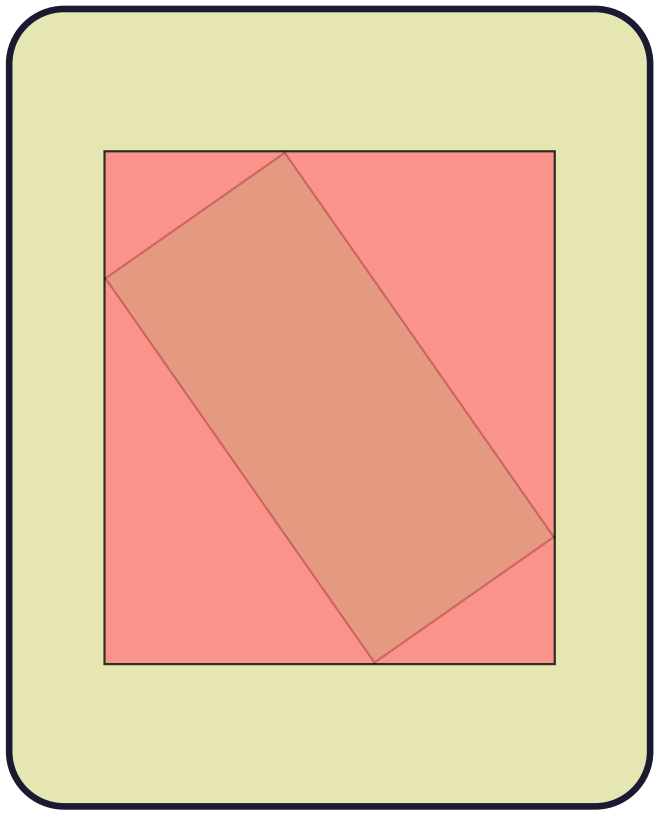
Toward numerical understanding

Displaying precision

Let $H \subset \mathbb{Q}_p^n$ be a lattice.

$$H_0 = \pi_1(H) \oplus \cdots \oplus \pi_n(H)$$

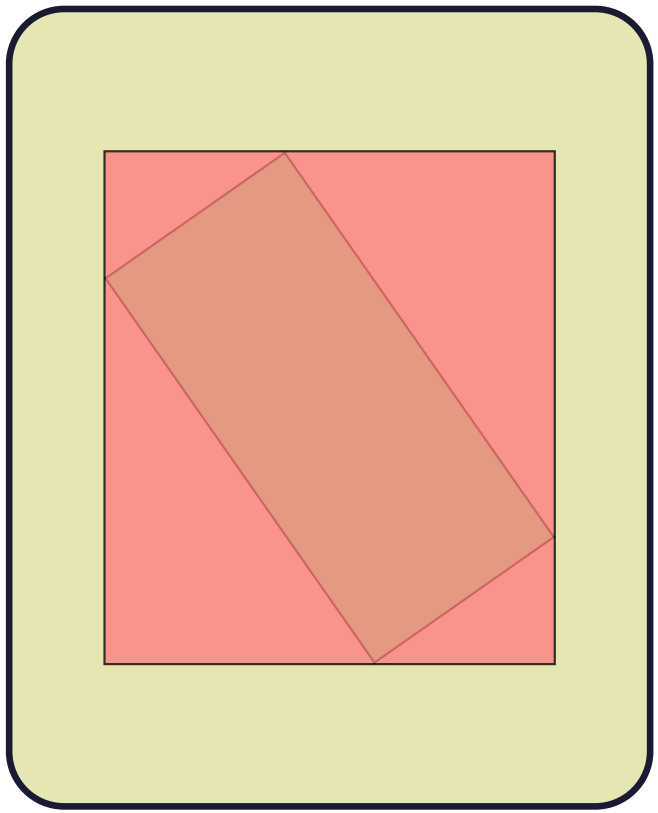
provides the **best precision on coordinates**.
It is the **smallest diagonal lattice** containing H.



Diffused digits

The number of **diffused digits of precision** of H is the length of H_0/H.

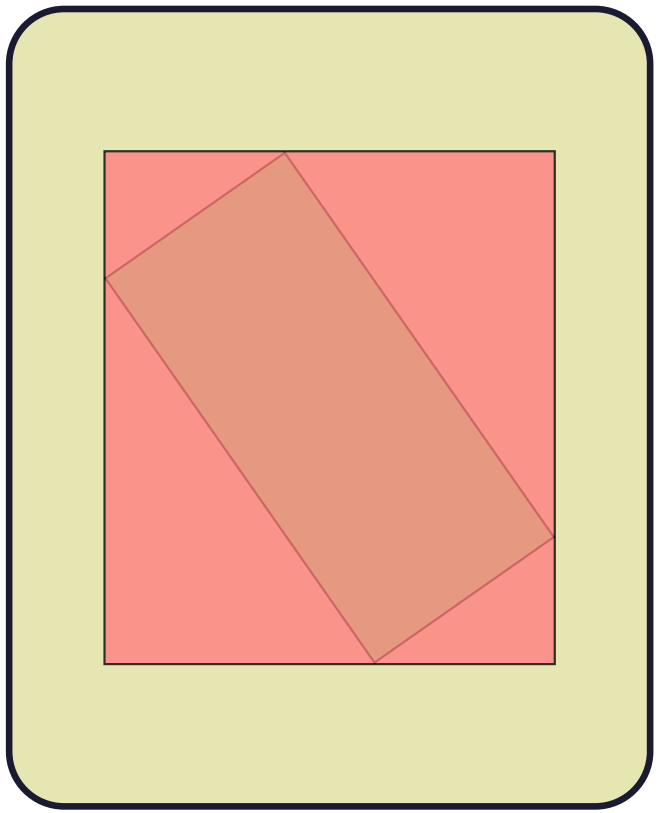
More on diffused digits



More on diffused digits

Diffused digits

The number of **diffused digits of precision** of H is the length of H_0/H.



More on diffused digits

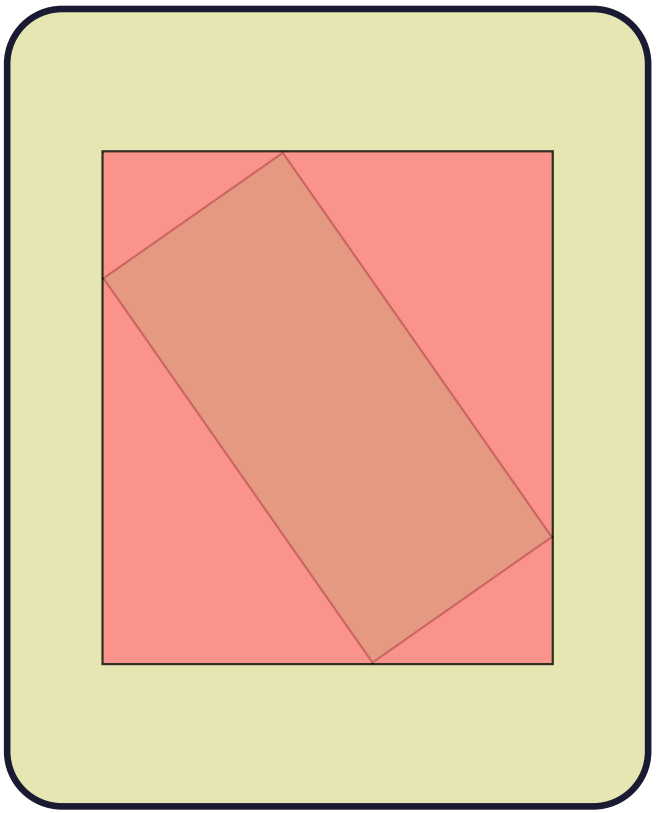
Diffused digits

The number of **diffused digits of precision** of H is the length of H_0/H.

Another definition

Here, the number of diffused digits is:

$$-\log_p\left(|H_0/H|\right).$$



Diffused digits: example

Diffused digits: the lattice

Let

$$H = \left\langle \begin{pmatrix} 1 \\ p \\ p^2 \end{pmatrix}, \begin{pmatrix} p \\ p^2 \\ 2p^4 \end{pmatrix}, \begin{pmatrix} 2p \\ p^2 \\ 2p^3 \end{pmatrix} \right\rangle.$$

Diffused digits: example

Diffused digits: the lattice

Let

$$H = \left\langle \begin{pmatrix} 1 \\ p \\ p^2 \end{pmatrix}, \begin{pmatrix} p \\ p^2 \\ 2p^4 \end{pmatrix}, \begin{pmatrix} 2p \\ p^2 \\ 2p^3 \end{pmatrix} \right\rangle.$$

Then

$$H_0 = \begin{pmatrix} 1 & & \\ & p & \\ & & p^2 \end{pmatrix}.$$

Diffused digits: example

Diffused digits: the lattice

Let

$$H = \left\langle \begin{pmatrix} 1 \\ p \\ p^2 \end{pmatrix}, \begin{pmatrix} p \\ p^2 \\ 2p^4 \end{pmatrix}, \begin{pmatrix} 2p \\ p^2 \\ 2p^3 \end{pmatrix} \right\rangle.$$

Then

$$H_0 = \begin{pmatrix} 1 & & \\ & p & \\ & & p^2 \end{pmatrix}.$$

Number of diffused digits

The SNF of H_0/H is: $\begin{pmatrix} 1 & & \\ & p & \\ & & p \end{pmatrix}$.

Diffused digits: example

Diffused digits: the lattice

Let

$$H = \left\langle \begin{pmatrix} 1 \\ p \\ p^2 \end{pmatrix}, \begin{pmatrix} p \\ p^2 \\ 2p^4 \end{pmatrix}, \begin{pmatrix} 2p \\ p^2 \\ 2p^3 \end{pmatrix} \right\rangle.$$

Then

$$H_0 = \begin{pmatrix} 1 & & \\ & p & \\ & & p^2 \end{pmatrix}.$$

Number of diffused digits

The SNF of H_0/H is: $\begin{pmatrix} 1 & & \\ & p & \\ & & p \end{pmatrix}$. Hence **2 diffused digits**.

Comparison: $\prod_{i=1}^{n} A_i \mod M$

Modulus M	n	Gain of precision	
		Jagged	Lattice (not dif. + dif.)
$X^5 + X^2 + 1$ (Irred. mod 2)	10	0.2	0.2 + 0.0
	50	4.2	4.2 + 0.0
	100	11.2	11.2 + 0.0
$X^5 + 1$ (Sep. mod 2)	10	0.4	0.9 + 6.0
	50	5.6	11.1 + 42.0
	100	13.6	27.0 + 87.0
$X^5 + 2$ (Eisenstein)	10	6.2	6.2 + 0.0
	50	44.0	44.0 + 0.0
	100	92.5	92.5 + 0.0
$(X+1)^5 + 2$ (Shift Eisenstein)	10	0.6	4.7 + 1.4
	50	7.1	42.6 + 1.4
	100	15.1	91.8 + 1.4
$X^5 + X + 2$ (Two slopes)	10	1.7	7.9 + 9.8
	50	8.1	70.7 + 59.8
	100	16.1	152.6 + 125.9

Figure: Precision for modular multiplication

Qualitative understanding: two possibilities

Qualitative understanding: two possibilities

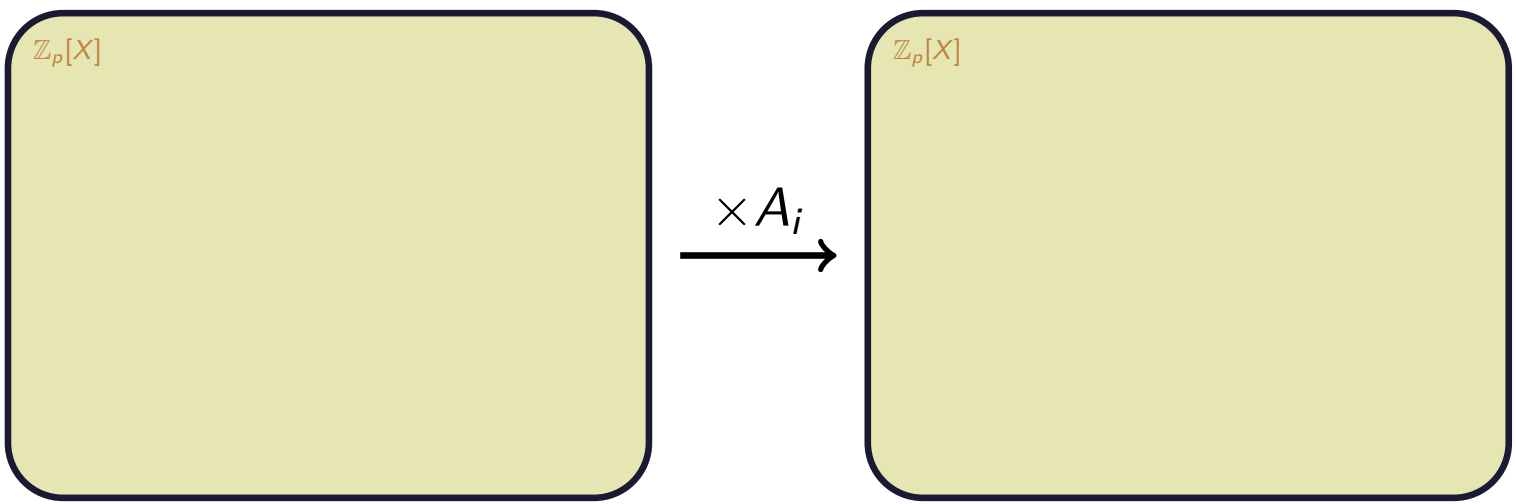
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A

Qualitative understanding: two possibilities

Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

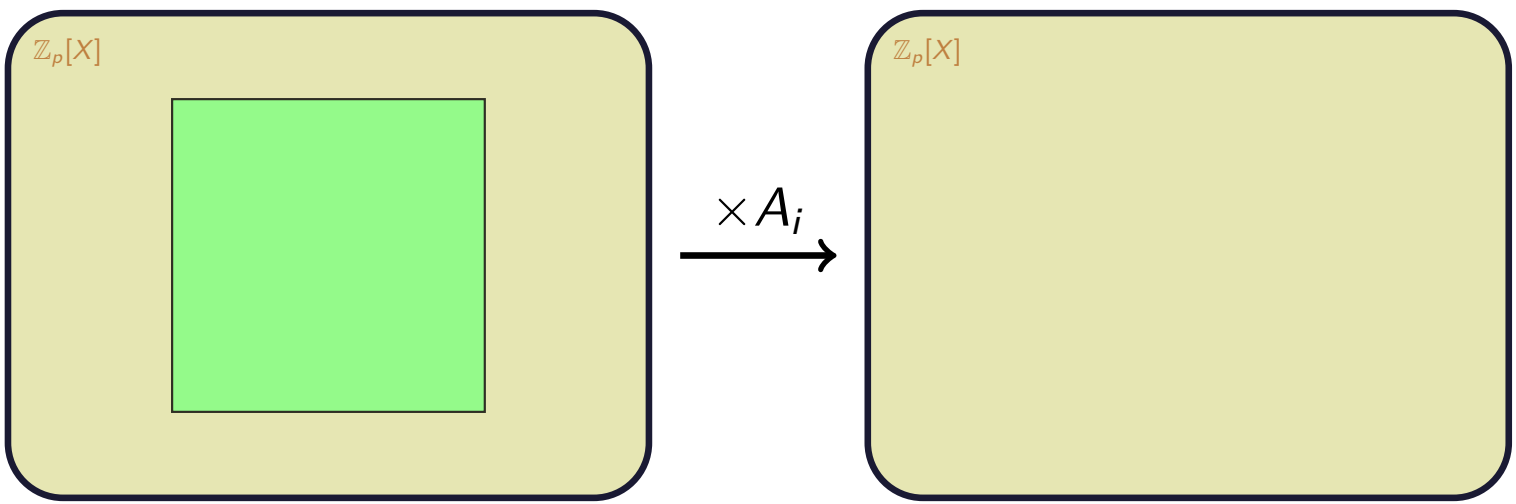
1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



Qualitative understanding: two possibilities

Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

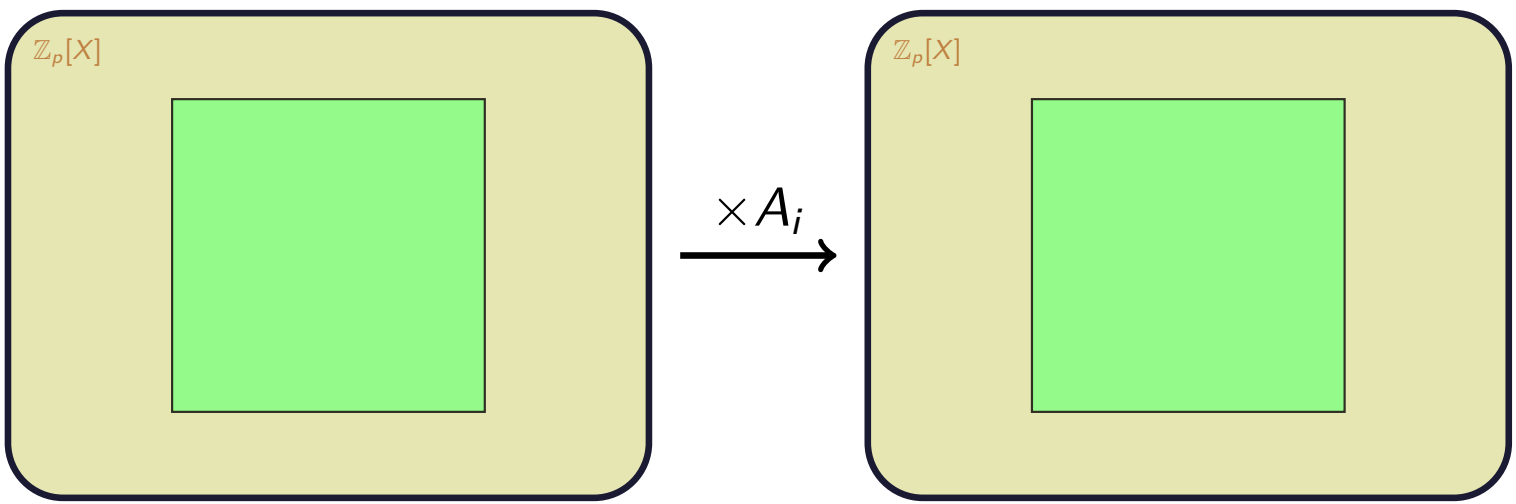
1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



Qualitative understanding: two possibilities

Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

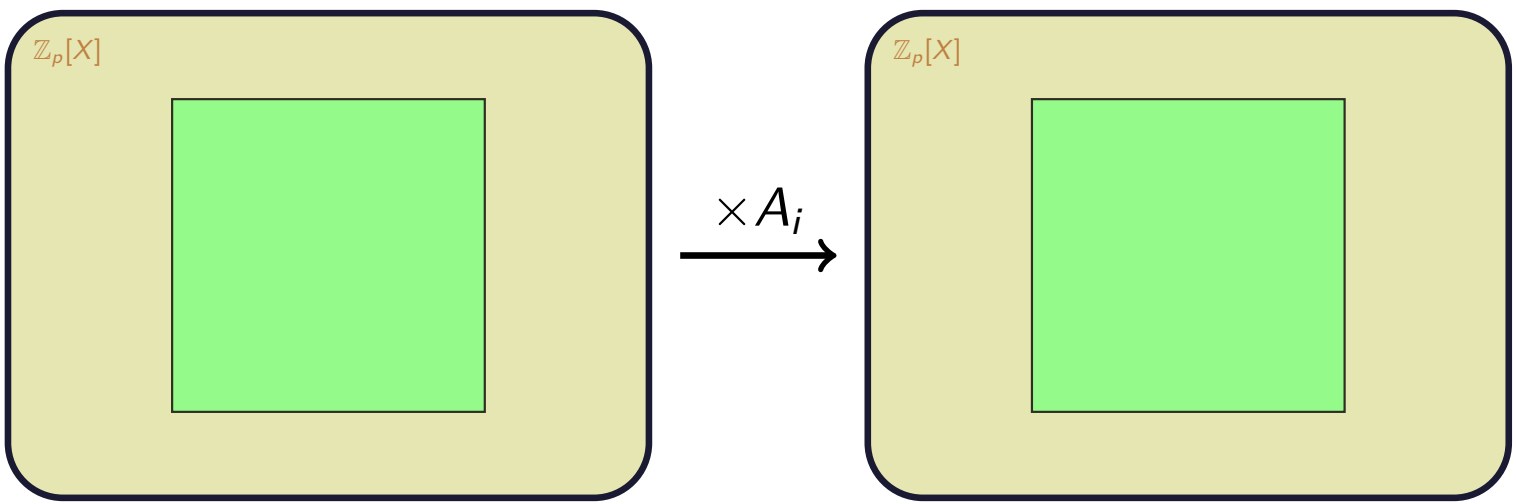
1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



Qualitative understanding: two possibilities

Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A

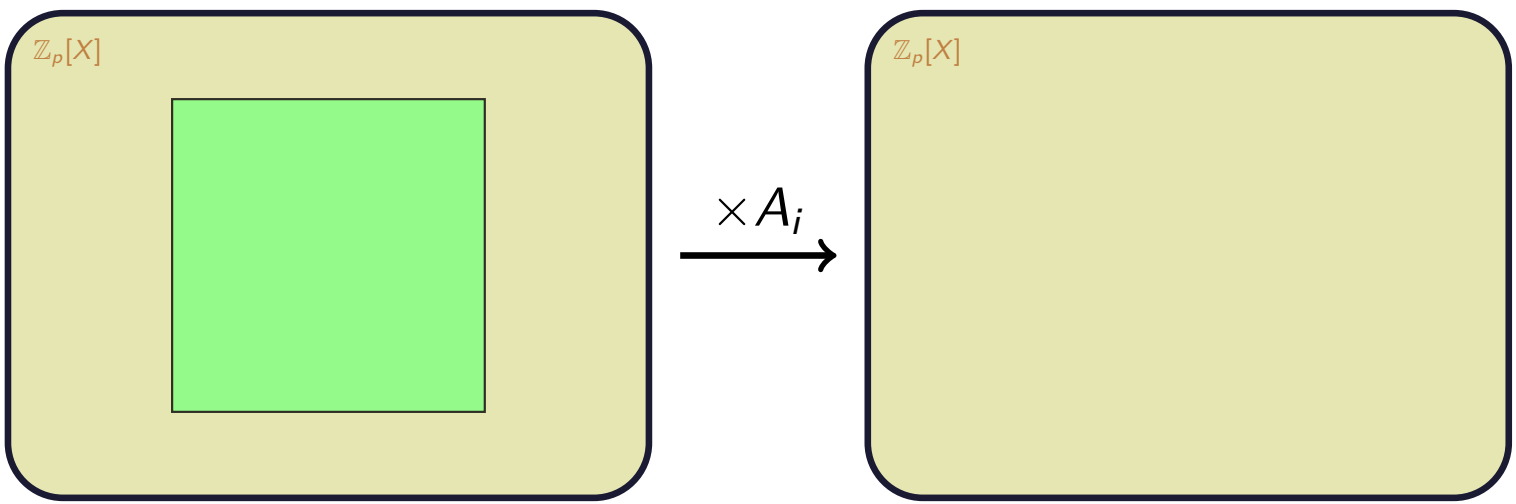


no diffused digits

Qualitative understanding: two possibilities

Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

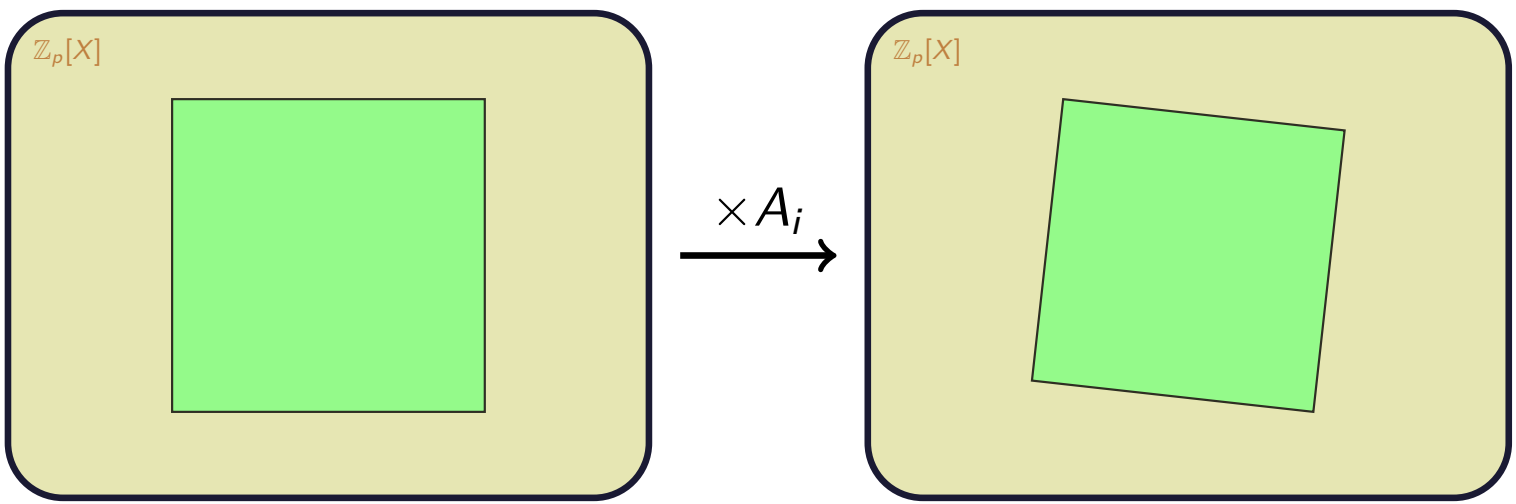
1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



Qualitative understanding: two possibilities

Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

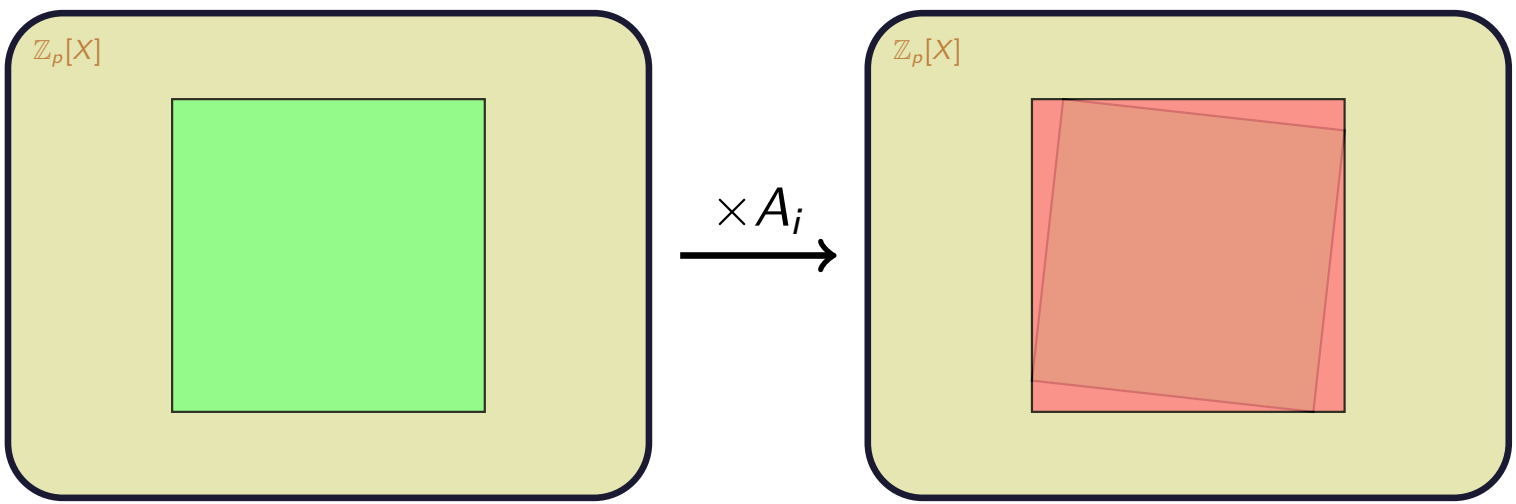
1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



Qualitative understanding: two possibilities

Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

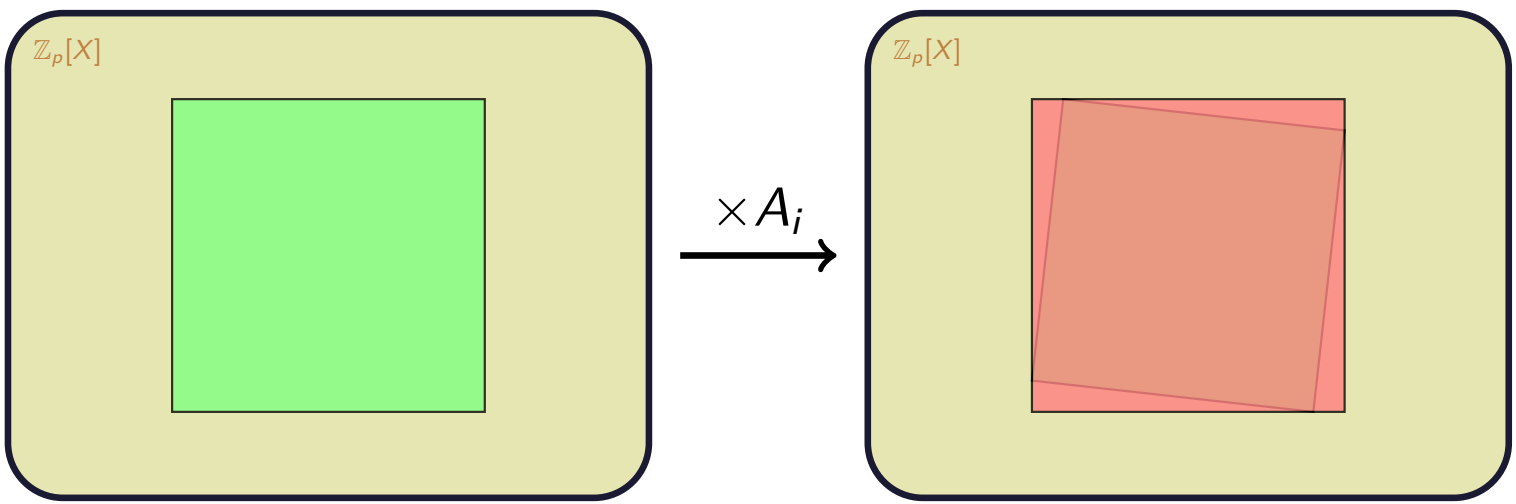
1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



Qualitative understanding: two possibilities

Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



diffused digits

Qualitative understanding: long-term

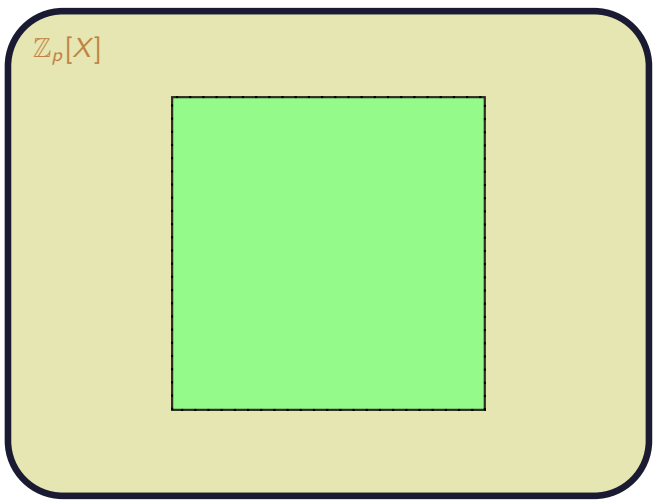
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A

Qualitative understanding: long-term

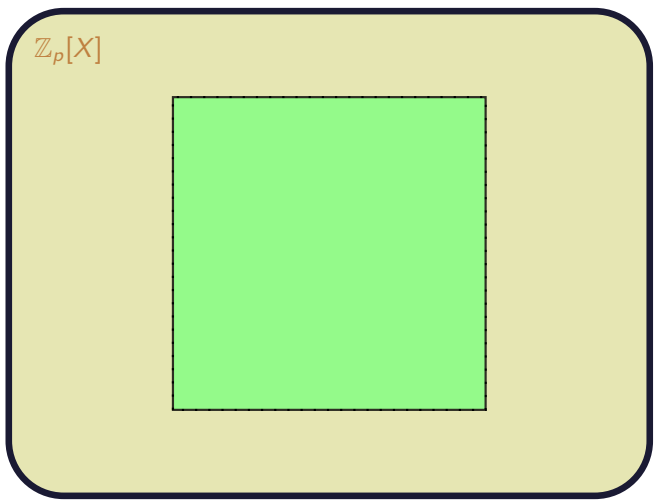
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 0$

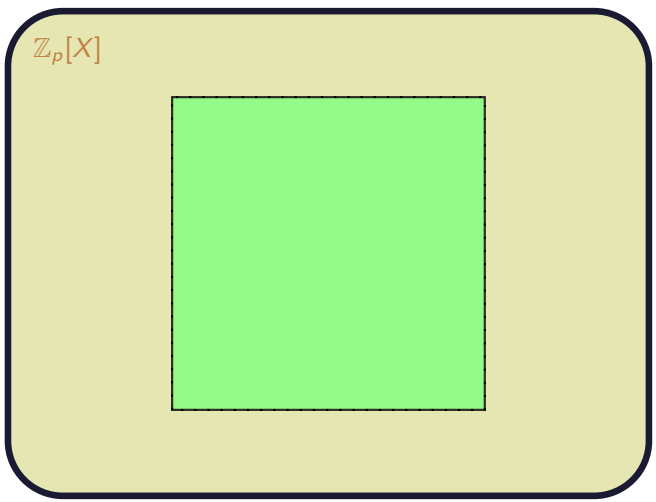


with lattice

Qualitative understanding: long-term

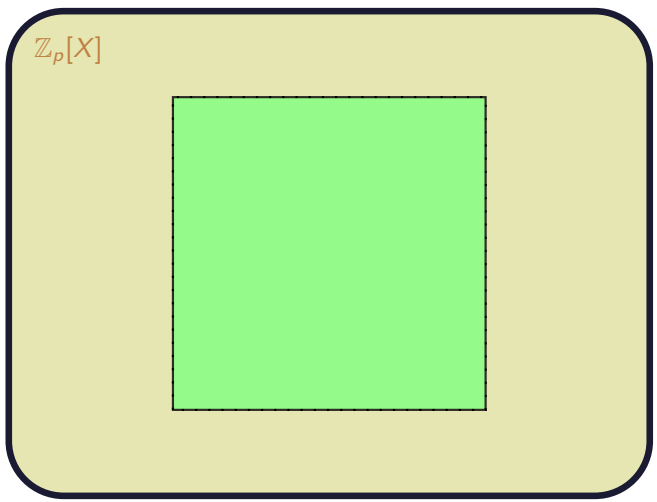
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 1$

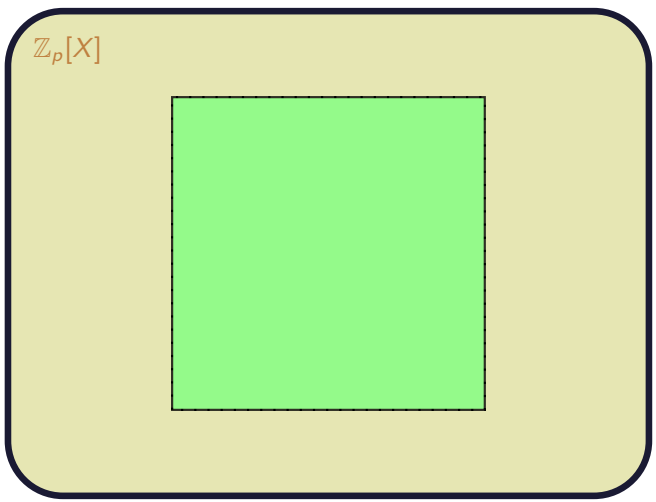


with lattice

Qualitative understanding: long-term

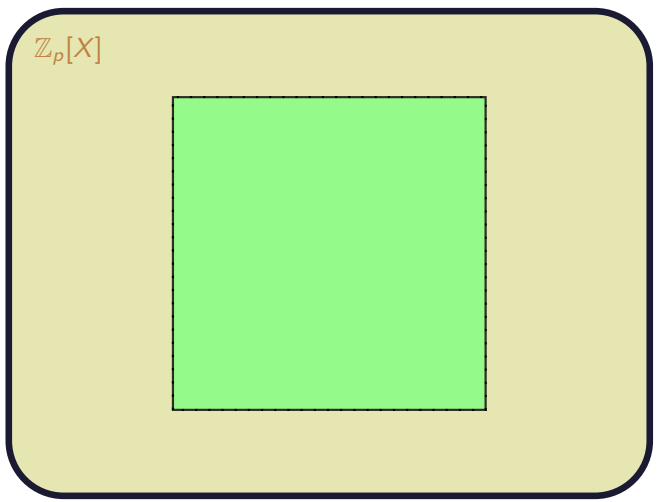
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 2$

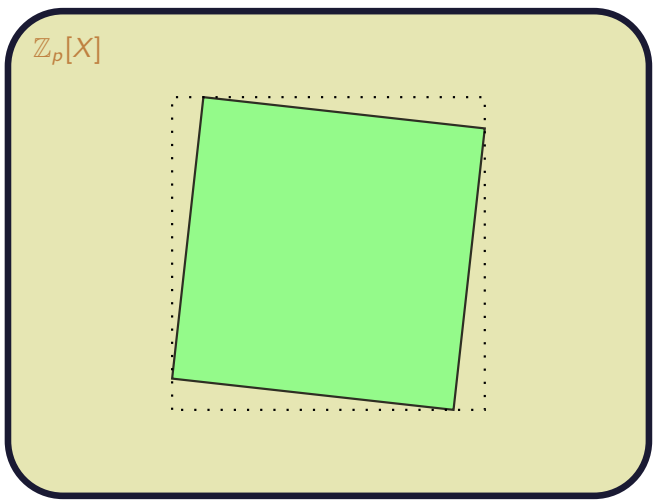


with lattice

Qualitative understanding: long-term

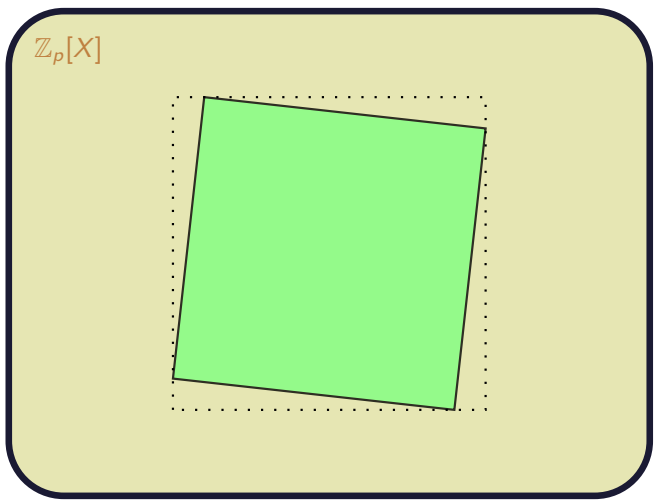
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 3$

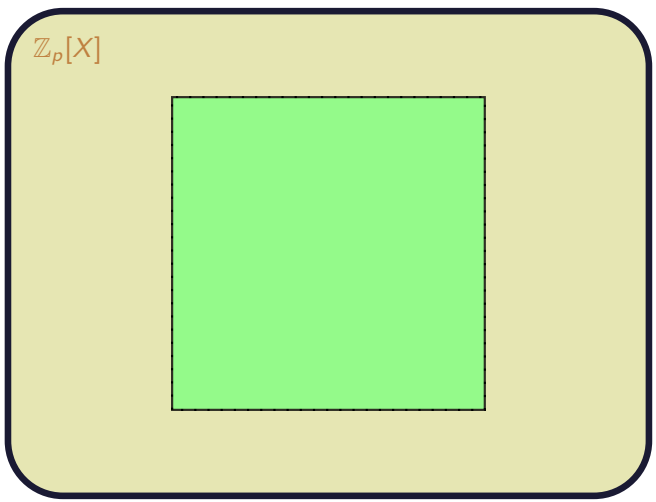


with lattice

Qualitative understanding: long-term

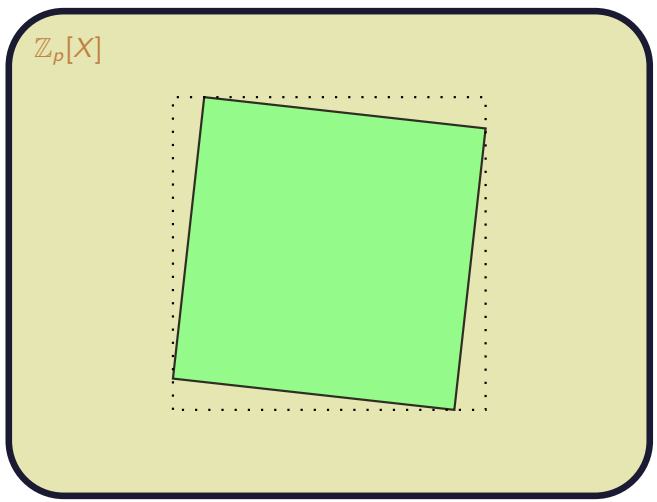
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 3$

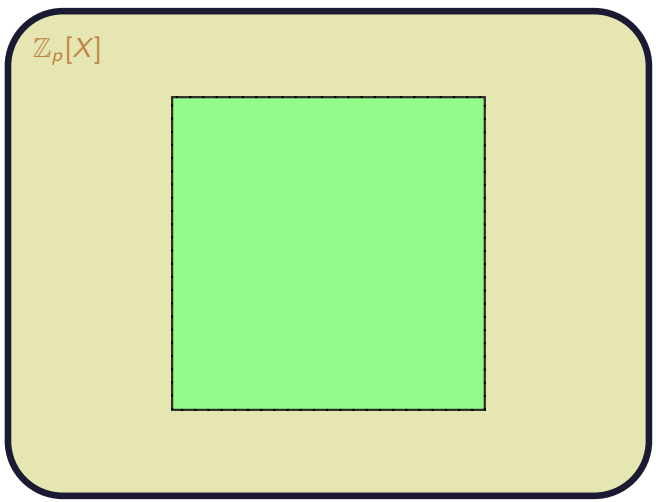


with lattice

Qualitative understanding: long-term

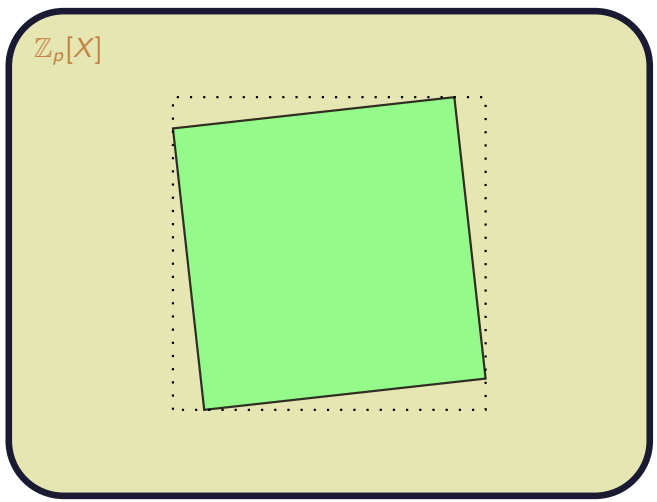
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 4$

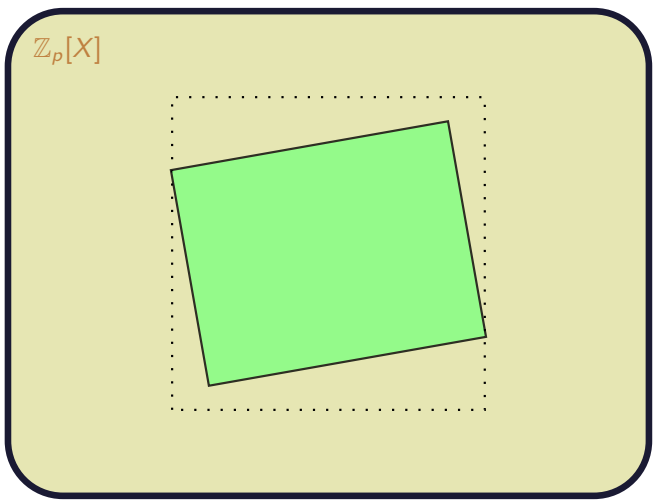


with lattice

Qualitative understanding: long-term

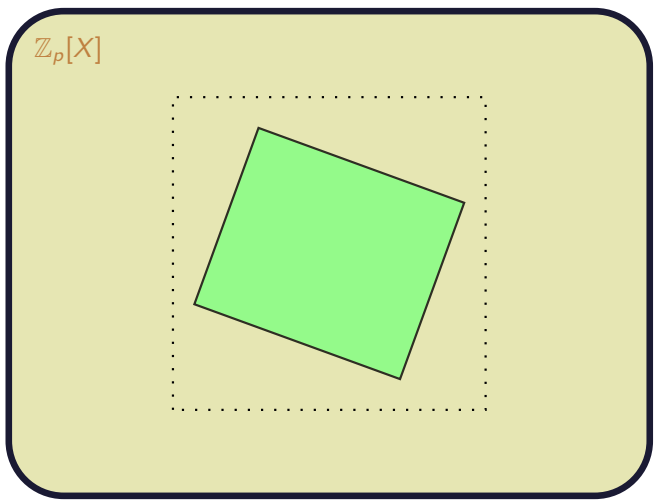
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 5$

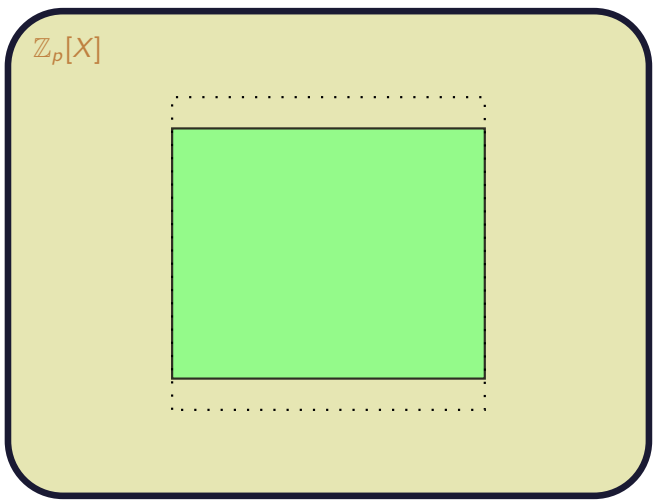


with lattice

Qualitative understanding: long-term

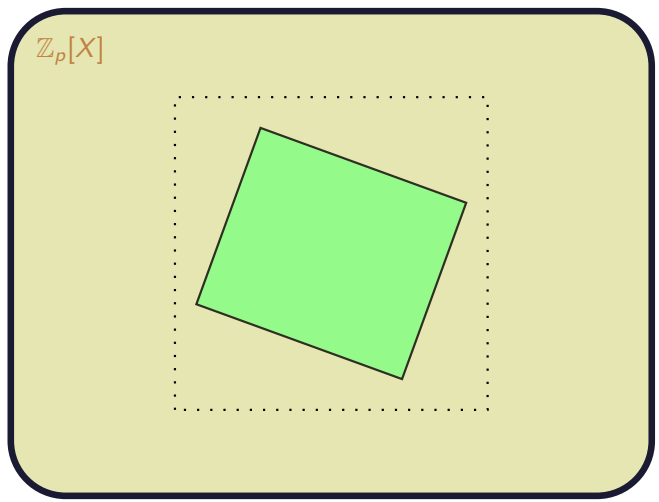
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 5$

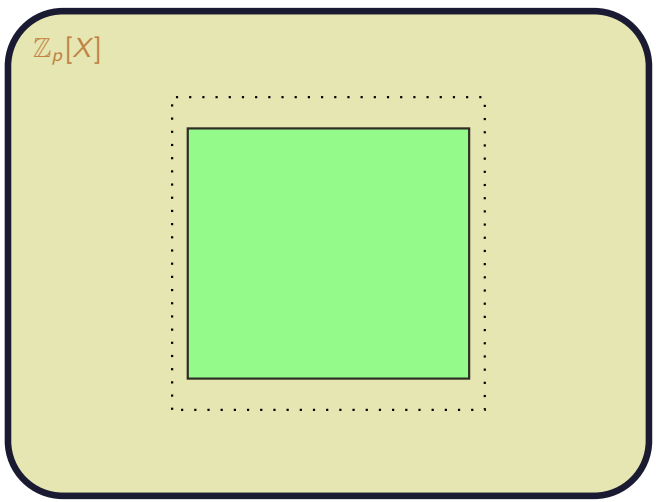


with lattice

Qualitative understanding: long-term

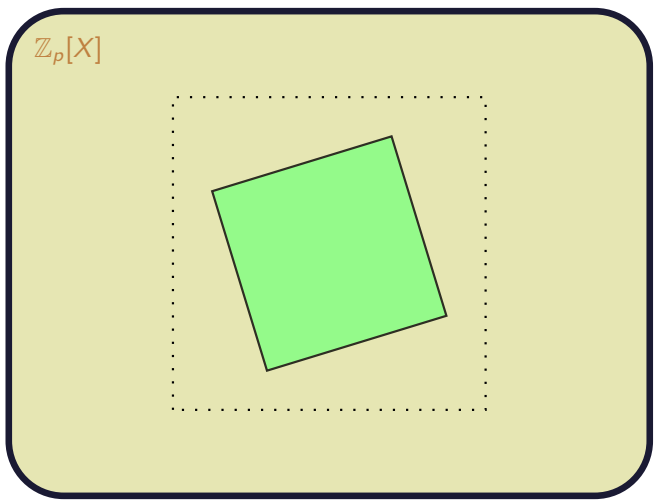
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 10$

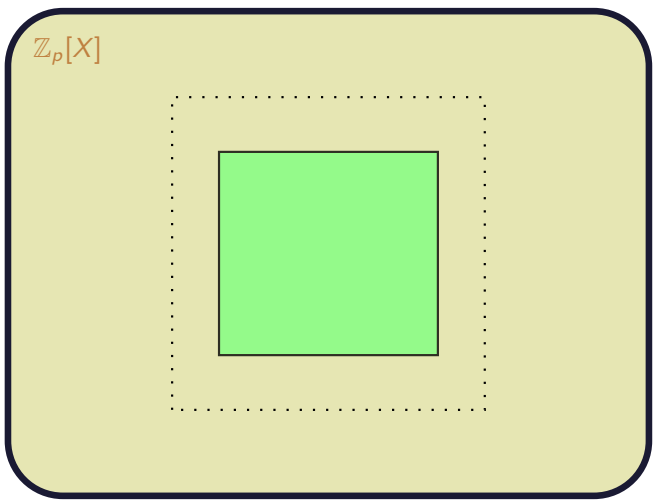


with lattice

Qualitative understanding: long-term

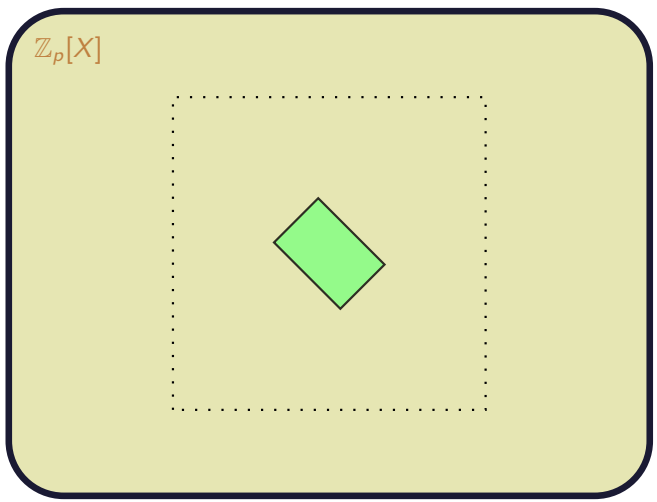
Input: $P, A_1, \ldots, A_n \in \mathbb{Z}_p[X]_d$ known at precision $O(p^N)$
Output: the product $A_1 A_2 \cdots A_n \mod P$

1. $A = 1 + O(p^N)$
2. for i in $1, 2, \ldots n$:
3. $\quad A = A \cdot A_i$
4. return A



without lattice

$i = 100$



with lattice

Table of contents

Newton polygon of a polynomial

Definition

Let $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{Q}_p[x]$ (remark: $\mathbb{Q}_p[\![x]\!]$ would also be fine).

Newton polygon of a polynomial

Definition

Let $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{Q}_p[x]$ (remark: $\mathbb{Q}_p[\![x]\!]$ would also be fine).
Let $U = \{(0, v(a_0)), \ldots, (n, v(a_n))\}$.

Newton polygon of a polynomial

Definition

Let $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{Q}_p[x]$ (remark: $\mathbb{Q}_p[\![x]\!]$ would also be fine).
Let $U = \{(0, v(a_0)), \ldots, (n, v(a_n))\}$.
We define **the Newton polygon** of f, $NP(f)$, as the **lower convex hull** of U.

Newton polygon of a polynomial

Definition

Let $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{Q}_p[x]$ (remark: $\mathbb{Q}_p[\![x]\!]$ would also be fine).
Let $U = \{(0, v(a_0)), \ldots, (n, v(a_n))\}$.
We define **the Newton polygon** of f, $NP(f)$, as the **lower convex hull** of U.
By lower convex hull, we mean the points of the convex hull of U below the straight line from $(0, (a_0))$ to $(n, v(a_n))$.

Newton polygon of a polynomial

Definition

Let $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{Q}_p[x]$ (remark: $\mathbb{Q}_p[\![x]\!]$ would also be fine).
Let $U = \{(0, v(a_0)), \ldots, (n, v(a_n))\}$.
We define **the Newton polygon** of f, $NP(f)$, as the **lower convex hull** of U.
By lower convex hull, we mean the points of the convex hull of U below the straight line from $(0, (a_0))$ to $(n, v(a_n))$.

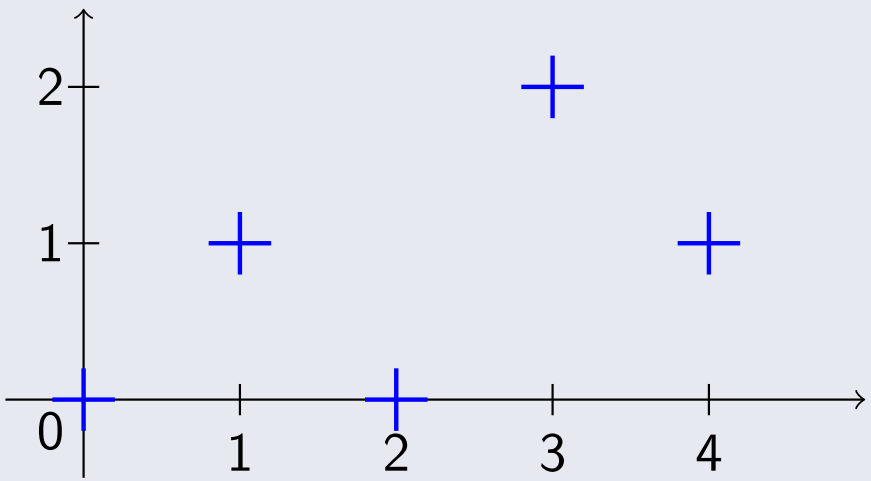
Proposition

Let $Newt_f$ be the (point-wise) biggest convex mapping below U. Then the graph of $Newt_f$ is (the lower frontier of) $NP(f)$.

例

A Newton polygon

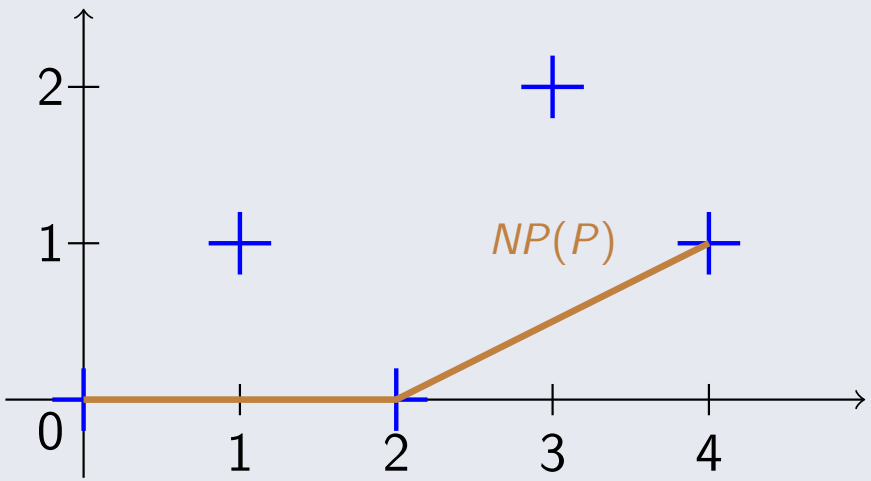
$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$



例

A Newton polygon

$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$



Vocabulary

Definition

A *slope of the Newton polygon* of f is an element of $Newt'_f([0, n])$.

Definition

If λ is a slope of $Newt_f$, we call *segment of slope* λ of $Newt_f$ the set $\{(x, Newt_f(x)) / Newt'_f(x) = \lambda\}$.

Definition

The *length* of this slope is the length of its projection on the x-axis.

Fundamental theorem of Newton polygons

Theorem

*f has a root of valuation λ **iff** $-\lambda$ is a slope of $Newt_f$.*

Fundamental theorem of Newton polygons

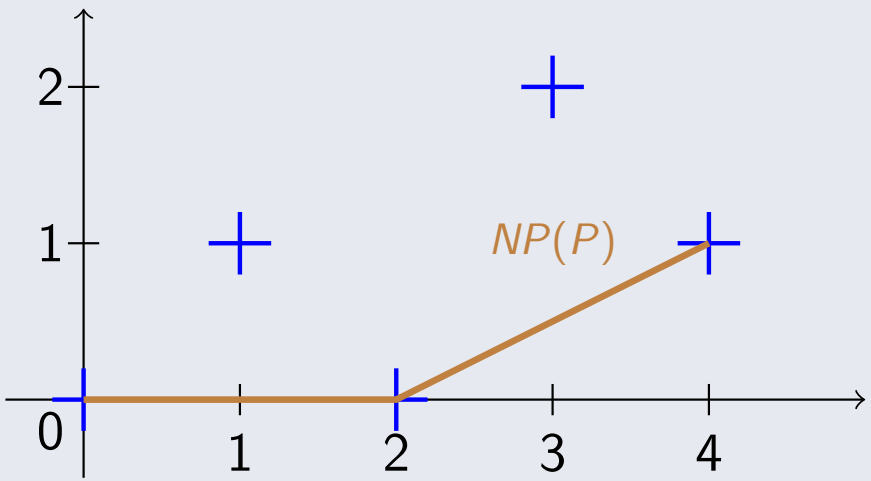
Theorem

*f has a root of valuation λ **iff** $-\lambda$ is a slope of $Newt_f$.*
Moreover, the number of roots of f (with multiplicity) of valuation λ, is the length of the segment of slope $-\lambda$ of $Newt_f$.

例

A Newton polygon

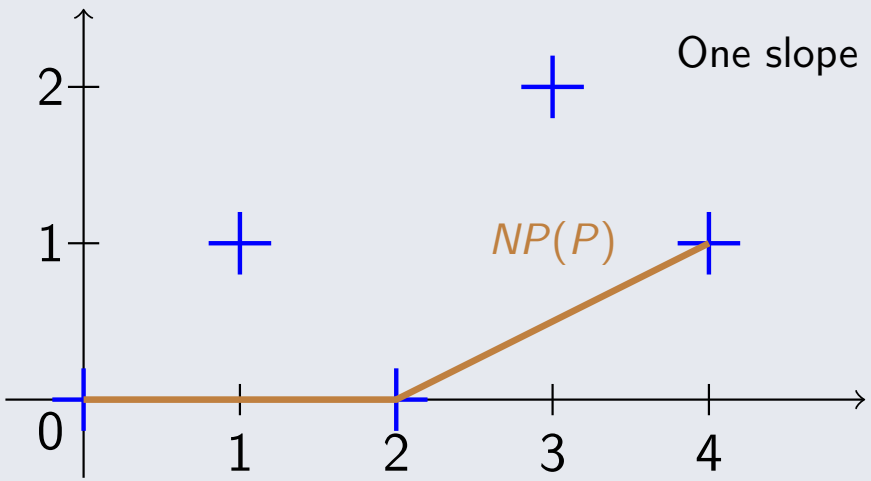
$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$



例

A Newton polygon

$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$

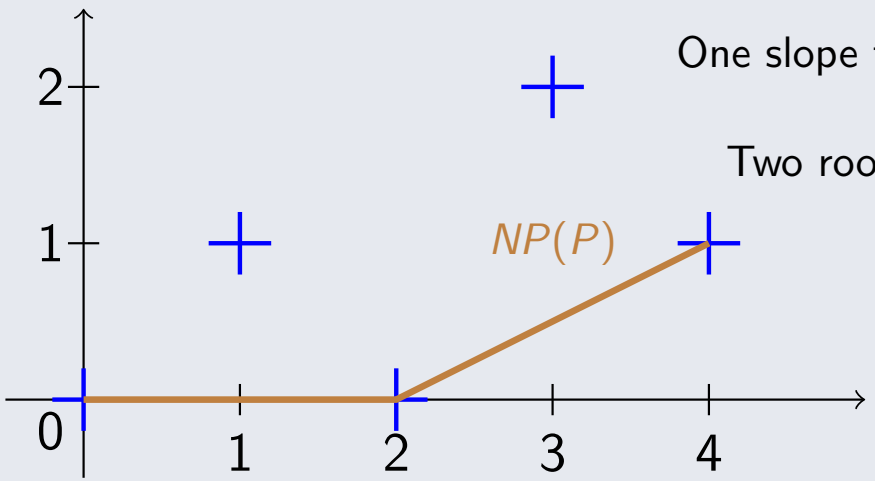


One slope for 0 of length 2, one slope 1/2 of length 2.

例

A Newton polygon

$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$



One slope for 0 of length 2, one slope $1/2$ of length 2.

Two roots of valuation 0, two of valuation $-1/2$.

Basic operations

Proposition (Addition)

If f and g are two polynomials, then the Newton polygon of $f+g$ can be ***lower-bounded*** *by taking the lower convex hull for the vertices of $Newt_f$ and $Newt_g$.*

Basic operations

Proposition (Addition)

If f and g are two polynomials, then the Newton polygon of $f+g$ can be ***lower-bounded*** *by taking the lower convex hull for the vertices of Newt_f and Newt_g.*

Proposition (Multiplicativity)

If f and g are two polynomials, then the Newton polygon of fg has for slopes that of f and g, with length the sum of that of f and g.

Some remarks

Proposition

If $P \in \mathbb{Q}_p[X]$ is irreducible, then all its roots have the same valuation. Hence, $Newt_P$ has only one slope.

Remark

The converse is false. For instance, $(X-1)(X-2)$ over $\mathbb{Q}_5$.

Some remarks

Proposition

If $P \in \mathbb{Q}_p[X]$ is irreducible, then all its roots have the same valuation. Hence, $Newt_P$ has only one slope.

Remark

The converse is false. For instance, $(X-1)(X-2)$ over $\mathbb{Q}_5$.

Corollary

If $Newt_P$ has more than one slope, P is not irreducible.

Some remarks

Proposition

If $P \in \mathbb{Q}_p[X]$ is irreducible, then all its roots have the same valuation. Hence, $Newt_P$ has only one slope.

Remark

The converse is false. For instance, $(X-1)(X-2)$ over $\mathbb{Q}_5$.

Corollary

If $Newt_P$ has more than one slope, P is not irreducible.

Remark

There are good irreducibility criterion based on testing whether one slope can be obtained by multiplication (namely, Dumas and Eisenstein).

Table of contents

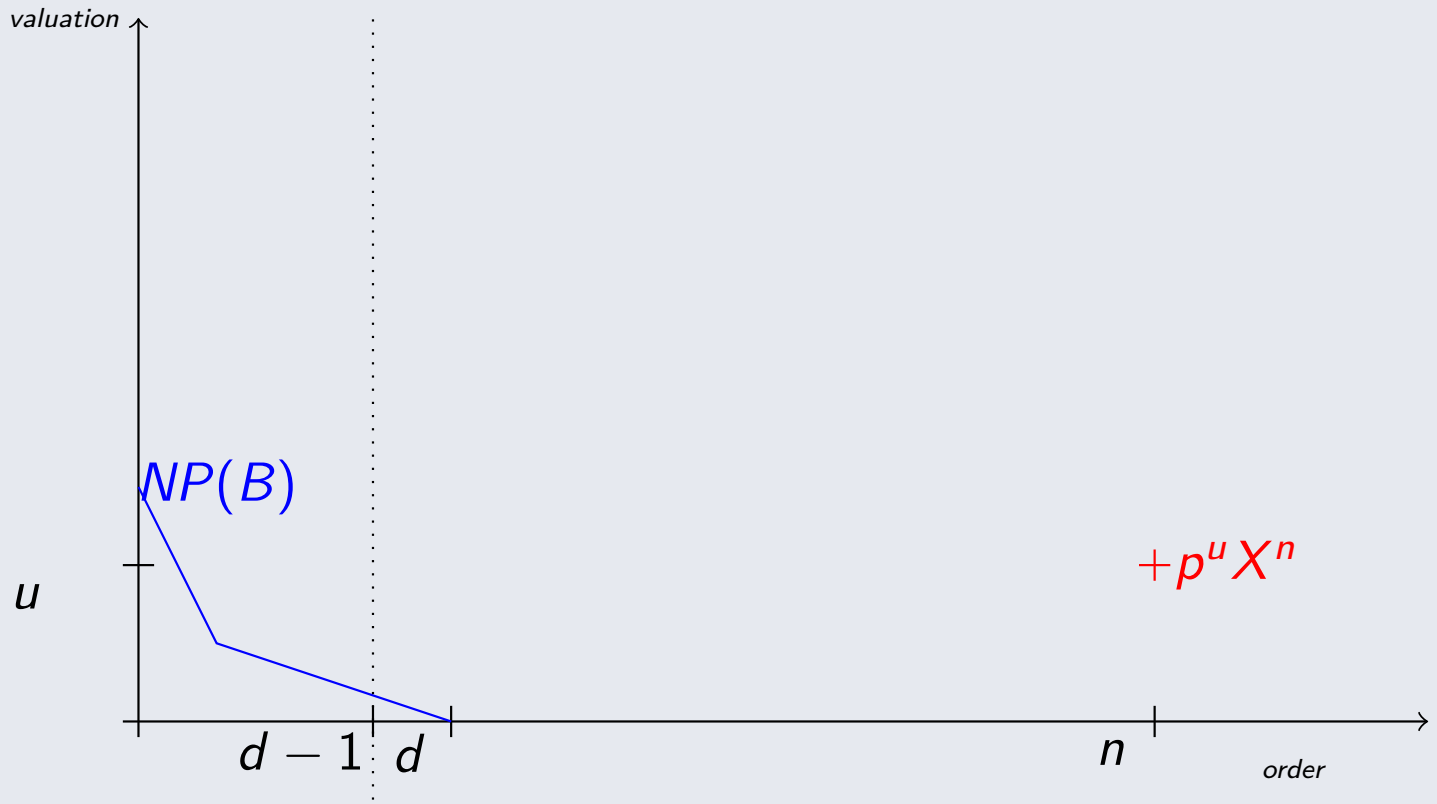
Euclidean division and Newton polygon

Lemma (Division lemma)

- *What is the Newton polygon of the* ***remainder*** *in the division of A by B (in $\mathbb{Q}_p[X]$)?*
- *What is the Newton polygon of the* ***quotient*** *in the division of A by B (in $\mathbb{Q}_p[X]$)?*

Euclidean division and Newton polygon

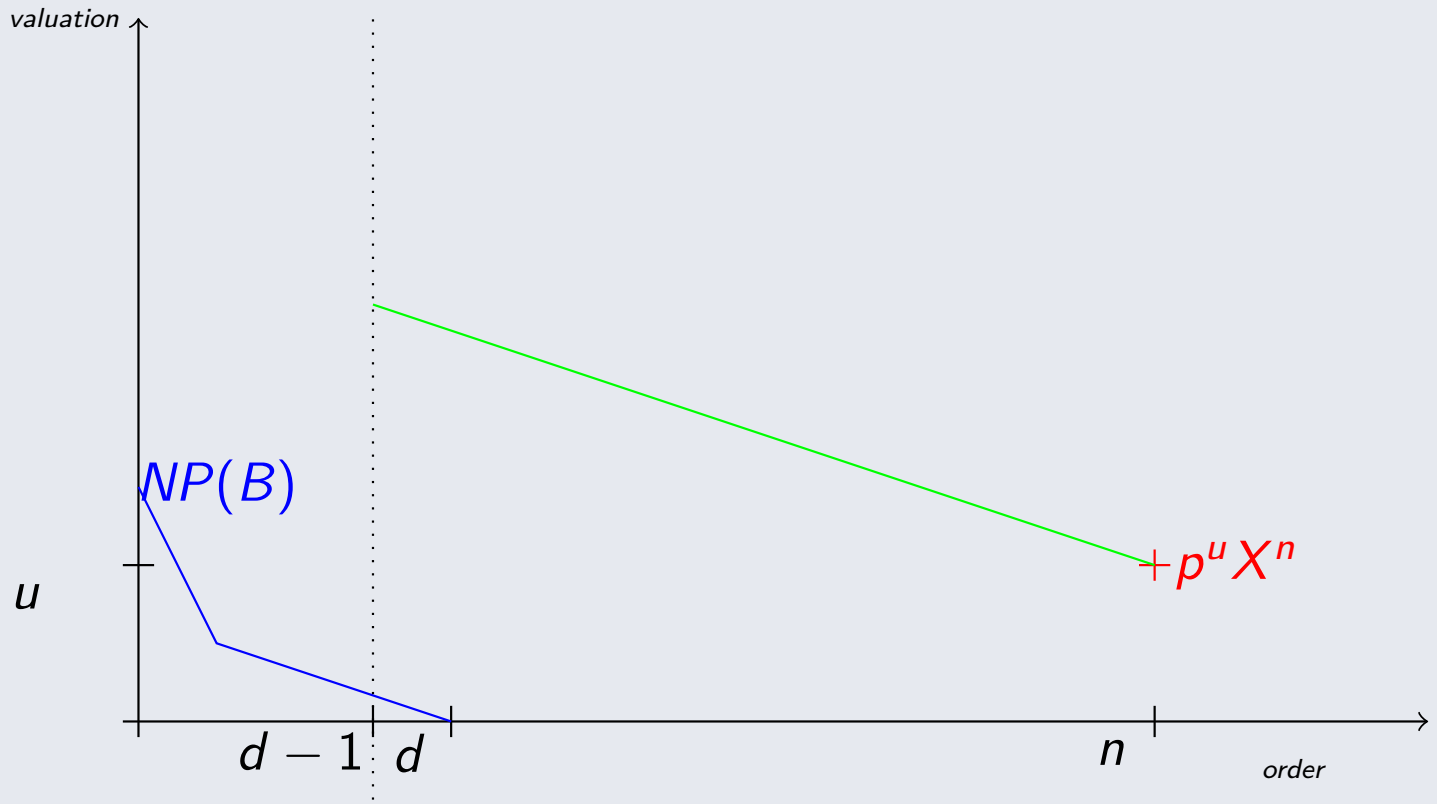
Lemma (Division lemma)



Division of $p^u X^n$ *by* B : $p^u X^n = BQ + R$

Euclidean division and Newton polygon

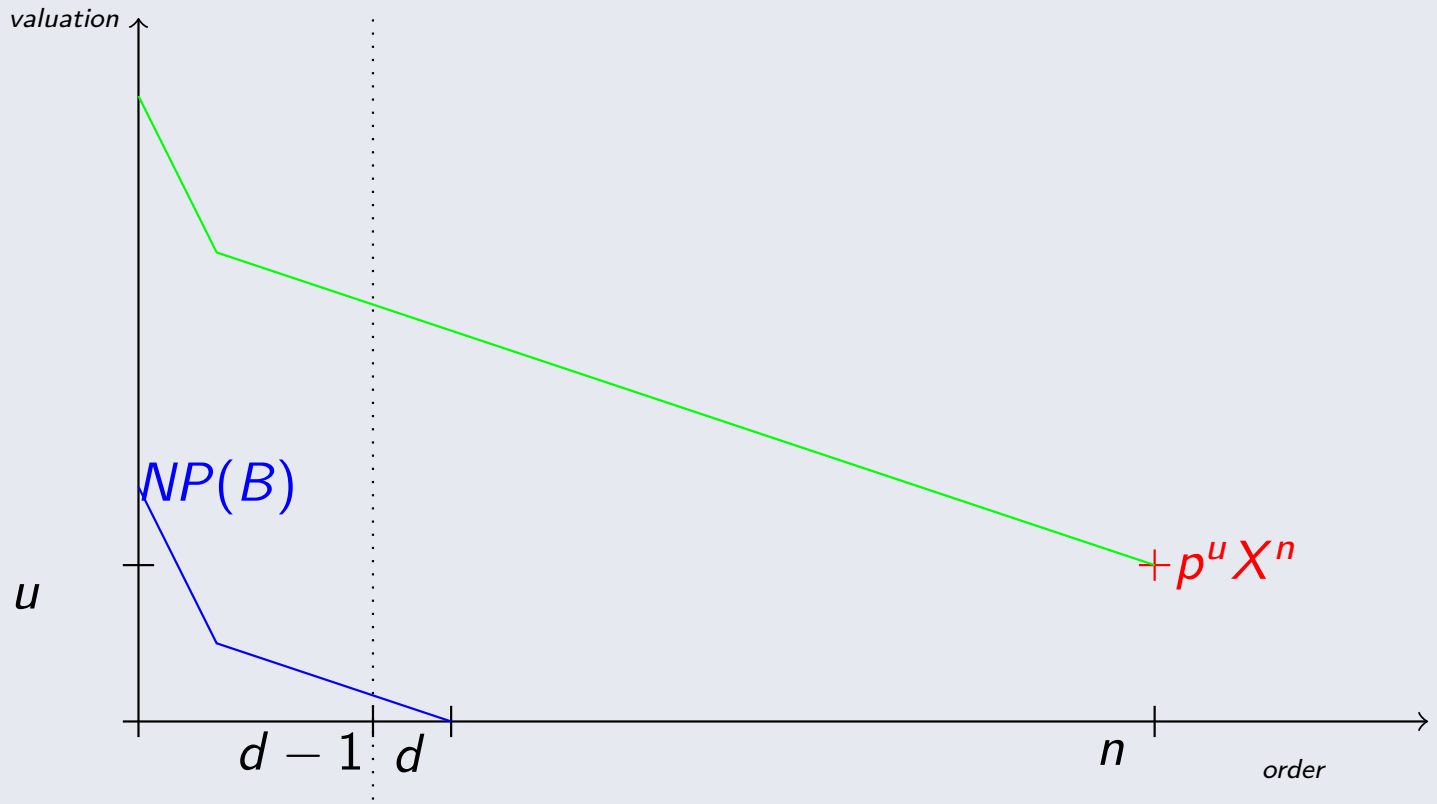
Lemma (Division lemma)



Division of $p^u X^n$ *by* B : $p^u X^n = BQ + R$

Euclidean division and Newton polygon

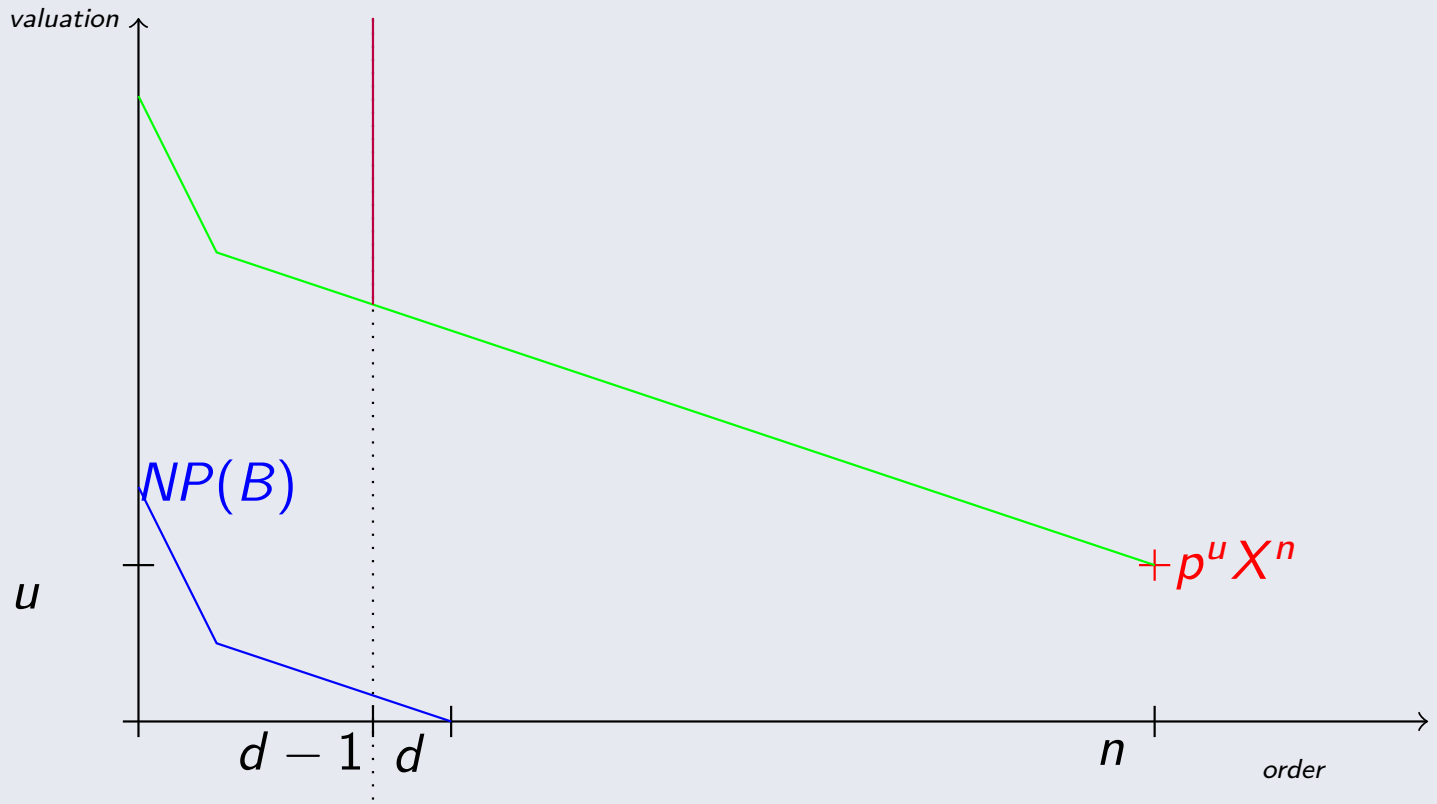
Lemma (Division lemma)



Division of p^uX^n *by* B : $p^uX^n = BQ + R$

Euclidean division and Newton polygon

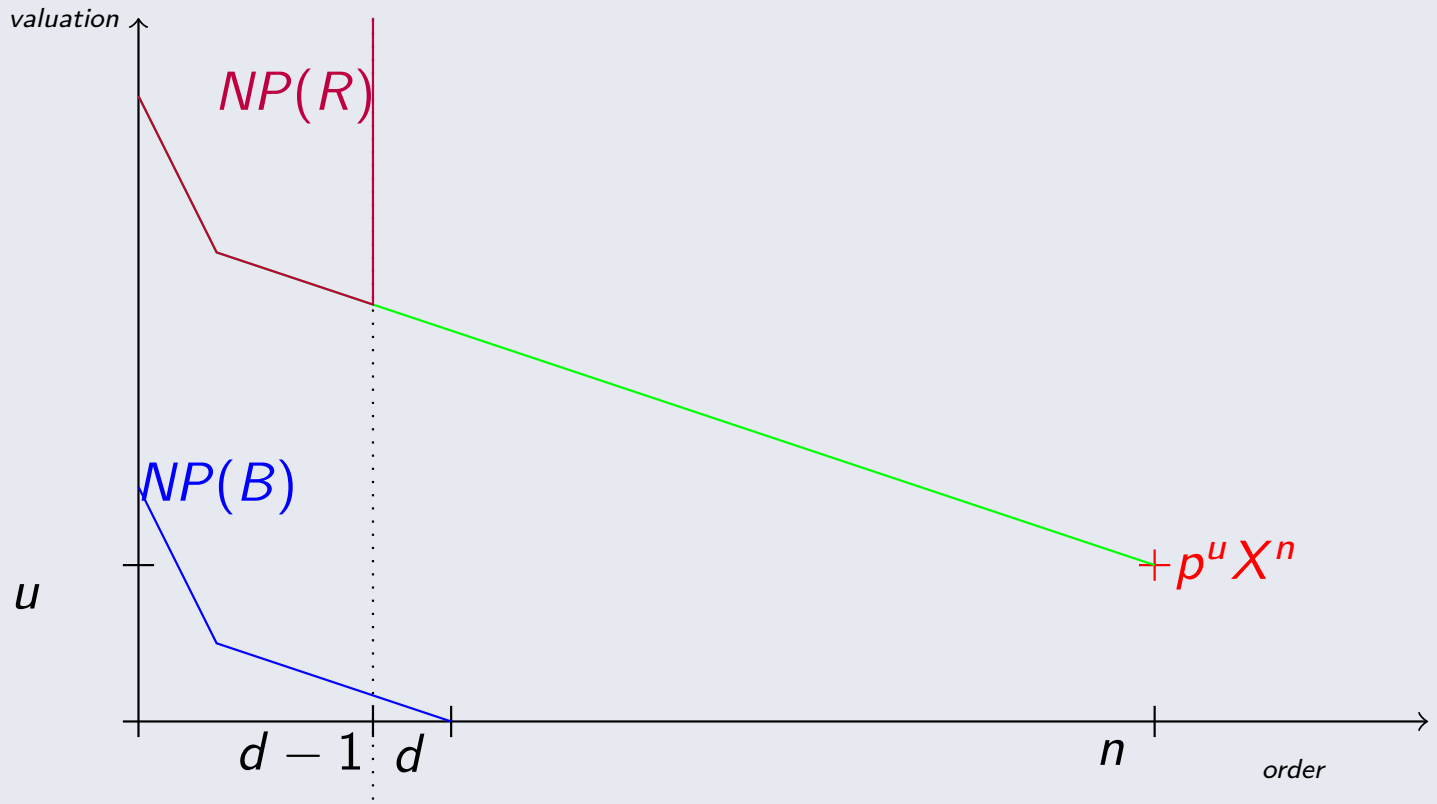
Lemma (Division lemma)



Division of p^uX^n *by* B : $p^uX^n = BQ + R$

Euclidean division and Newton polygon

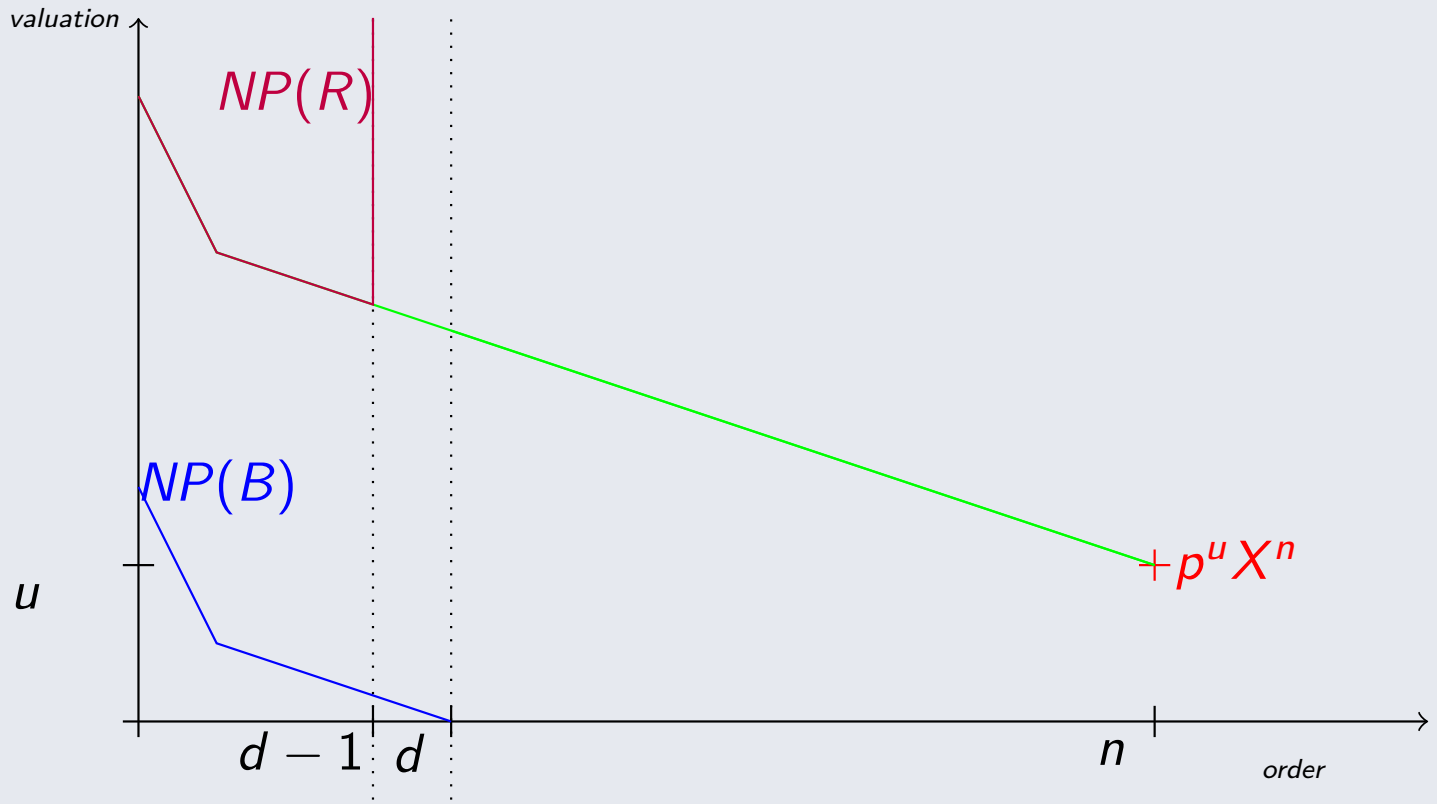
Lemma (Division lemma)



Division of $p^u X^n$ *by* B : $p^u X^n = BQ + R$

Euclidean division and Newton polygon

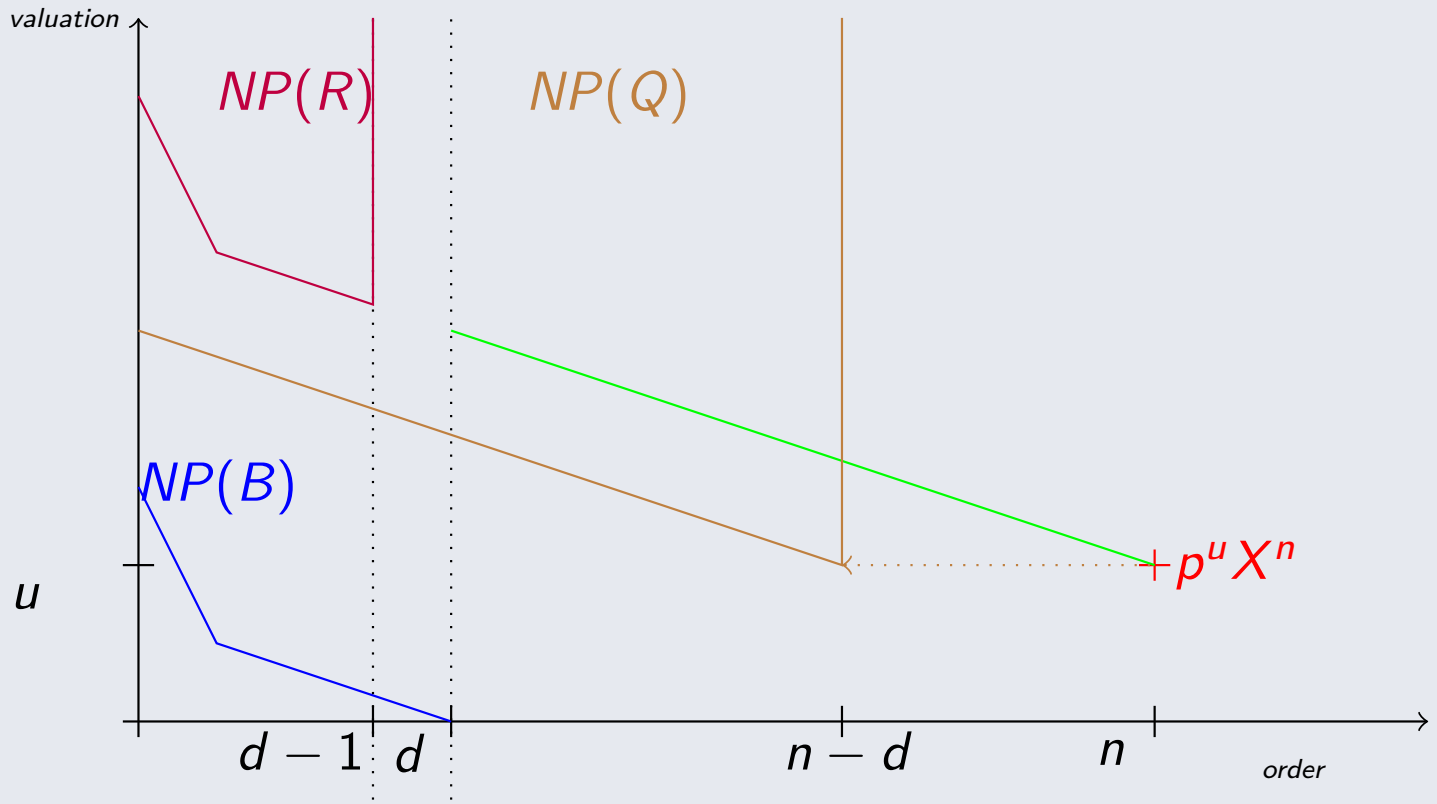
Lemma (Division lemma)



Division of $p^u X^n$ *by* B : $p^u X^n = BQ + R$

Euclidean division and Newton polygon

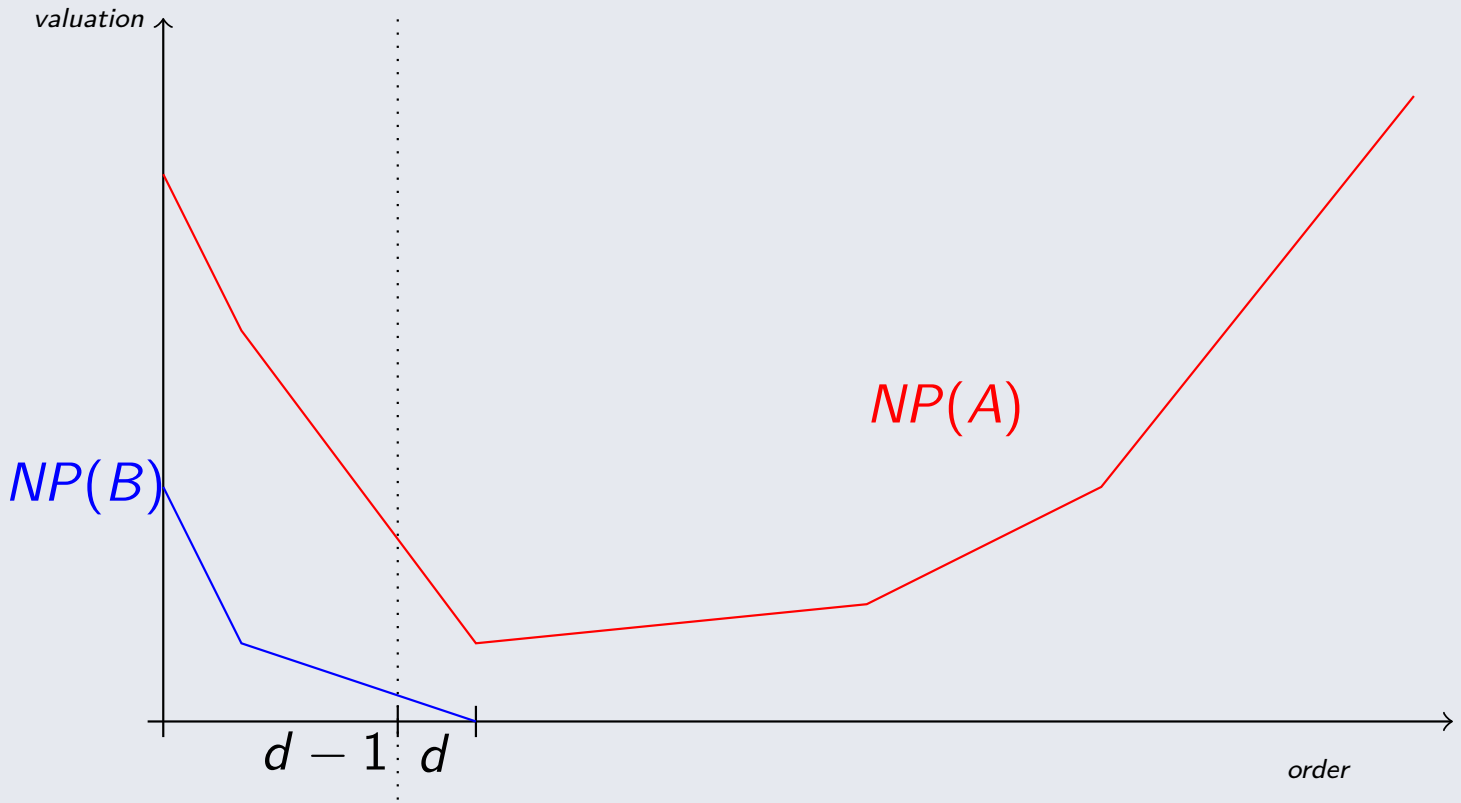
Lemma (Division lemma)



Division of p^uX^n *by* B : $p^uX^n = BQ + R$

Euclidean division and Newton polygon

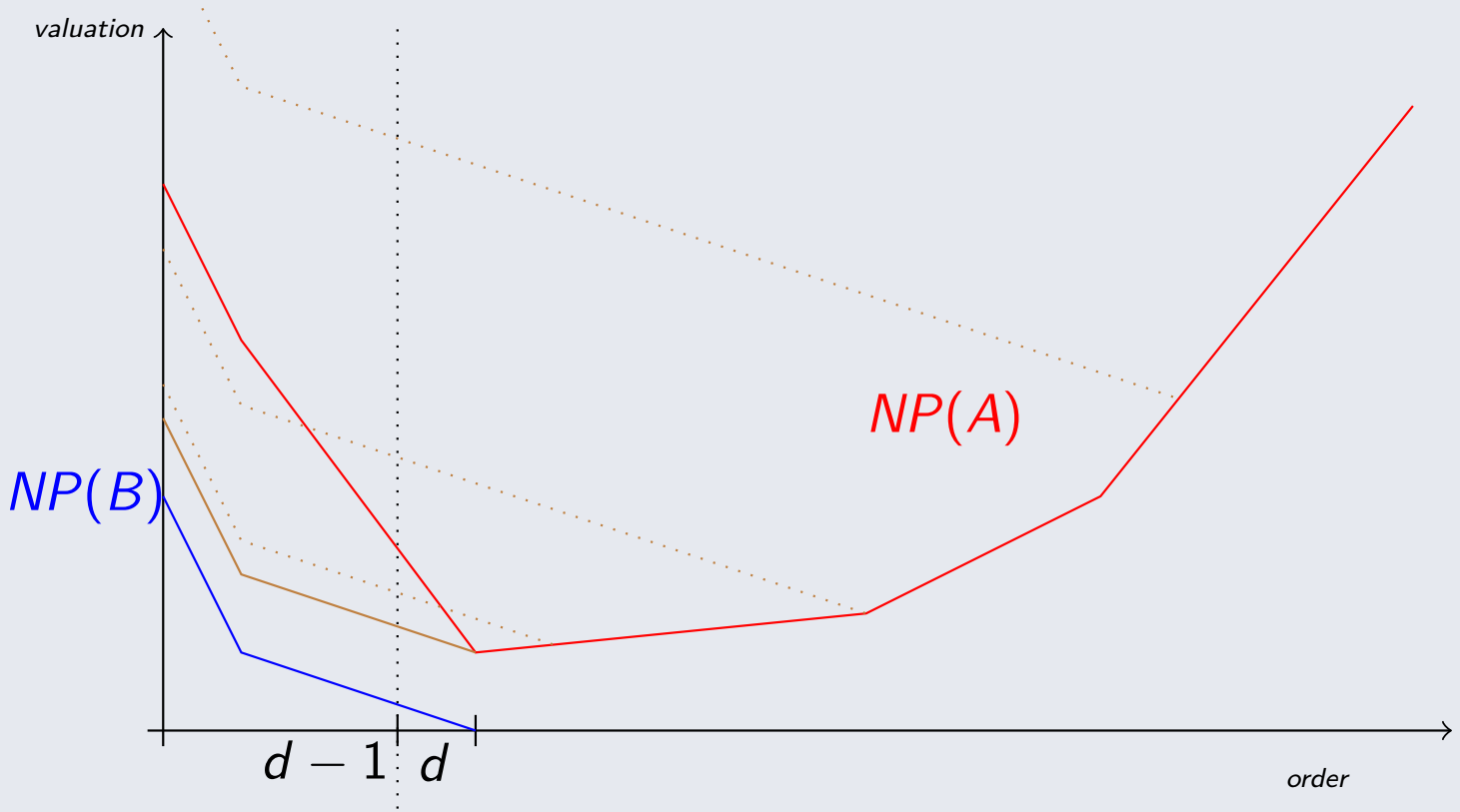
Lemma (Division lemma)



Division of A by B : $A = BQ + R$

Euclidean division and Newton polygon

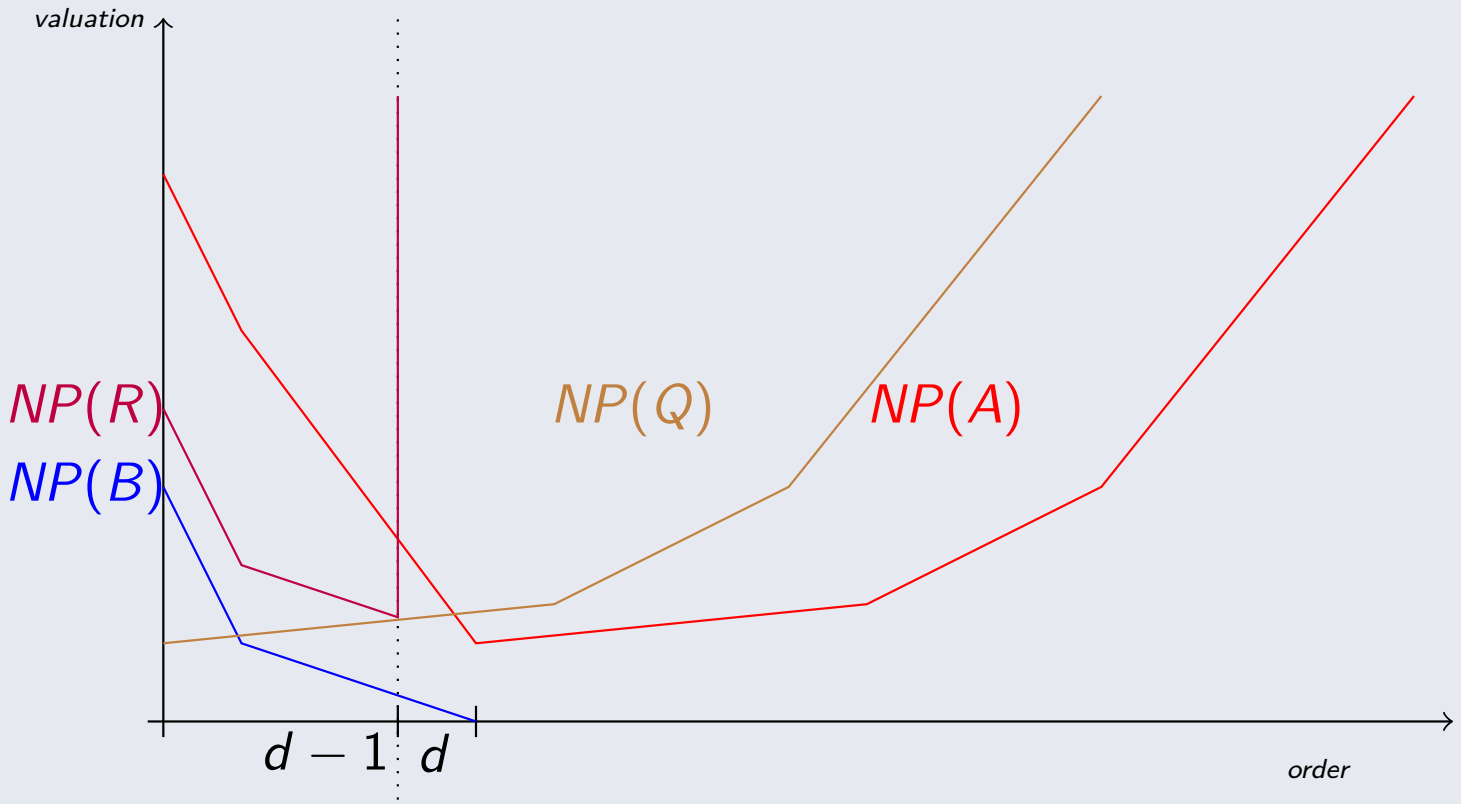
Lemma (Division lemma)



Division of A by B : $A = BQ + R$

Euclidean division and Newton polygon

Lemma (Division lemma)



Division of A by B : $A = BQ + R$

Table of contents

Handling the precision

Lattice precision

A and B are known with precision lattice H_A and H_B. Then (H_Q, H_R) are given by the Euclidean division of $H_A - QH_B$ by B.

Handling the precision

Lattice precision

A and B are known with precision lattice H_A and H_B. Then (H_Q, H_R) are given by the Euclidean division of $H_A - QH_B$ by B.

Newton precision

For $A = BQ + R$ with A known with precision-polygon φ, we can apply the previous construction to φ **divided** by B to obtain the precision on Q and R.

Handling the precision

Lattice precision

A and B are known with precision lattice H_A and H_B. Then (H_Q, H_R) are given by the Euclidean division of $H_A - QH_B$ by B.

Newton precision

For $A = BQ + R$ with A known with precision-polygon φ, we can apply the previous construction to φ **divided** by B to obtain the precision on Q and R.

Remark

This proved to be useful to handle precision for the computation of the characteristic polynomial.

Comparison: $\prod_{i=1}^{n} A_i \mod M$

Modulus M	n	Gain of precision		
		Jagged	Newton	Lattice (not dif. + dif.)
$X^5 + X^2 + 1$ (Irred. mod 2)	10	0.2	0.2	0.2 + 0.0
	50	4.2	4.2	4.2 + 0.0
	100	11.2	11.2	11.2 + 0.0
$X^5 + 1$ (Sep. mod 2)	10	0.4	0.4	0.9 + 6.0
	50	5.6	5.6	11.1 + 42.0
	100	13.6	13.6	27.0 + 87.0
$X^5 + 2$ (Eisenstein)	10	6.2	6.2	6.2 + 0.0
	50	44.0	44.0	44.0 + 0.0
	100	92.5	92.5	92.5 + 0.0
$(X+1)^5 + 2$ (Shift Eisenstein)	10	0.6	0.6	4.7 + 1.4
	50	7.1	7.1	42.6 + 1.4
	100	15.1	15.1	91.8 + 1.4
$X^5 + X + 2$ (Two slopes)	10	1.7	1.7	7.9 + 9.8
	50	8.1	8.1	70.7 + 59.8
	100	16.1	16.1	152.6 + 125.9

Figure: Precision for modular multiplication

Table of contents

Factoring respecting slopes

Theorem

Let $f \in \mathbb{Q}_p[X]$. Then,

Factoring respecting slopes

Theorem

Let $f \in \mathbb{Q}_p[X]$. Then,

- *We can write $f = \prod_i f_i$.*

Factoring respecting slopes

Theorem

Let $f \in \mathbb{Q}_p[X]$. Then,

- *We can write $f = \prod_i f_i$.*
- *The f_i's are all of **one slope**.*

Factoring respecting slopes

Theorem

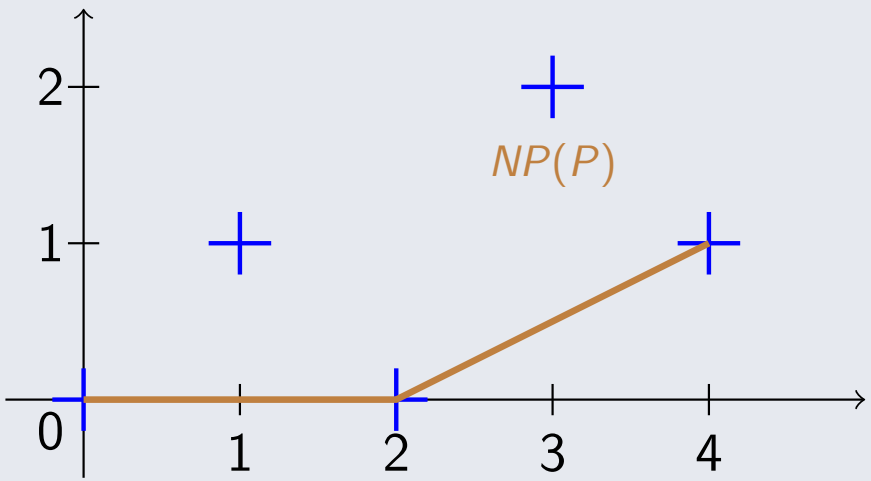
Let $f \in \mathbb{Q}_p[X]$. Then,

- *We can write $f = \prod_i f_i$.*
- *The f_i's are all of **one slope**.*
- *They have **respectively different slopes**.*

例

A Newton polygon

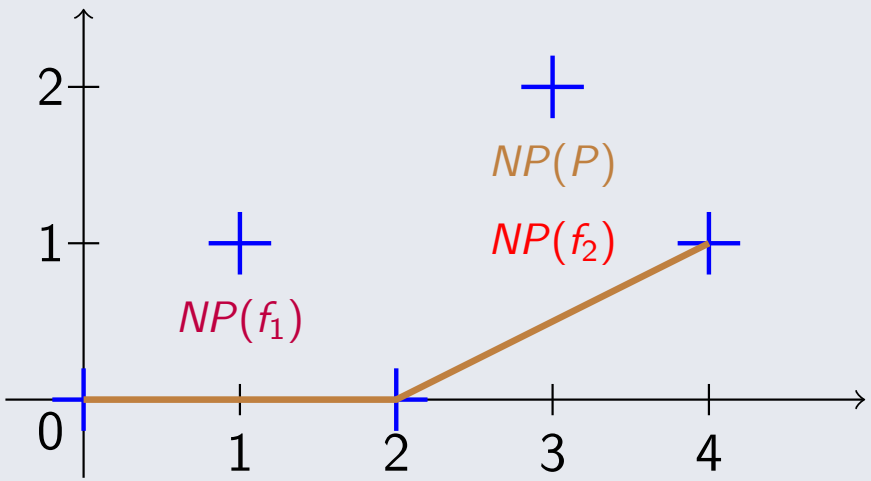
$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$.



例

A Newton polygon

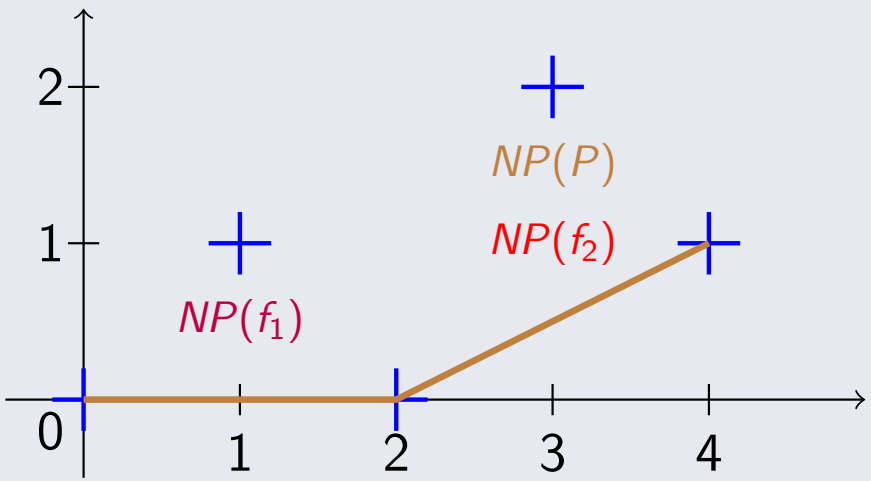
$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$.



例

A Newton polygon

$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$.

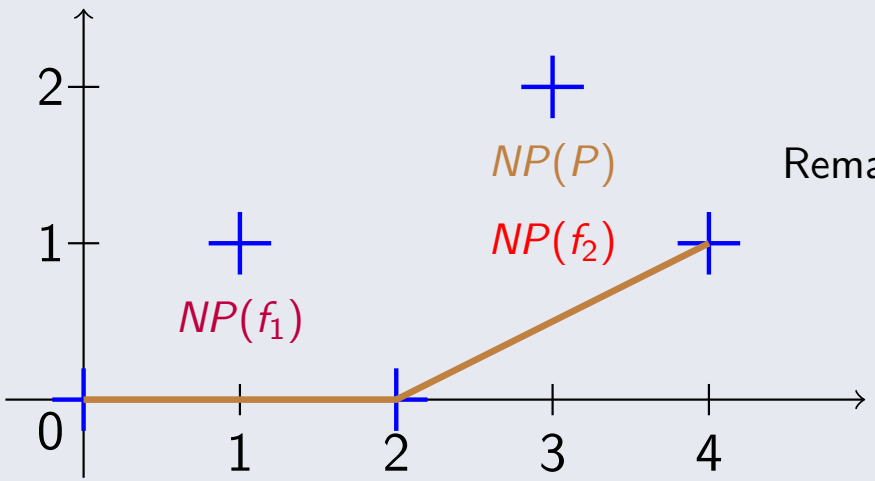


$$P = (2 + 3X + X^2) \times (1 + 3X^2)$$

例

A Newton polygon

$P = 2 + 3X + 7X^2 + 9X^3 + 3X^4$, over $\mathbb{Q}_3$.



$$P = (2 + 3X + X^2) \times (1 + 3X^2)$$

Remark: $2 + 3X + X^2 = (1 + X)(1 + 2X)$.

A Newton iteration

The iteration

Already found in *Polynomial root finding over local rings and application to error correcting codes* by Berthomieu, Lecerf, Quintin:

$$\begin{aligned} A_{i+1} &:= A_i + (V_i P \mod A_i) \\ B_{i+1} &:= P \ \backslash\text{quo}\ A_{i+1} \\ V_{i+1} &:= (2V_i - V_i^2 B_{i+1}) \mod A_{i+1} \end{aligned}$$

The result

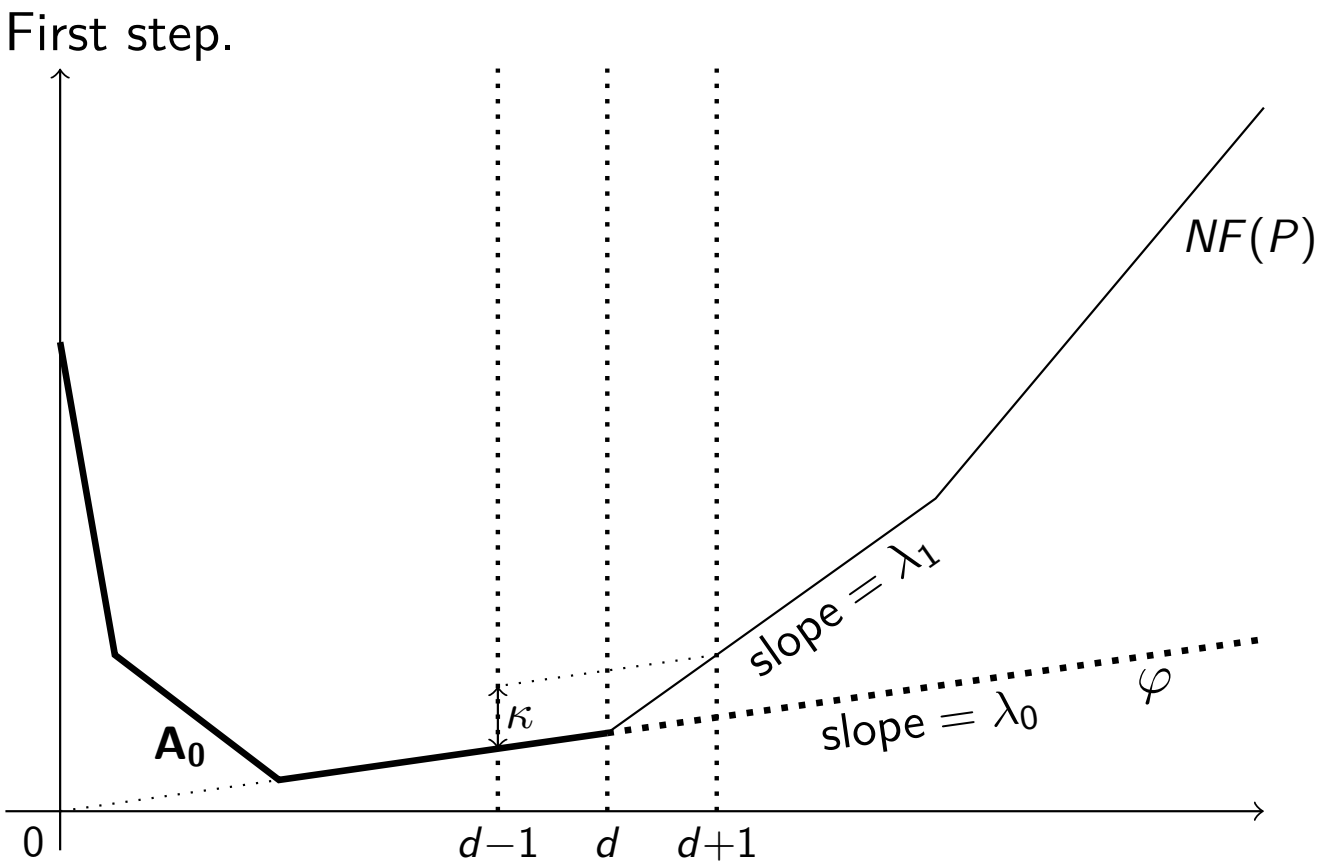
A_i, B_i, V_i converge **quadratically** to A, B, V such that $AB = P$, V is the inverse of B modulo A and A, B have the desired Newton polygons.

Ideas on the proof

About the proof

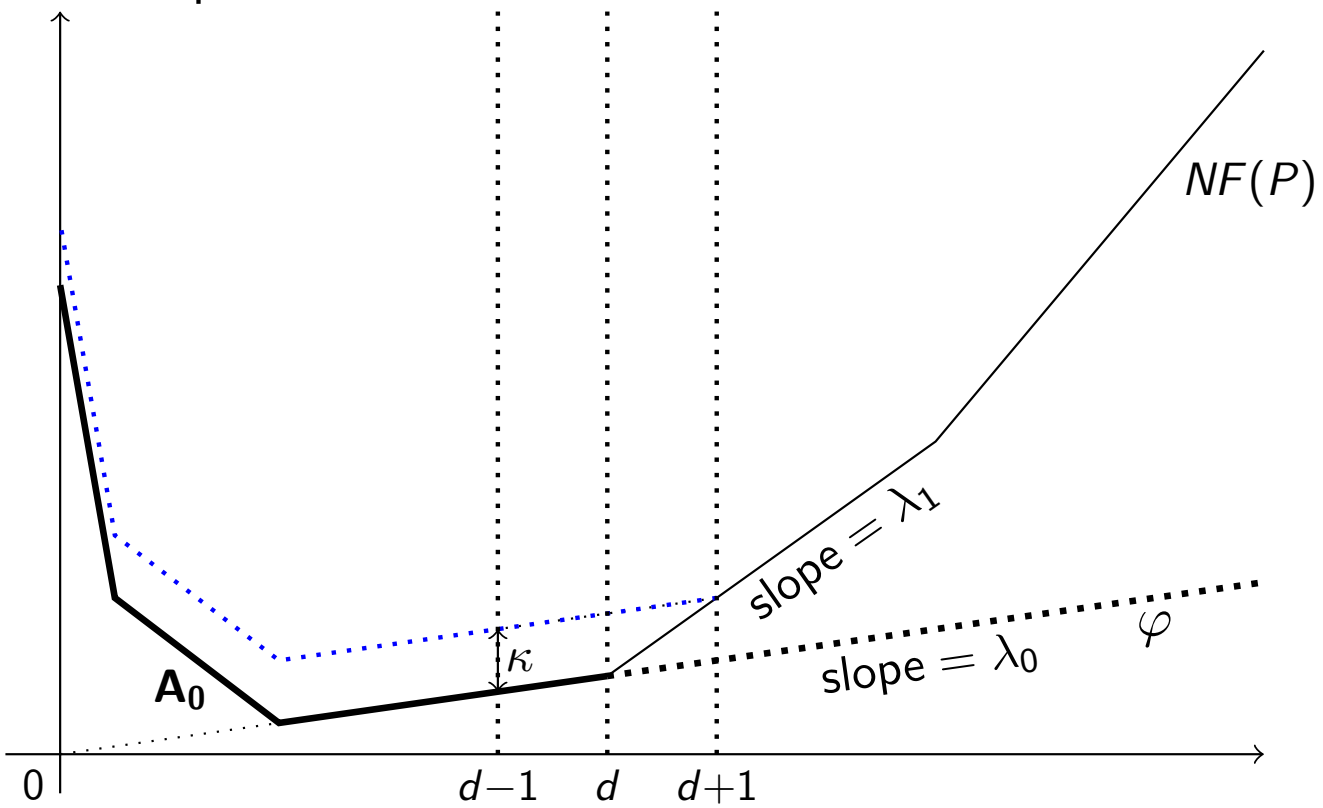
- We monitor $R_i = A_{i+1} - A_i$ and $S_i = P \mod A_i$.
- We prove that both $NP(R_i)$ and $NP(S_i)$ goes to infinity.

Illustration

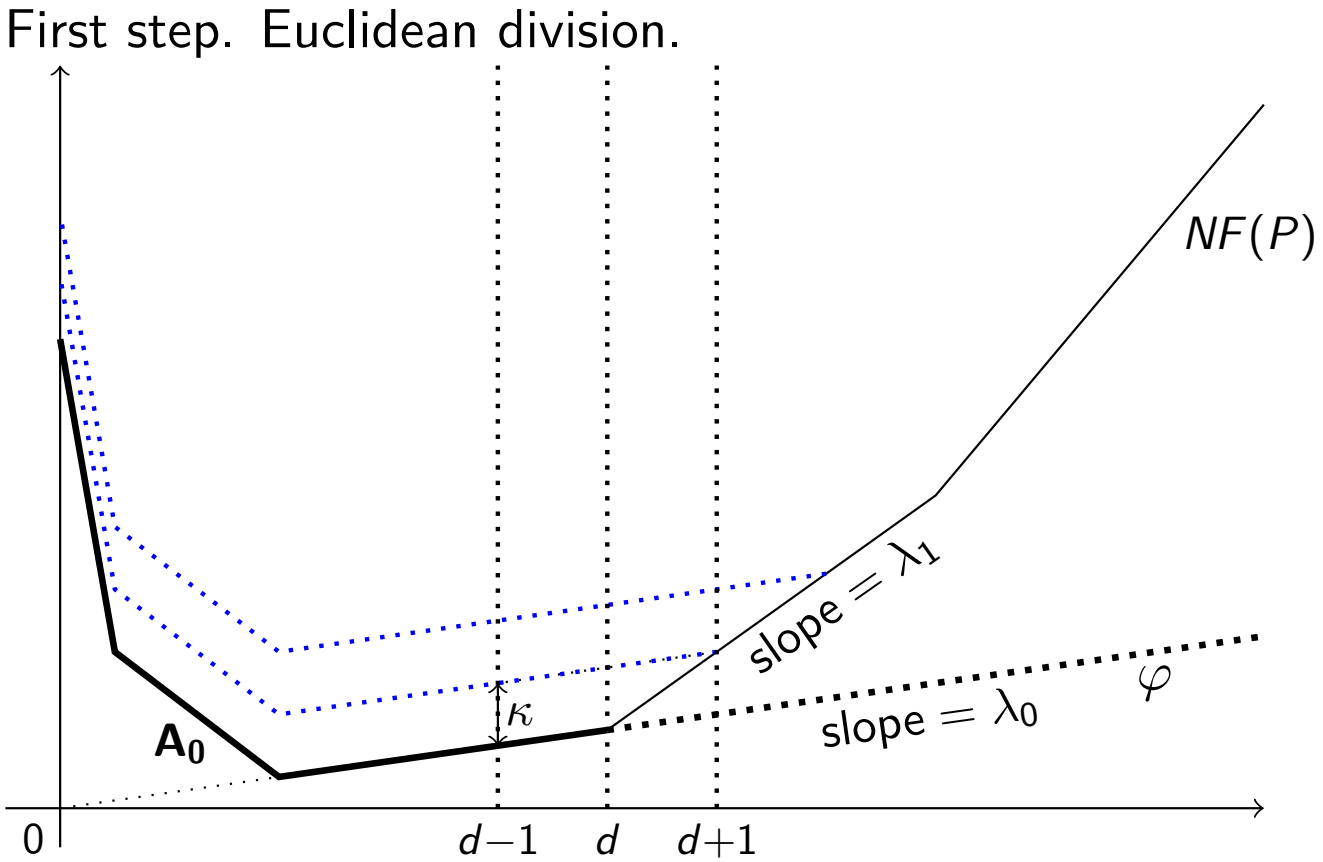


Illustration

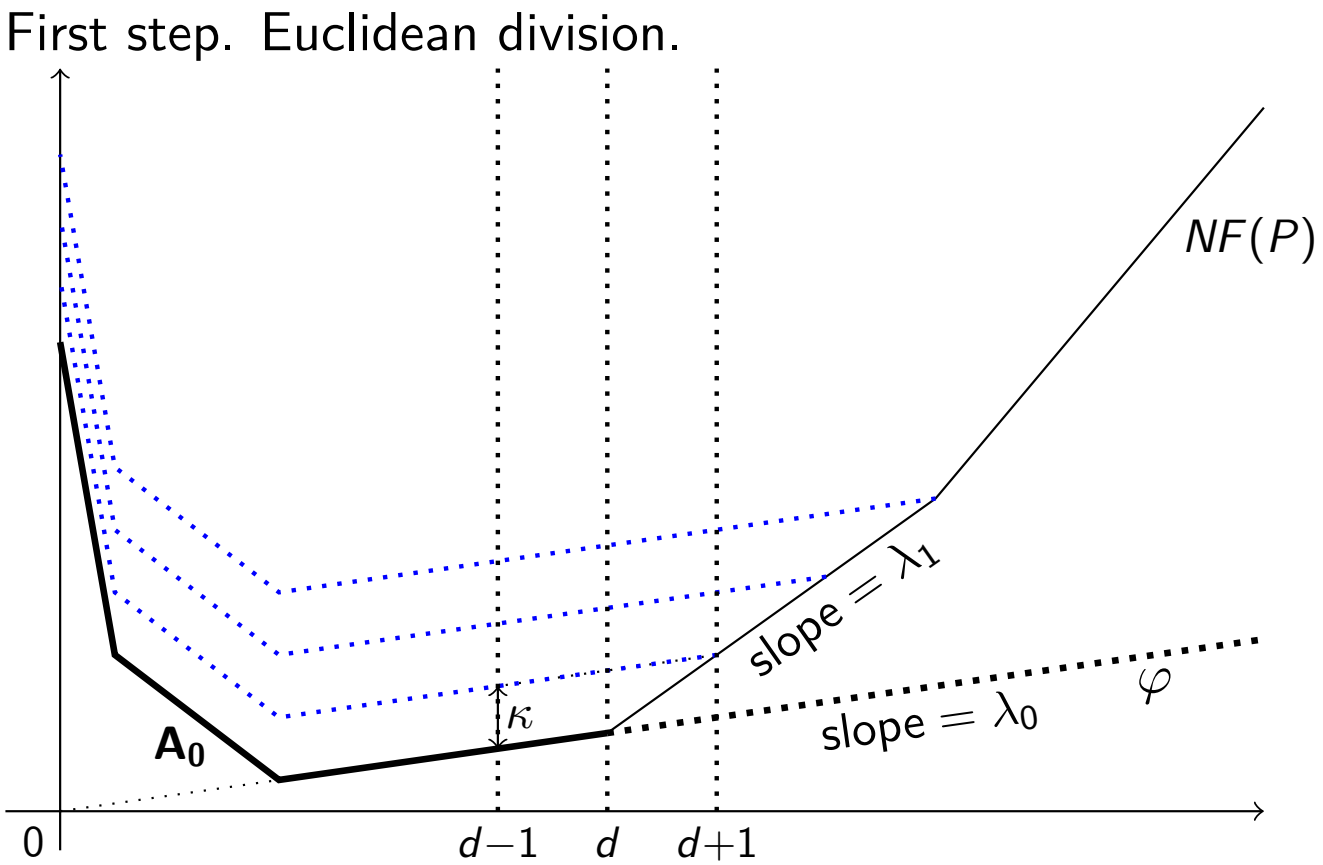
First step. Euclidean division.



Illustration

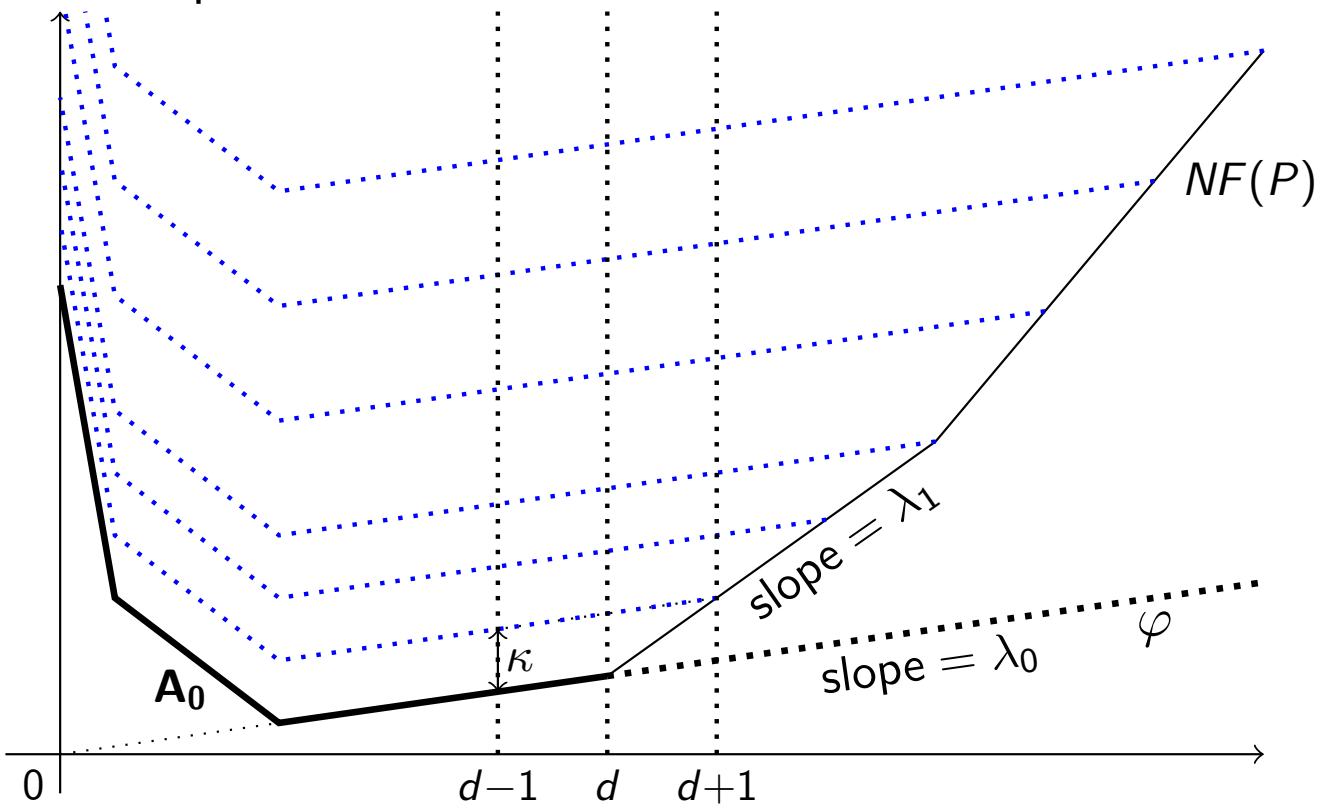


Illustration



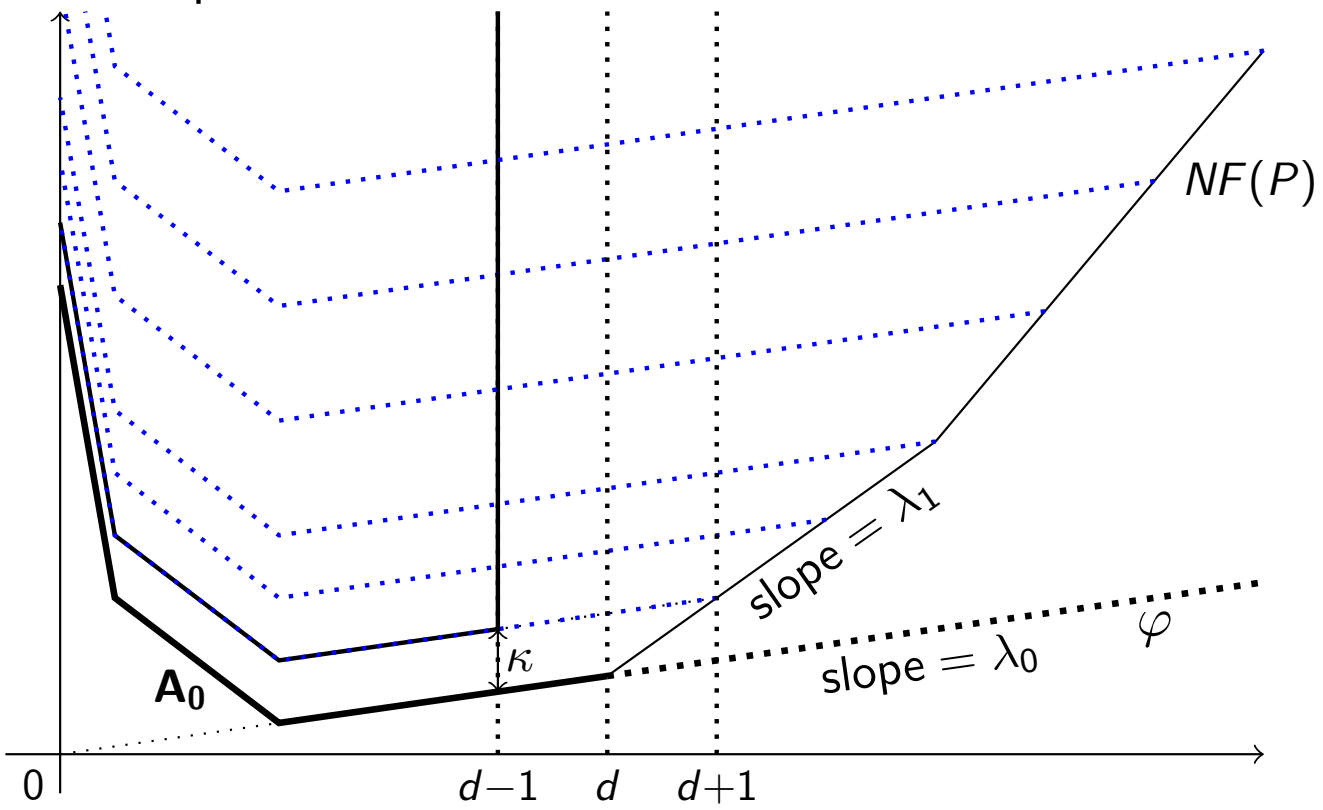
Illustration

First step. Euclidean division.



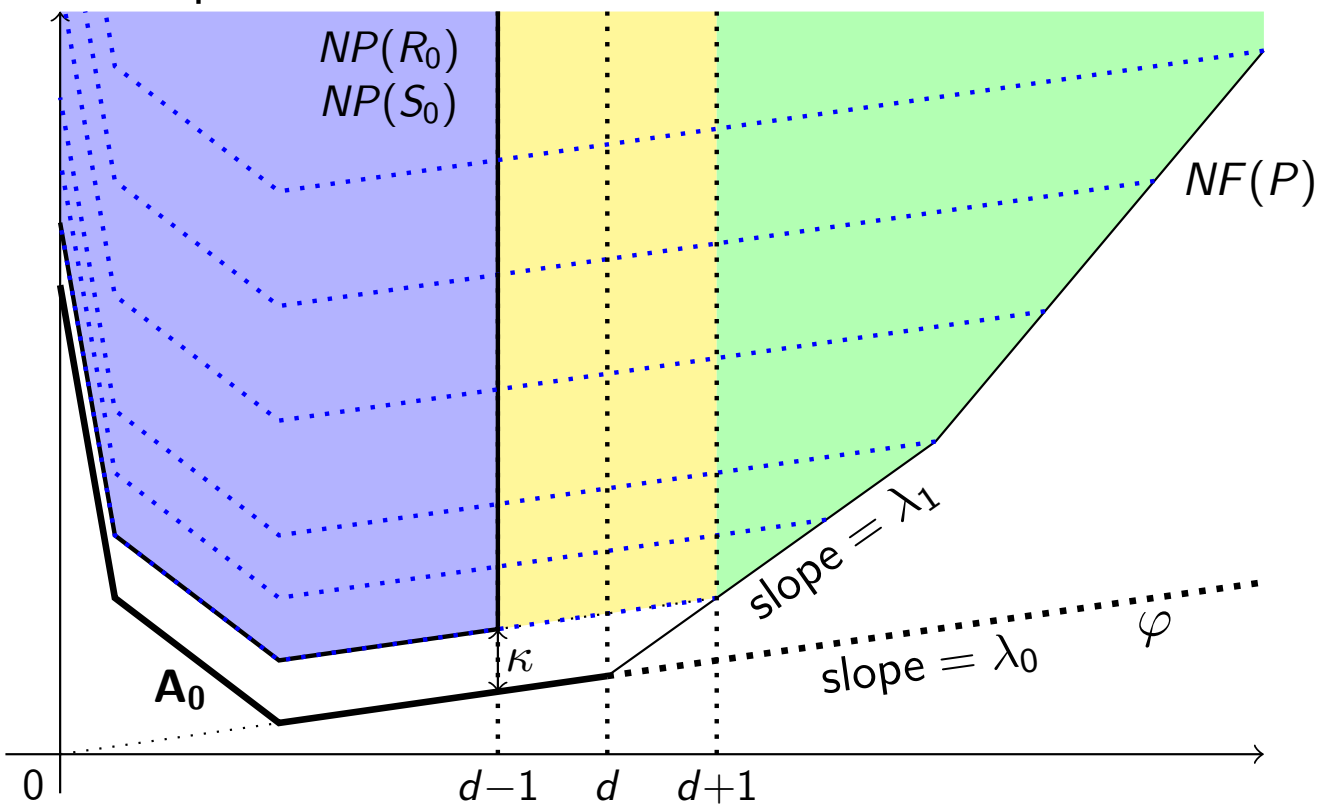
Illustration

First step. Euclidean division.



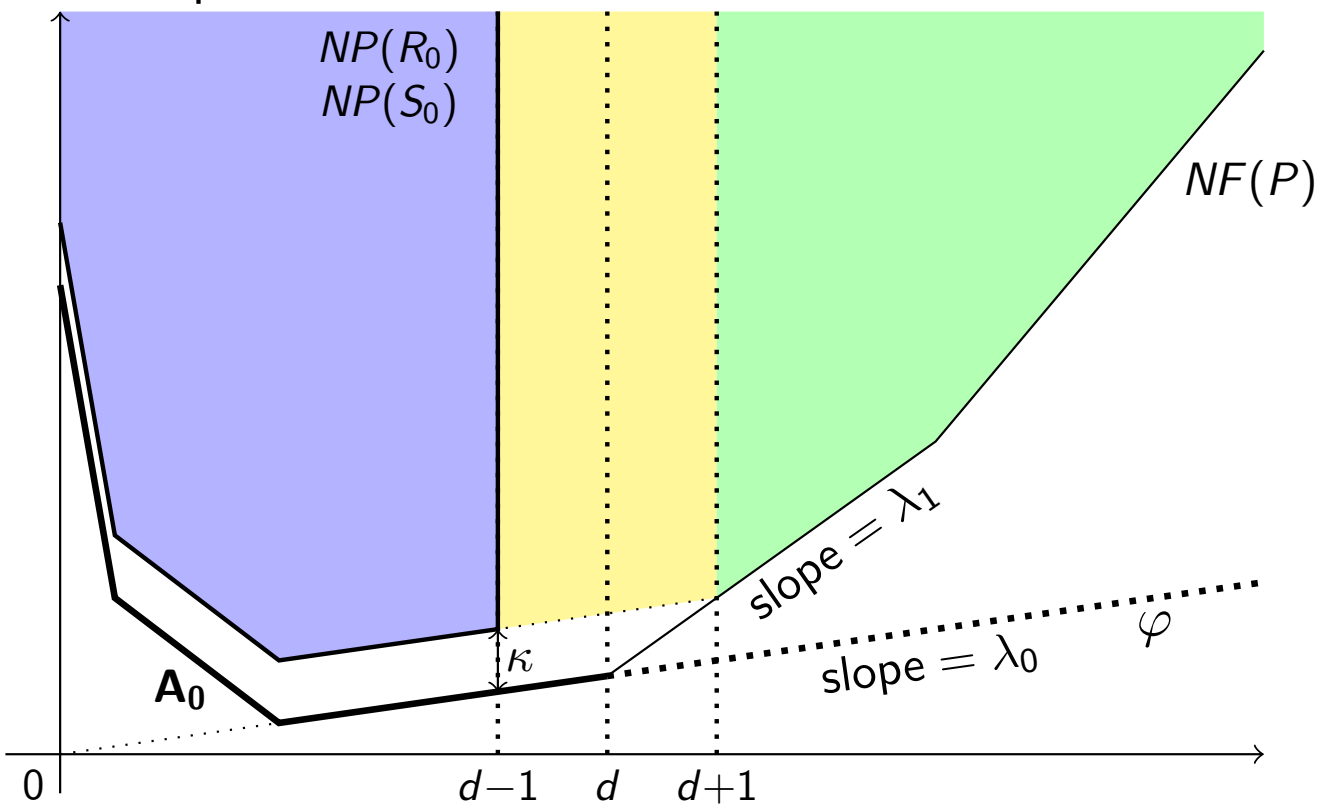
Illustration

First step.



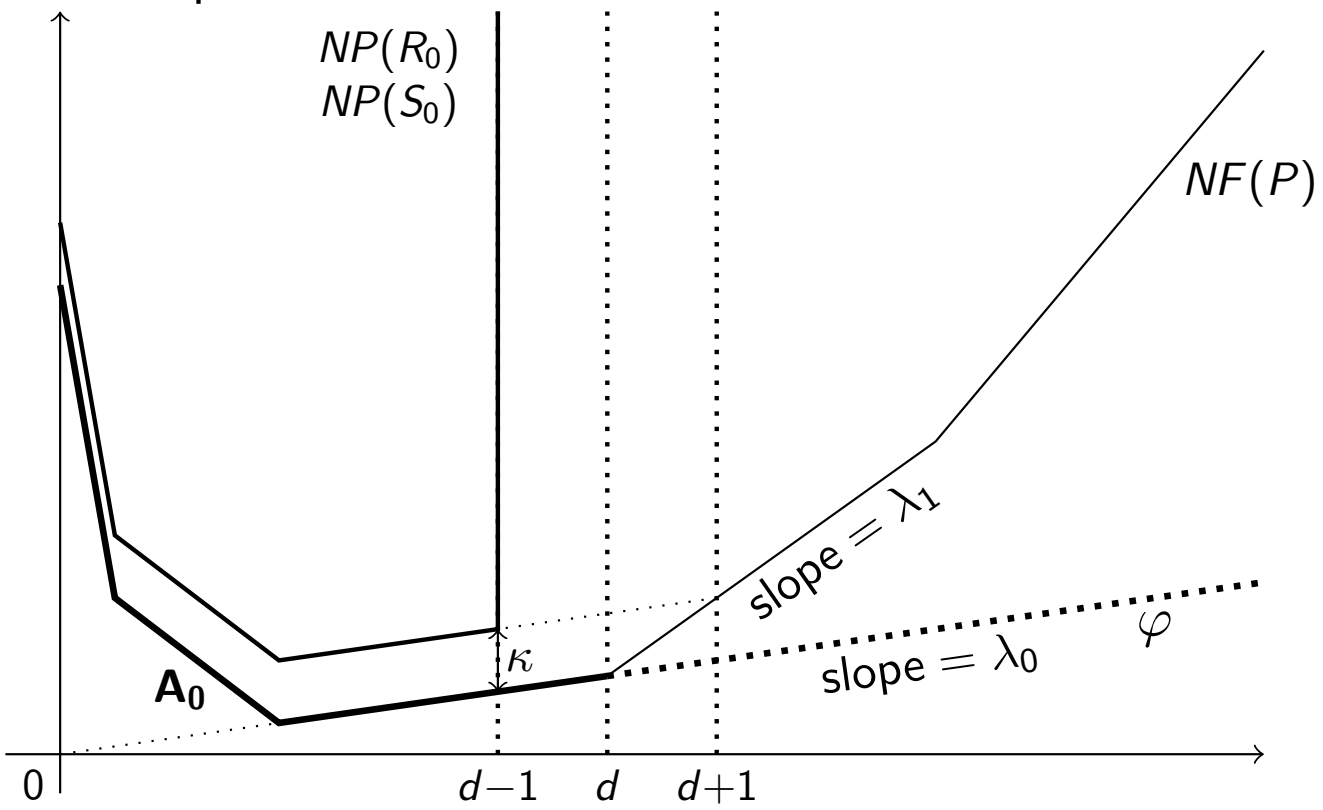
Illustration

First step.

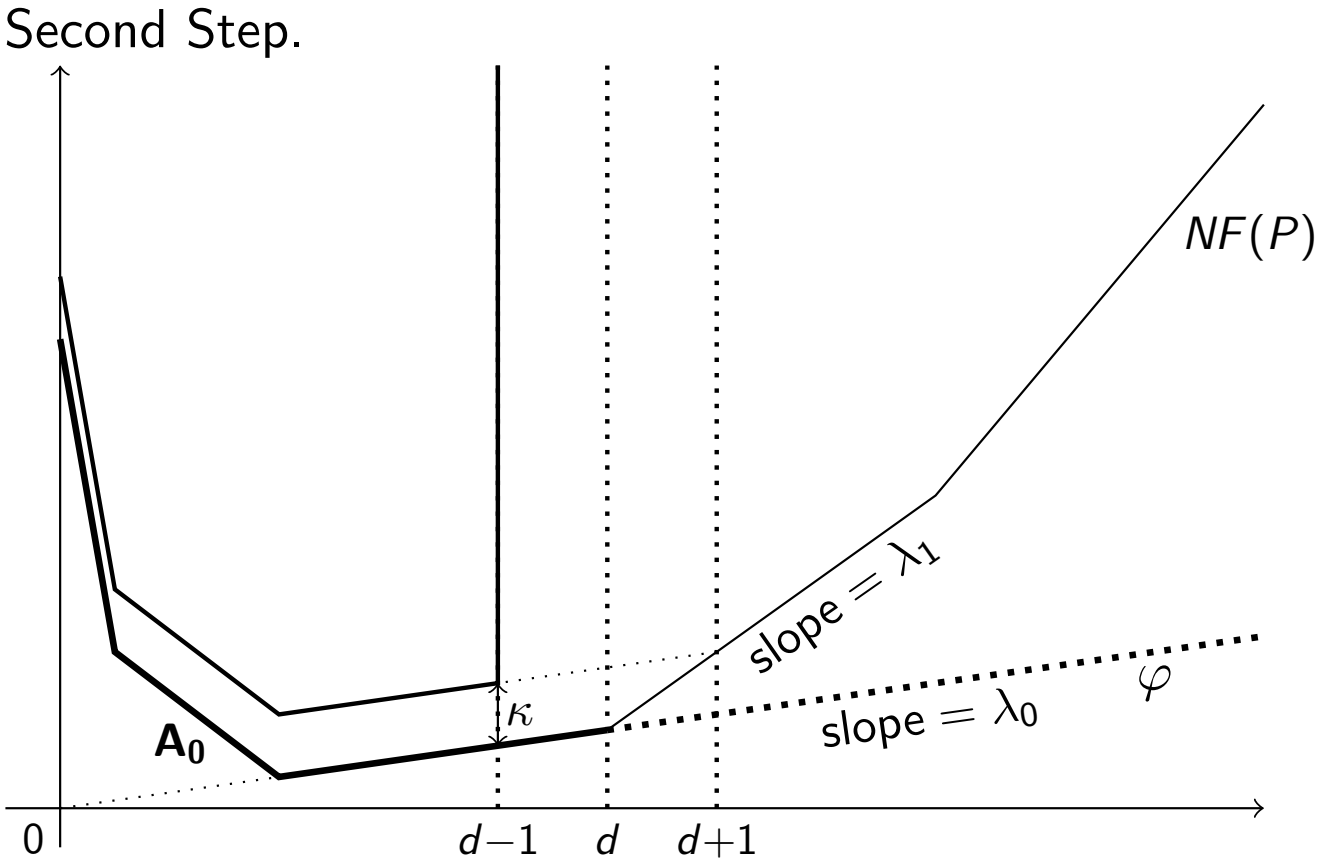


Illustration

First step.

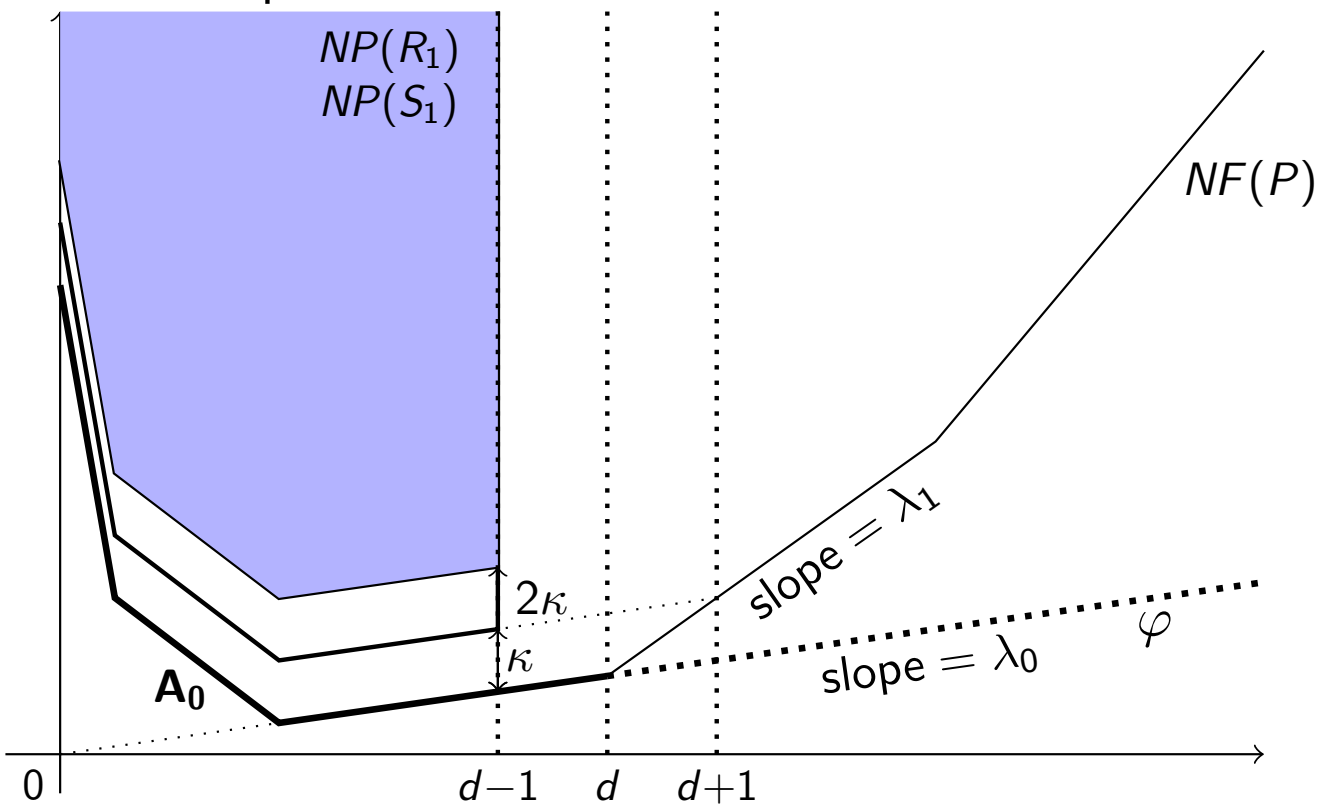


Illustration

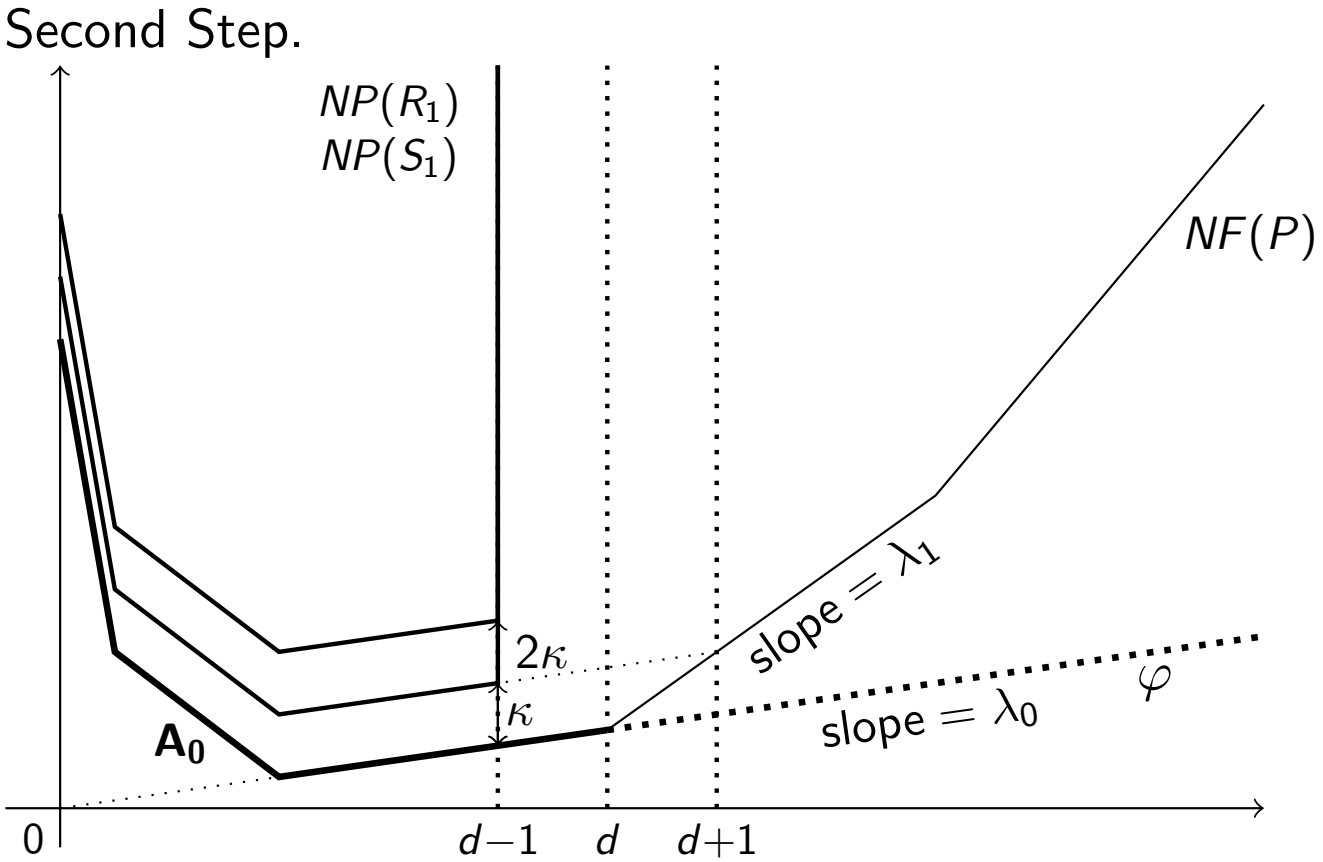


Illustration

Second Step.

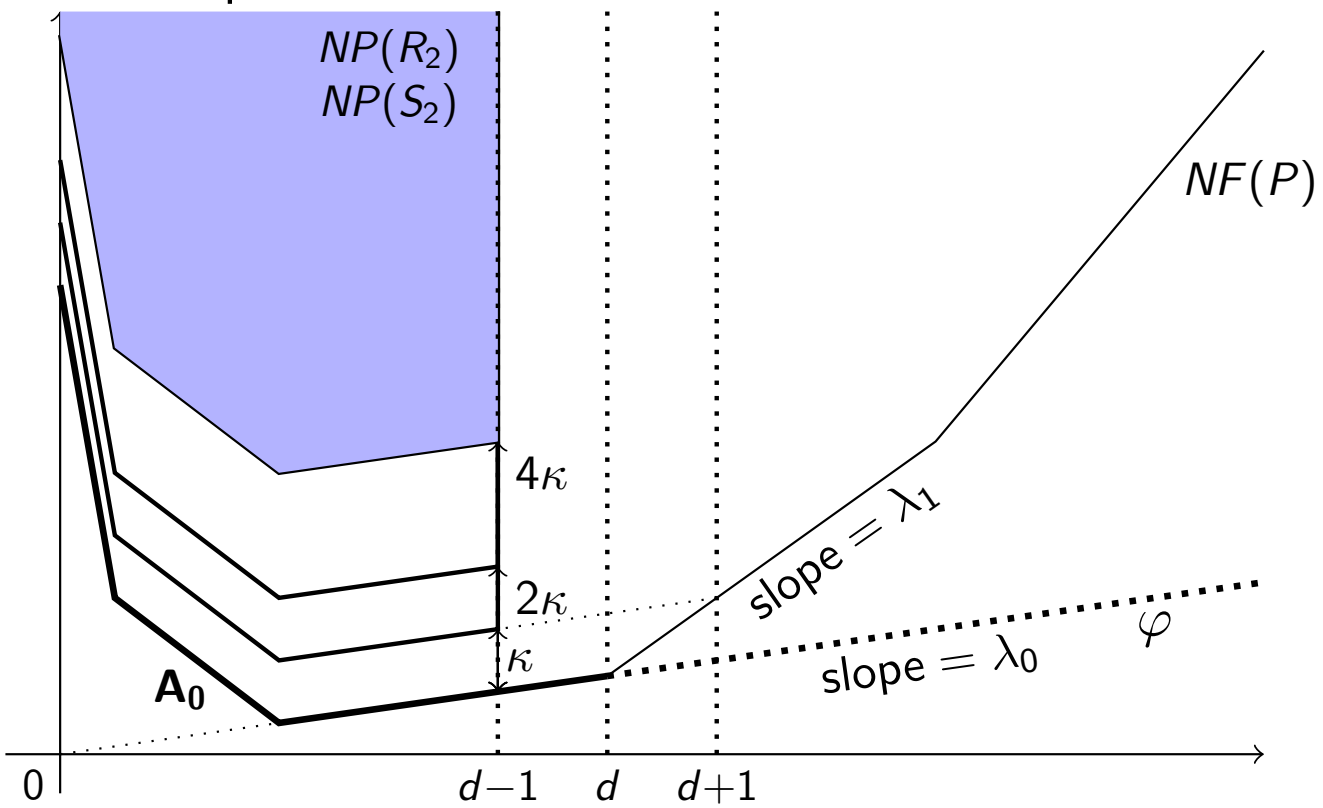


Illustration



Illustration

Third Step.



Illustration

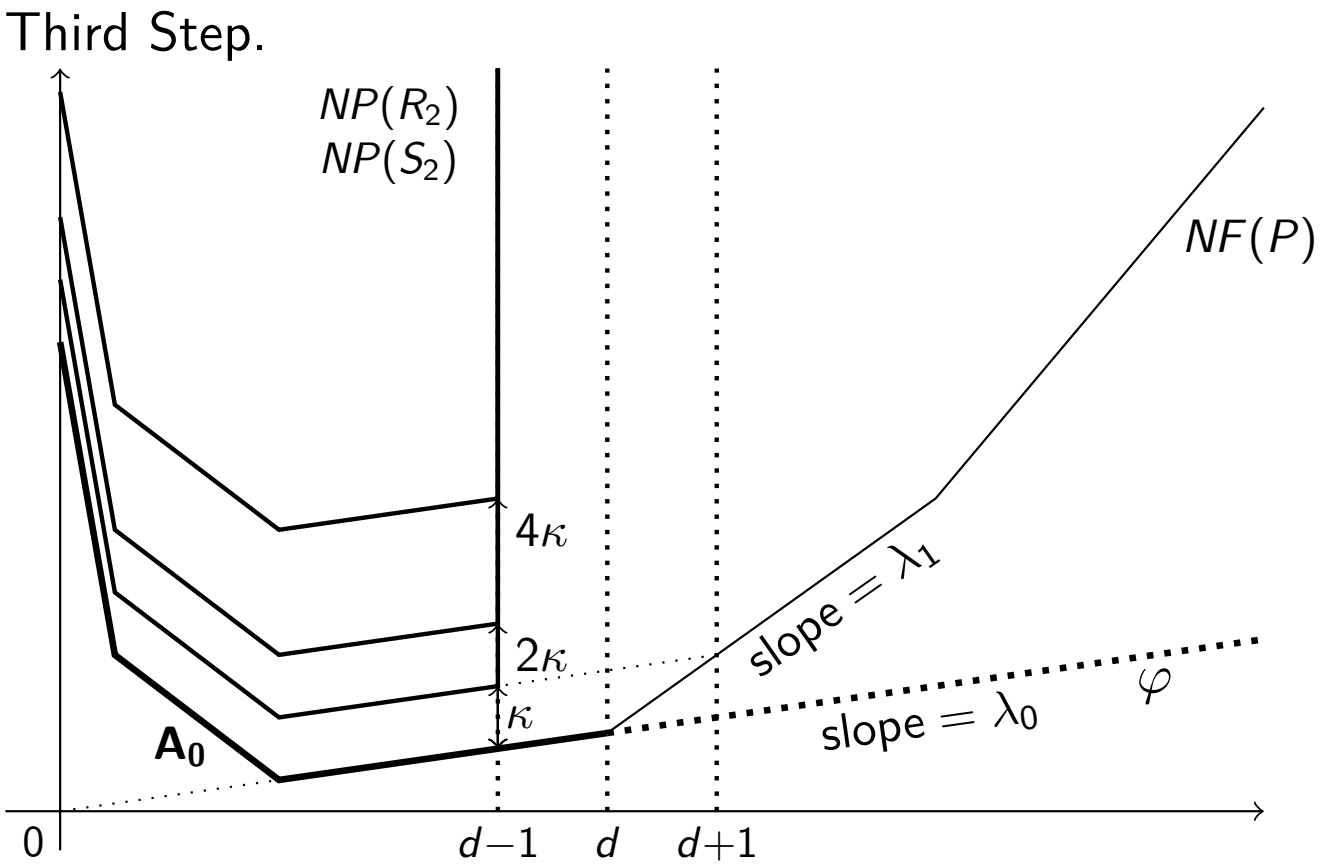


Table of contents

What about precision?

Setting

Let $F_A : P \mapsto A^{(1)}$ be the application such that $P = A^{(1)}B^{(1)}$, with $A^{(1)}, B^{(1)}$ corresponding to the slopes before/after the breakpoint d.

What about precision?

Setting

Let $F_A : P \mapsto A^{(1)}$ be the application such that $P = A^{(1)}B^{(1)}$, with $A^{(1)}, B^{(1)}$ corresponding to the slopes before/after the breakpoint d.

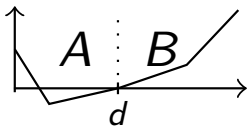
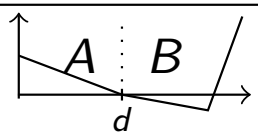
Differential

The application $F_A : P \mapsto A^{(1)}$ is of class C^1. Its differential at some point P is the linear mapping

$$dP \mapsto dA^{(1)} = (V^{(1)}\, dP) \mod A^{(1)}$$

where $A^{(1)}B^{(1)} = P$ and $V^{(1)}$ is the inverse of $B^{(1)}$ modulo $A^{(1)}$.

Some numerical results: $A \mapsto AB \mapsto A$.

Polynomials	Precision	Mean gain of precision		
		Jagged	Newton	Lattice
	absolute	−14.5	−14.7	0.0
	relative	−1.5	−3.6	0.0
	absolute	0.0	0.0	0.0
	relative	−0.3	−1.2	0.0

To sum up

On p-adic precision

To sum up

On p-adic precision

- Step-by-step analysis: as a first step. Can show differentiability and naïve loss in precision during the computation.

To sum up

On p-adic precision

- Step-by-step analysis: as a first step. Can show differentiability and naïve loss in precision during the computation.
- Differential calculus: **intrinsic** and can handle both **gain** and **loss**.

To sum up

On p-adic precision

- Step-by-step analysis: as a first step. Can show differentiability and naïve loss in precision during the computation.
- Differential calculus: **intrinsic** and can handle both **gain** and **loss**.
- Lattice precision: achieving and understandig the best precision.

To sum up

On p-adic precision

- Step-by-step analysis: as a first step. Can show differentiability and naïve loss in precision during the computation.
- Differential calculus: **intrinsic** and can handle both **gain** and **loss**.
- Lattice precision: achieving and understandig the best precision.

On polynomial computations

To sum up

On p-adic precision

- Step-by-step analysis: as a first step. Can show differentiability and naïve loss in precision during the computation.
- Differential calculus: **intrinsic** and can handle both **gain** and **loss**.
- Lattice precision: achieving and understandig the best precision.

On polynomial computations

- **Diffused digits** for modular multiplication.

To sum up

On p-adic precision

- Step-by-step analysis: as a first step. Can show differentiability and naïve loss in precision during the computation.
- Differential calculus: **intrinsic** and can handle both **gain** and **loss**.
- Lattice precision: achieving and understandig the best precision.

On polynomial computations

- **Diffused digits** for modular multiplication.
- **Newton iteration** for **slope factorisation**.

References

Initial article

- Xavier Caruso, David Roe and Tristan Vaccon Tracking p-adic precision, ANTS XI, 2014.

Linear Algebra

- Xavier Caruso, David Roe and Tristan Vaccon p-adic stability in linear algebra, ISSAC 2015.

Polynomial Computations

- Xavier Caruso, David Roe and Tristan Vaccon Division and Slope Factorization of p-Adic Polynomials, ISSAC 2016.

Thank you for your attention

Thanks