On some p-adic differential equations

with separation of variables

Pierre Lairez, **Tristan Vaccon**

TU Berlin, 立教大学 (Rikkyo University)

ISSAC 2016

RIKKYO UNIVERSITY

Table of contents

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 ;
- Counting-point algorithm: Satoh, SEA, and Kedlaya's and Lauder's 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 ;
- Counting-point algorithm: Satoh, SEA, and Kedlaya's and Lauder's algorithms via p-adic cohomology.

My personal (long-term) motivation

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

Table of contents

Motivation for isogeny computations

Study of elliptic curves

- Isogenies are "morphisms" between elliptic curves ;

Motivation for isogeny computations

Study of elliptic curves

- Isogenies are "morphisms" between elliptic curves ;
- Relationship between curves: yields point-counting algorithms (*e.g.* SEA).

Motivation for isogeny computations

Study of elliptic curves

- Isogenies are "morphisms" between elliptic curves ;
- Relationship between curves: yields point-counting algorithms (*e.g.* SEA).

Cryptosytems

- De Fao, Jao and Plût have proposed cryptosystems based on isogenies between elliptic curves and their computation.

Motivation for isogeny computations

Study of elliptic curves

- Isogenies are "morphisms" between elliptic curves ;
- Relationship between curves: yields point-counting algorithms (*e.g.* SEA).

Cryptosytems

- De Fao, Jao and Plût have proposed cryptosystems based on isogenies between elliptic curves and their computation.
- In particular: key-exchange, proof of identity, public-key encryption...

Motivation for isogeny computations

Study of elliptic curves

- Isogenies are "morphisms" between elliptic curves ;
- Relationship between curves: yields point-counting algorithms (*e.g.* SEA).

Cryptosytems

- De Fao, Jao and Plût have proposed cryptosystems based on isogenies between elliptic curves and their computation.
- In particular: key-exchange, proof of identity, public-key encryption... They are candidate for **Post-Quantum Cryptography**.

Motivation for isogeny computations

Study of elliptic curves

- Isogenies are "morphisms" between elliptic curves ;
- Relationship between curves: yields point-counting algorithms (*e.g.* SEA).

Cryptosytems

- De Fao, Jao and Plût have proposed cryptosystems based on isogenies between elliptic curves and their computation.
- In particular: key-exchange, proof of identity, public-key encryption... They are candidate for **Post-Quantum Cryptography**.
- Hence, we need deep **understanding of the computation of isogenies**.

How to compute isogenies?

How to compute isogenies?

Isogeny and Differential equations (*cf* Schoof-Elkies-Atkin algorithm, Bostan-Morain-Salvy-Schost 08, Lercier-Sirvent 08, ...)

Let E and $\tilde{E}$ be two elliptic curves over $\mathbb{Z}/p\mathbb{Z}$:

$$E : y^2 = x^3 + Ax + B,$$
$$\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}.$$

How to compute isogenies?

Isogeny and Differential equations (*cf* Schoof-Elkies-Atkin algorithm, Bostan-Morain-Salvy-Schost 08, Lercier-Sirvent 08, ...)

Let E and $\tilde{E}$ be two elliptic curves over $\mathbb{Z}/p\mathbb{Z}$:

$$E : y^2 = x^3 + Ax + B,$$
$$\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}.$$

Let us assume that there exists some normalized isogeny I between E and $\tilde{E}$. Then, for some rational fraction U,

$$I(x, y) = (U(x), yU'(x)),$$

How to compute isogenies?

Isogeny and Differential equations (*cf* Schoof-Elkies-Atkin algorithm, Bostan-Morain-Salvy-Schost 08, Lercier-Sirvent 08, ...)

Let E and $\tilde{E}$ be two elliptic curves over $\mathbb{Z}/p\mathbb{Z}$:

$$E : y^2 = x^3 + Ax + B,$$
$$\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}.$$

Let us assume that there exists some normalized isogeny I between E and $\tilde{E}$. Then, for some rational fraction U,

$$I(x, y) = (U(x), yU'(x)),$$

Writing $U = \frac{1}{S(\frac{1}{\sqrt{x}})^2}$, we get :

$$(Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6.$$

Change of variable and the differential equation

The differential equation

Let S be such that $U = \frac{1}{S(\frac{1}{\sqrt{x}})^2}$.

We have the following differential equation for S :

$$(Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6.$$

Change of variable and the differential equation

The differential equation

Let S be such that $U = \frac{1}{S(\frac{1}{\sqrt{x}})^2}$.

We have the following differential equation for S :

$$(Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6.$$

It rewrites as:

$$y'^2 = g(x)h(y).$$

Change of variable and the differential equation

The differential equation

Let S be such that $U = \frac{1}{S(\frac{1}{\sqrt{x}})^2}$.

We have the following differential equation for S :

$$(Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6.$$

It rewrites as:

$$y'^2 = g(x)h(y).$$

Solving a differential equation in $\mathbb{Z}/p\mathbb{Z}$???

- **Not easy**:

$$\int X^{p-1} = \frac{1}{p}X^p ?$$

Change of variable and the differential equation

The differential equation

Let S be such that $U = \frac{1}{S(\frac{1}{\sqrt{x}})^2}$.

We have the following differential equation for S :

$$(Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6.$$

It rewrites as:

$$y'^2 = g(x)h(y).$$

Solving a differential equation in $\mathbb{Z}/p\mathbb{Z}$???

- **Not easy**:
$$\int X^{p-1} = \frac{1}{p}X^p ?$$
- We would like to be in **zero characteristic**: let's go **p-adic**!

Previous take on this topic

Linear Differential Equation

Bostan, Gonzalez-Vega, Perdry & Schost in 2005 and Grenet, Lecerf & van der Hoeven in 2016 have tackled this case completely.

Isogeny computation and differential equations

Used inside variants of SEA. Main references are Bostan, Morain, Salvy & Schost in 2008 and Lercier & Sirvent in 2008.

Table of contents

Change of variable and the differential equation

The differential equation

Let S be such that

$$U = \frac{1}{S(\frac{1}{\sqrt{x}})^2}.$$

Then if $A, B, \tilde{A}, \tilde{B}$ are in $\mathbb{Z}_p$,

$$S \in \mathbb{Z}_p[[t]]$$

We have the following differential equation for S :

$$(Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6.$$

A p-adic computation of a solution

Computing the isogeny

Given E and $\widetilde{E}$, the goal is to compute the isogeny I *via* the differential equation:

$$\begin{cases} S(0) = 0, \\ (Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6. \end{cases}$$

Going through $\mathbb{Z}_p$

Not easy to solve a differential equation in $\mathbb{Z}/p\mathbb{Z}$.

A p-adic computation of a solution

Computing the isogeny

Given E and $\widetilde{E}$, the goal is to compute the isogeny I *via* the differential equation:

$$\begin{cases} S(0) = 0, \\ (Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6. \end{cases}$$

Going through $\mathbb{Z}_p$

Not easy to solve a differential equation in $\mathbb{Z}/p\mathbb{Z}$. Consequently:

A p-adic computation of a solution

Computing the isogeny

Given E and $\widetilde{E}$, the goal is to compute the isogeny I *via* the differential equation:

$$\begin{cases} S(0) = 0, \\ (Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6. \end{cases}$$

Going through $\mathbb{Z}_p$

Not easy to solve a differential equation in $\mathbb{Z}/p\mathbb{Z}$. Consequently:

1. Lift (consistently) from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$.

A p-adic computation of a solution

Computing the isogeny

Given E and $\widetilde{E}$, the goal is to compute the isogeny I *via* the differential equation:

$$\begin{cases} S(0) = 0, \\ (Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6. \end{cases}$$

Going through $\mathbb{Z}_p$

Not easy to solve a differential equation in $\mathbb{Z}/p\mathbb{Z}$. Consequently:

1. Lift (consistently) from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$.
2. Solve the differential equation in $\mathbb{Z}_p$.

A p-adic computation of a solution

Computing the isogeny

Given E and $\widetilde{E}$, the goal is to compute the isogeny I *via* the differential equation:

$$\begin{cases} S(0) = 0, \\ (Bx^6 + Ax^4 + 1)S'^2 = 1 + \tilde{A}S^4 + \tilde{B}S^6. \end{cases}$$

Going through $\mathbb{Z}_p$

Not easy to solve a differential equation in $\mathbb{Z}/p\mathbb{Z}$. Consequently:

1. Lift (consistently) from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$.
2. Solve the differential equation in $\mathbb{Z}_p$.
3. Reduce mod p to get the solution in $\mathbb{Z}/p\mathbb{Z}$.

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:

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

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

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.

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

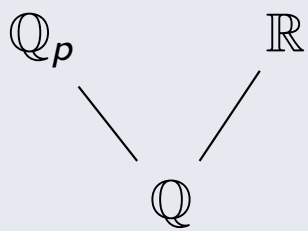
$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

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

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 $\ldots\overline{654,3}^7 = 3 \times 7^{-1} + 4 \times 7^0 + 5 \times 7^1 + 6 \times 7^2 + O(7^3)$ 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,

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

Table of contents

Reduction of the problem

Change of equation

When $p \neq 2$, we can replace $y'^2 \times G = H(y)$ by $y' = g \times h(y)$ with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$.

Reduction of the problem

Change of equation

When $p \neq 2$, we can replace $y'^2 \times G = H(y)$ by $\boxed{y' = g \times h(y)}$ with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$.

Reduction of the problem

Change of equation

When $p \neq 2$, we can replace $y'^2 \times G = H(y)$ by $\boxed{y' = g \times h(y)}$ with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$.

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Naïve iteration

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Naïve iteration

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Direct computation

We can write

$$(n+1)y_{n+1} = P_n(g_{\leq n}, h_{\leq n}, y_{\leq n}),$$

for some P_n with integer coefficients.

Naïve iteration

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Direct computation

We can write

$$(n+1)y_{n+1} = P_n(g_{\leq n}, h_{\leq n}, y_{\leq n}),$$

for some P_n with integer coefficients.

Loss in precision

Loss: $val(n!) \geq \frac{n - \log_p n}{p-1}$ at the n-th step.

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Direct analysis

Newton scheme to solve $y' = g \times h(y)$:

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Direct analysis

Newton scheme to solve $y' = g \times h(y)$:

$$N_{g,h}(u) \leftarrow u - h(u) \int \left(\frac{u'}{h(u)} - g \right).$$

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Direct analysis

Newton scheme to solve $y' = g \times h(y)$:

$$N_{g,h}(u) \leftarrow u - h(u) \int \left(\frac{u'}{h(u)} - g \right).$$

Remark

$$\int O(p^m) x^k = \frac{O(p^m)}{k+1} x^{k+1}.$$

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Direct analysis

Newton scheme to solve $y' = g \times h(y)$:

$$N_{g,h}(u) \leftarrow u - h(u) \int \left(\frac{u'}{h(u)} - g \right).$$

Remark

$$\int O(p^m) x^k = \frac{O(p^m)}{k+1} x^{k+1}.$$

One loses $O(\log_p N)$ at each step, for N the order of truncation.

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Direct analysis

Newton scheme to solve $y' = g \times h(y)$:

$$N_{g,h}(u) \leftarrow u - h(u) \int \left(\frac{u'}{h(u)} - g \right).$$

Remark

$$\int O(p^m) x^k = \frac{O(p^m)}{k+1} x^{k+1}.$$

One loses $O(\log_p N)$ at each step, for N the order of truncation.

To compute $y \mod x^{2^N+1}$, we need an initial precision of $O(N^2)$ digits.

Our problem

We wish to solve the following differential equation, with $g, h \in \mathbb{Z}_p[\![x]\!]^\times$:

$$\begin{cases} y(0) = 0, \\ y' = g \times h(y). \end{cases}$$

Direct analysis

Newton scheme to solve $y' = g \times h(y)$:

$$N_{g,h}(u) \leftarrow u - h(u) \int \left(\frac{u'}{h(u)} - g \right).$$

Remark

$$\int O(p^m) x^k = \frac{O(p^m)}{k+1} x^{k+1}.$$

One loses $O(\log_p N)$ at each step, for N the order of truncation.

To compute $y \mod x^{2^N+1}$, we need an initial precision of $O(N^2)$ digits.
Loss in precision **quadratic in the number of steps**.

Summary: precision and p-adic computations

Direct method for precision

Summary: precision and p-adic computations

Direct method for precision

- Is enough to get a first view of the problem.

Summary: precision and p-adic computations

Direct method for precision

- Is enough to get a first view of the problem.
- **Depends heavily** on the algorithm chosen for the computation

Summary: precision and p-adic computations

Direct method for precision

- Is enough to get a first view of the problem.
- **Depends heavily** on the algorithm chosen for the computation
- No idea on what is **optimal**.

Summary: precision and p-adic computations

Direct method for precision

- Is enough to get a first view of the problem.
- **Depends heavily** on the algorithm chosen for the computation
- No idea on what is **optimal**.

Two new questions

Summary: precision and p-adic computations

Direct method for precision

- Is enough to get a first view of the problem.
- **Depends heavily** on the algorithm chosen for the computation
- No idea on what is **optimal**.

Two new questions

- Is there an **optimal loss in precision**?

Summary: precision and p-adic computations

Direct method for precision

- Is enough to get a first view of the problem.
- **Depends heavily** on the algorithm chosen for the computation
- No idea on what is **optimal**.

Two new questions

- Is there an **optimal loss in precision**?
- If so, can we **achieve this loss**?

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

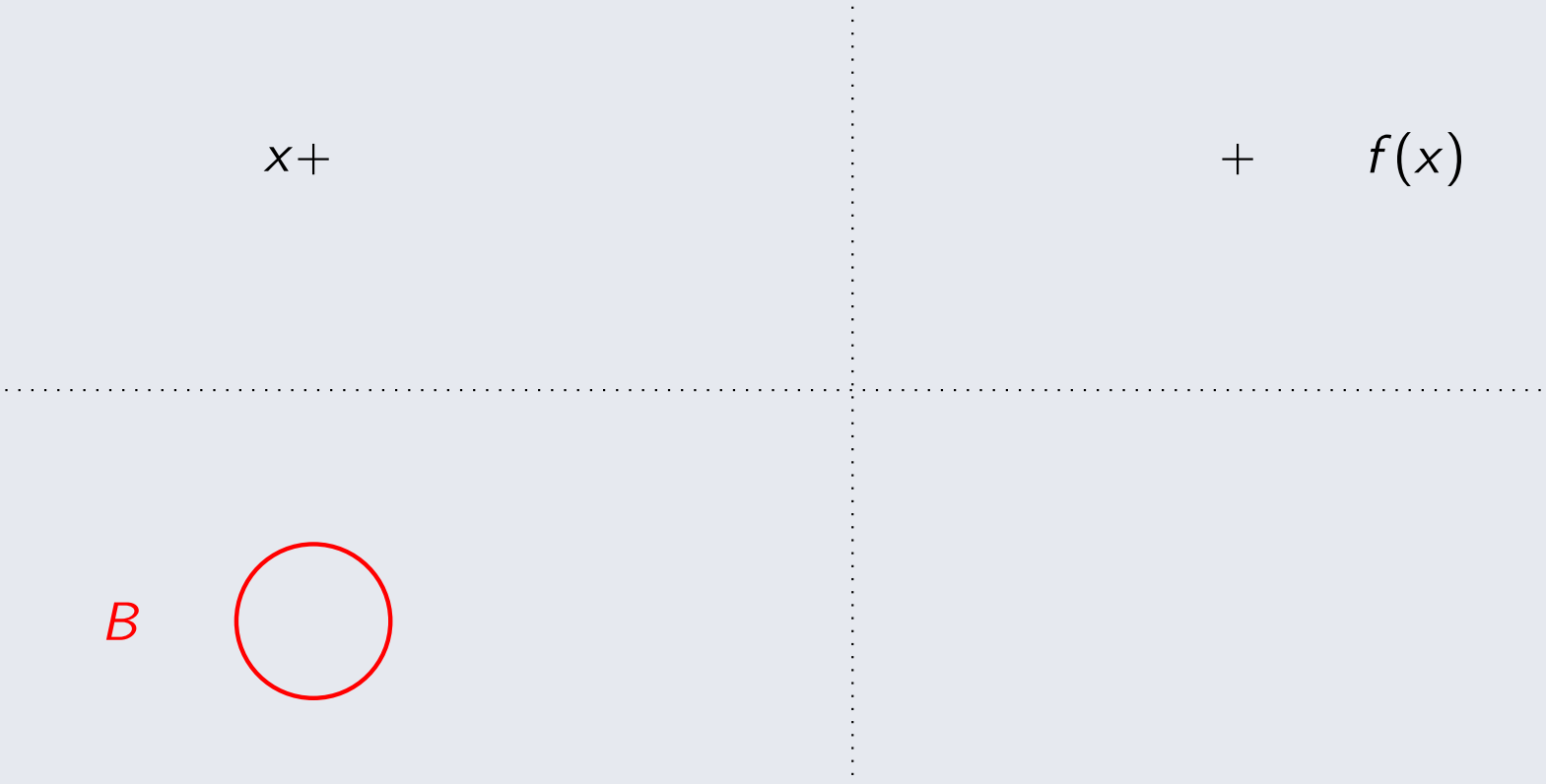
Lemma (CRV14)

*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**,*

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

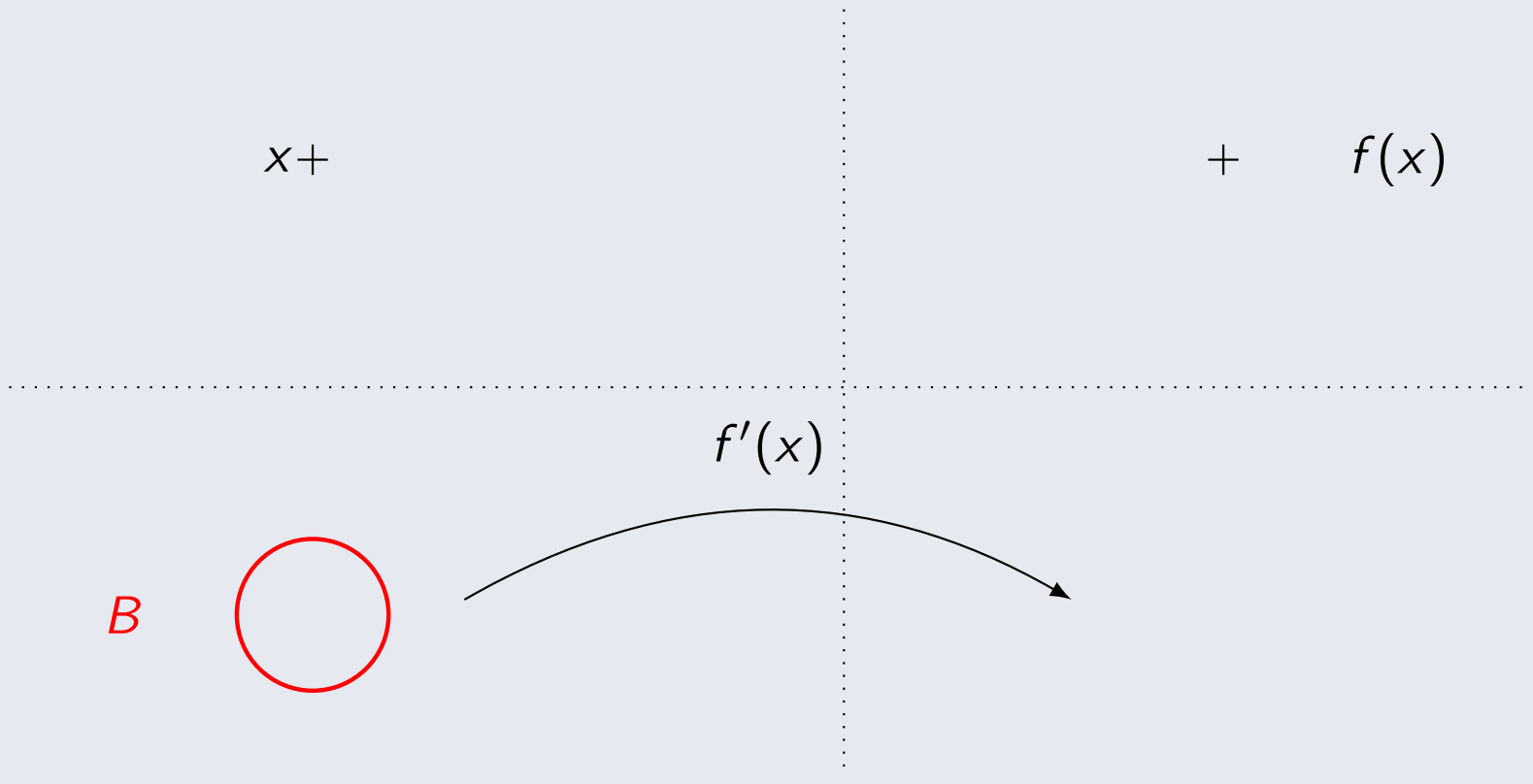
Geometrical meaning

Interpretation



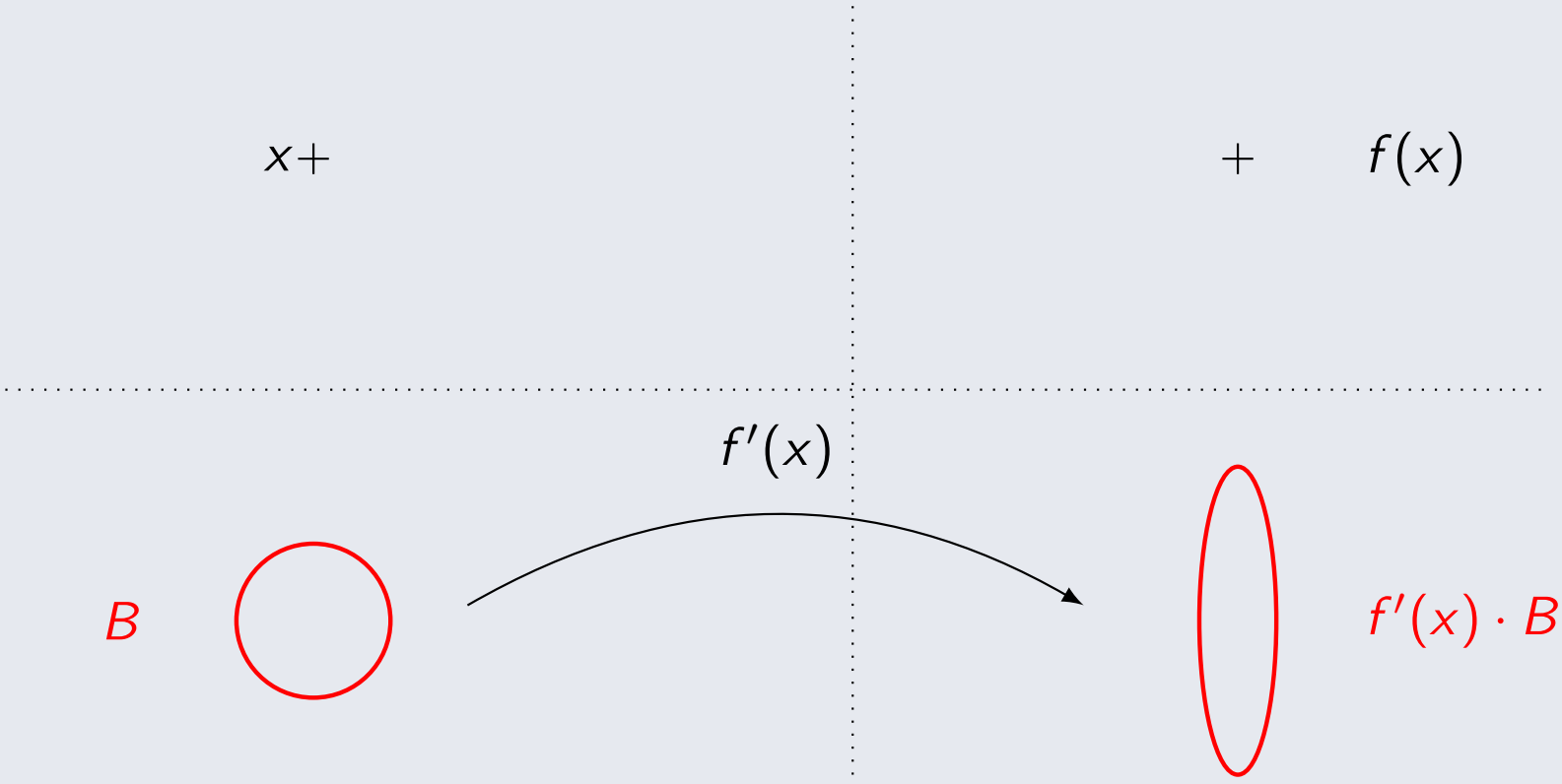
Geometrical meaning

Interpretation



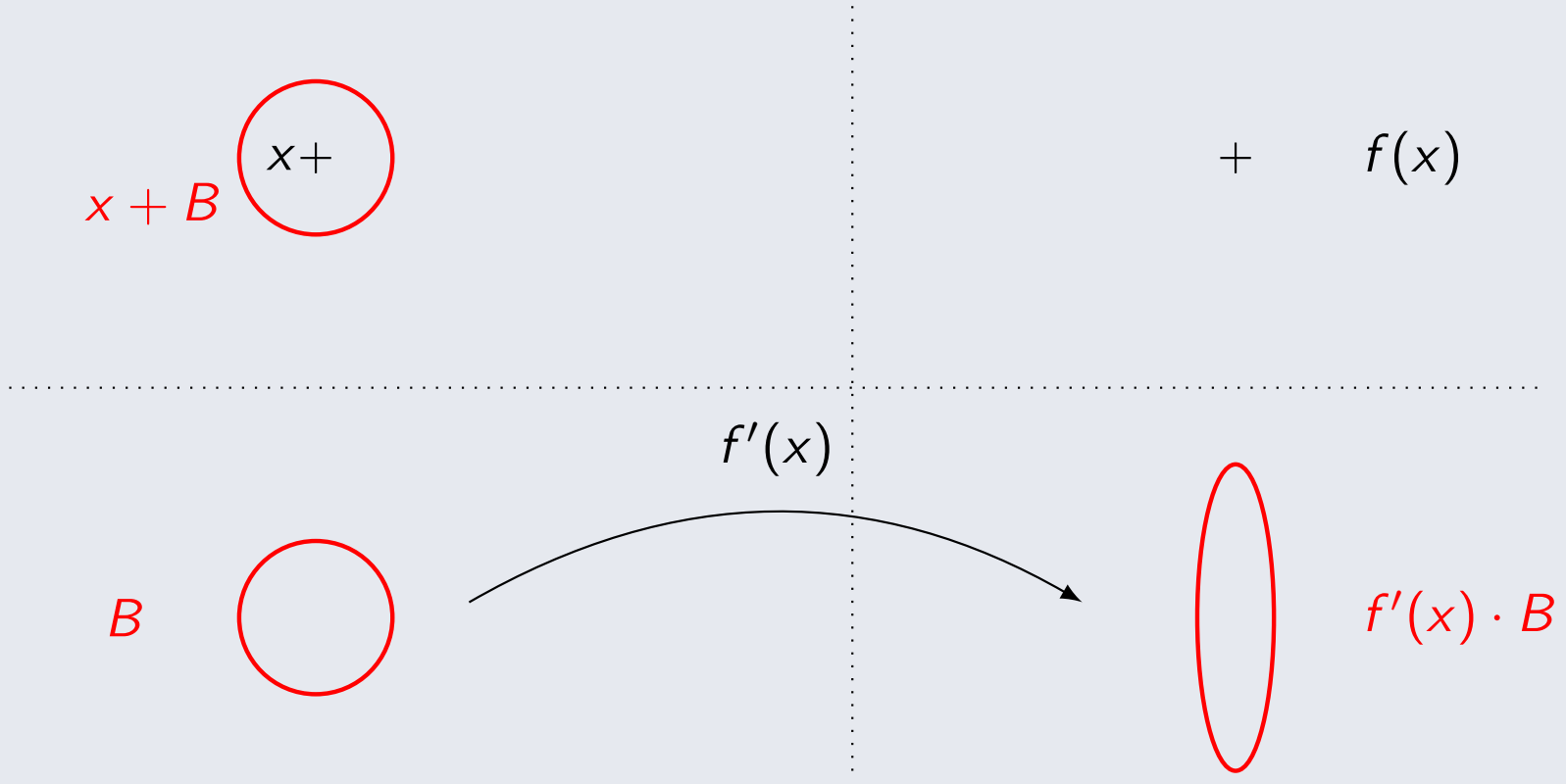
Geometrical meaning

Interpretation



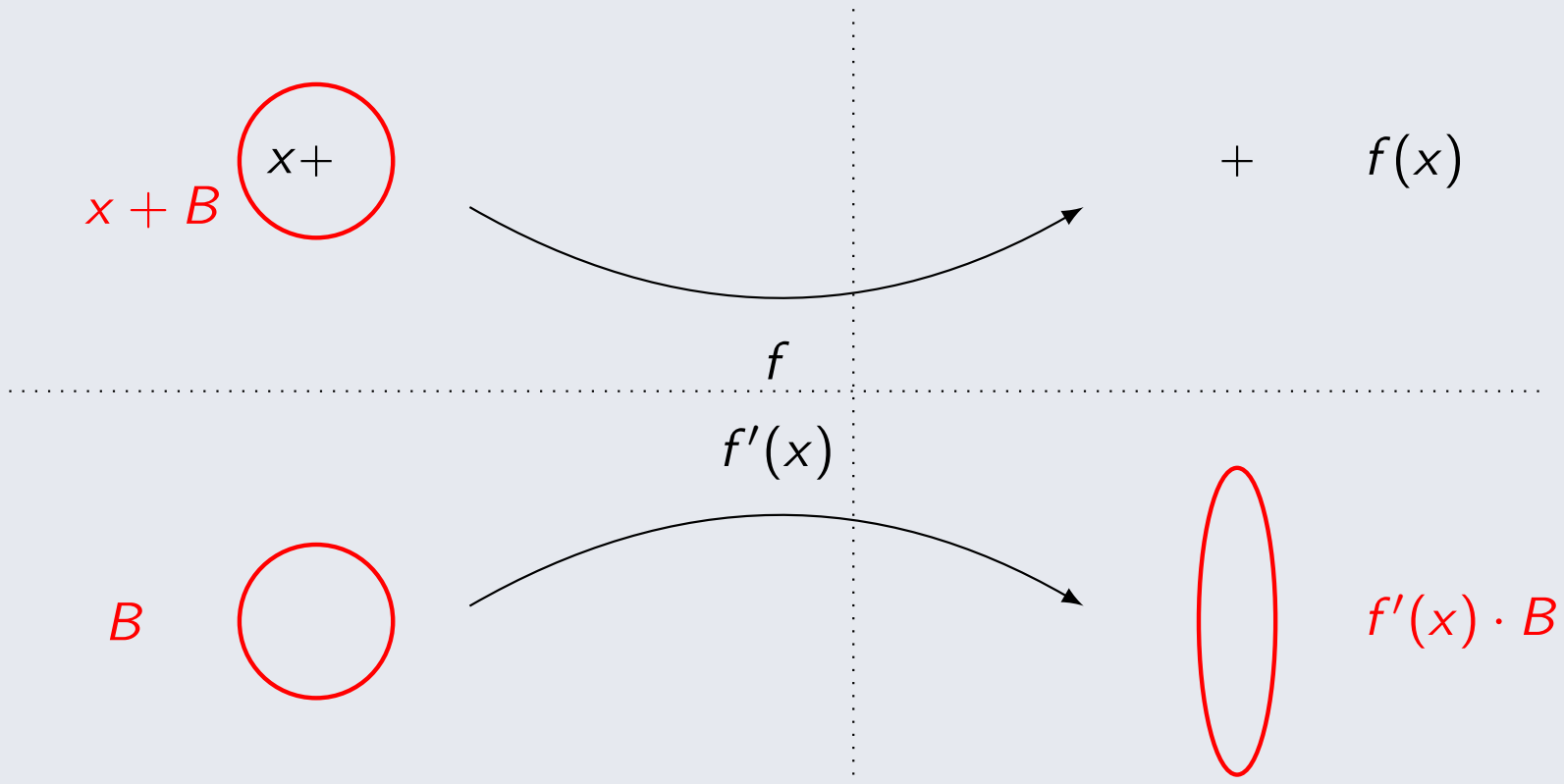
Geometrical meaning

Interpretation



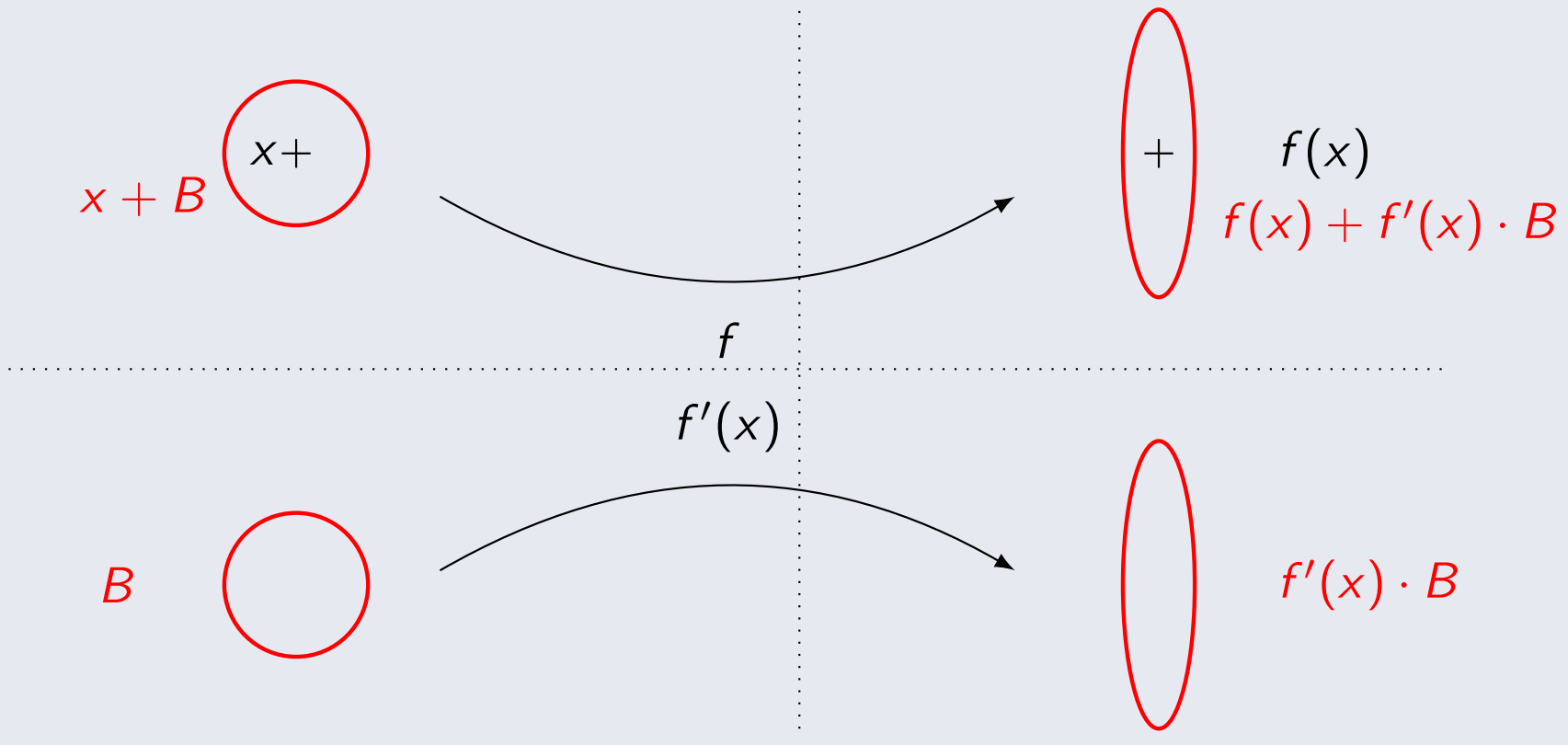
Geometrical meaning

Interpretation



Geometrical meaning

Interpretation



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

Differential and differential equation

Theorem

Let $\Phi : (g, h) \mapsto y$ *such that* $y(0) = 0$ *and* $y' = gh(y)$. *Then,*

$$\Phi'(g, h) \cdot (\delta g, \delta h) = h(y) \int \delta g + \frac{g \delta h(y)}{h(y)}.$$

Differential and differential equation

Theorem

Let $\Phi : (g, h) \mapsto y$ *such that* $y(0) = 0$ *and* $y' = gh(y)$. *Then,*

$$\Phi'(g, h) \cdot (\delta g, \delta h) = h(y) \int \delta g + \frac{g \delta h(y)}{h(y)}.$$

Proposition

In our case, $p \neq 2$, $y, g, h \in \mathbb{Z}_p[\![x]\!]$, $g(0) = h(0) = 1$. *If* $\delta g = \delta h = O(p^k)$, *then*

Differential and differential equation

Theorem

Let $\Phi : (g, h) \mapsto y$ *such that* $y(0) = 0$ *and* $y' = gh(y)$. *Then,*

$$\Phi'(g, h) \cdot (\delta g, \delta h) = h(y) \int \delta g + \frac{g \delta h(y)}{h(y)}.$$

Proposition

In our case, $p \neq 2$, $y, g, h \in \mathbb{Z}_p[\![x]\!]$, $g(0) = h(0) = 1$. *If* $\delta g = \delta h = O(p^k)$, *then*

$$\Phi'(y) \cdot (\delta g, \delta h) \mod x^{2^N+1} \in \frac{O(p^k)}{p^N} \mathbb{Z}_p[\![x]\!].$$

First conclusion on the application of the lemma

Proposition

$\Phi(g,h) \mod (p, t^{2^n})$ *is determined by* $g, h \mod (p^{1+\log_p 2^n}, t^{2^n})$. *In other words, we have a* logarithmic loss *in precision.*

First conclusion on the application of the lemma

Proposition

$\Phi(g,h) \mod (p, t^{2^n})$ *is determined by* $g, h \mod (p^{1+\log_p 2^n}, t^{2^n})$. *In other words, we have a* logarithmic loss *in precision.*

Remark

To prove this result, we compute the norms of the differential of higher order. It is possible to give explicit bounds and apply our framework.

What happens in practice ?

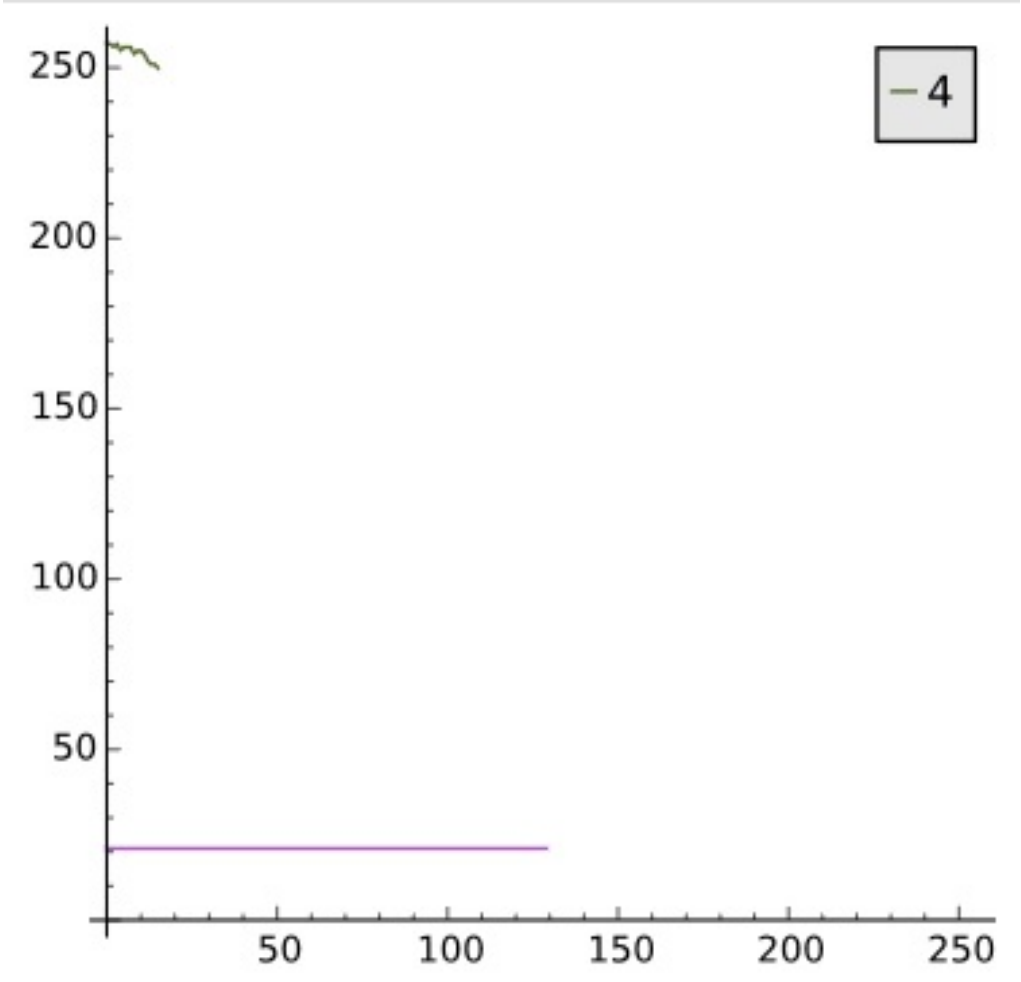


Figure: Precision over the output

What happens in practice ?

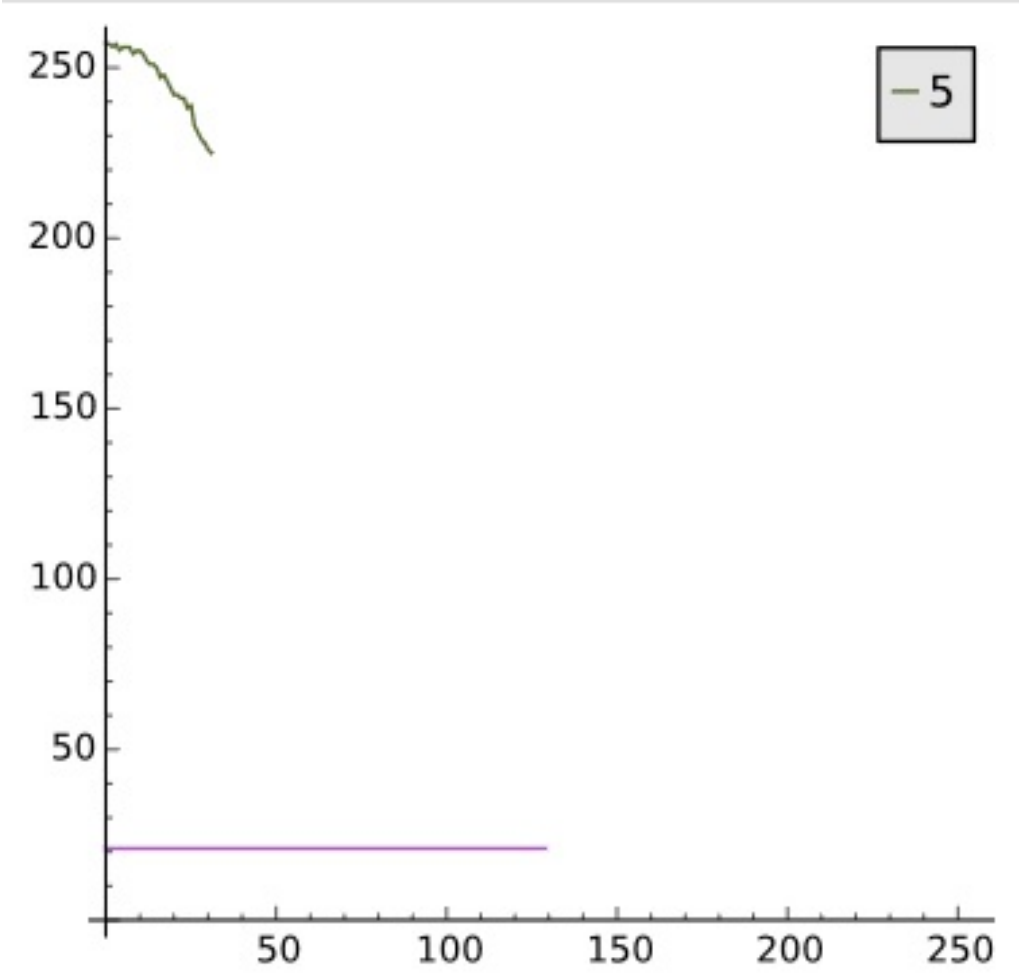


Figure: Precision over the output

What happens in practice ?

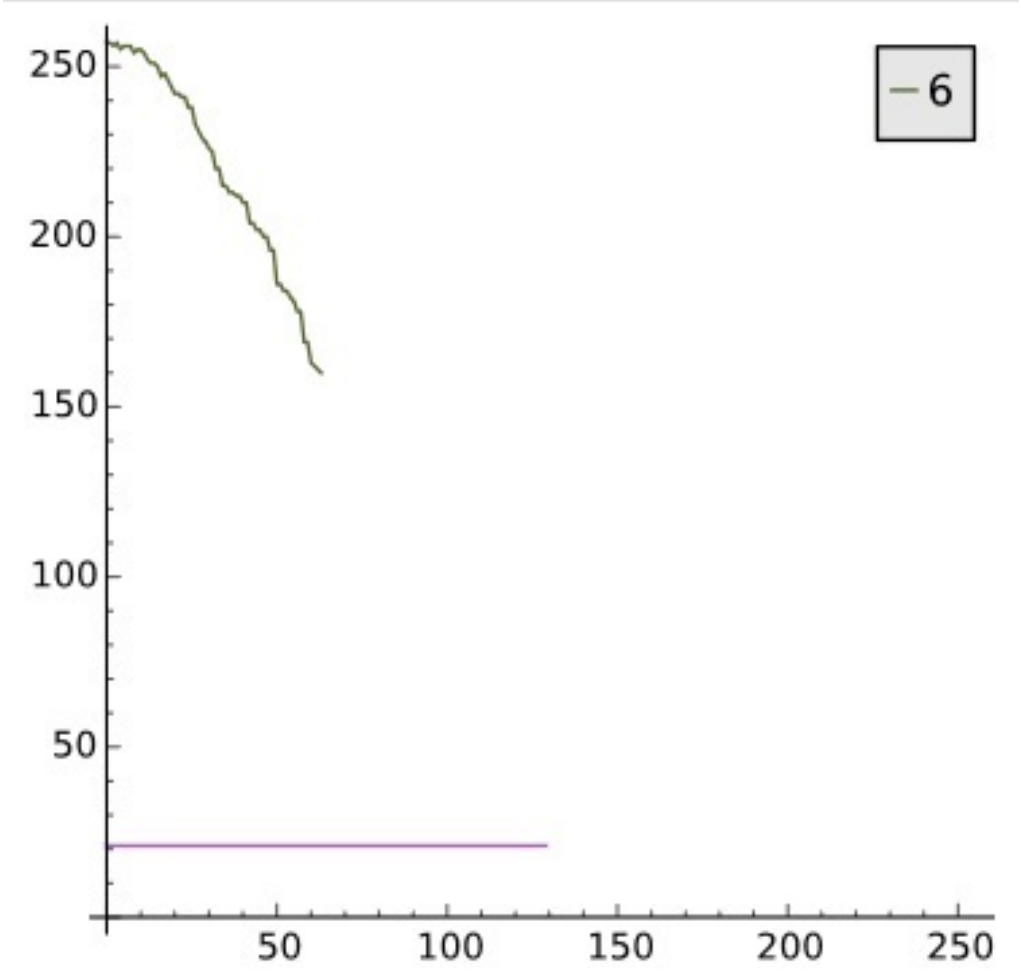


Figure: Precision over the output

What happens in practice ?

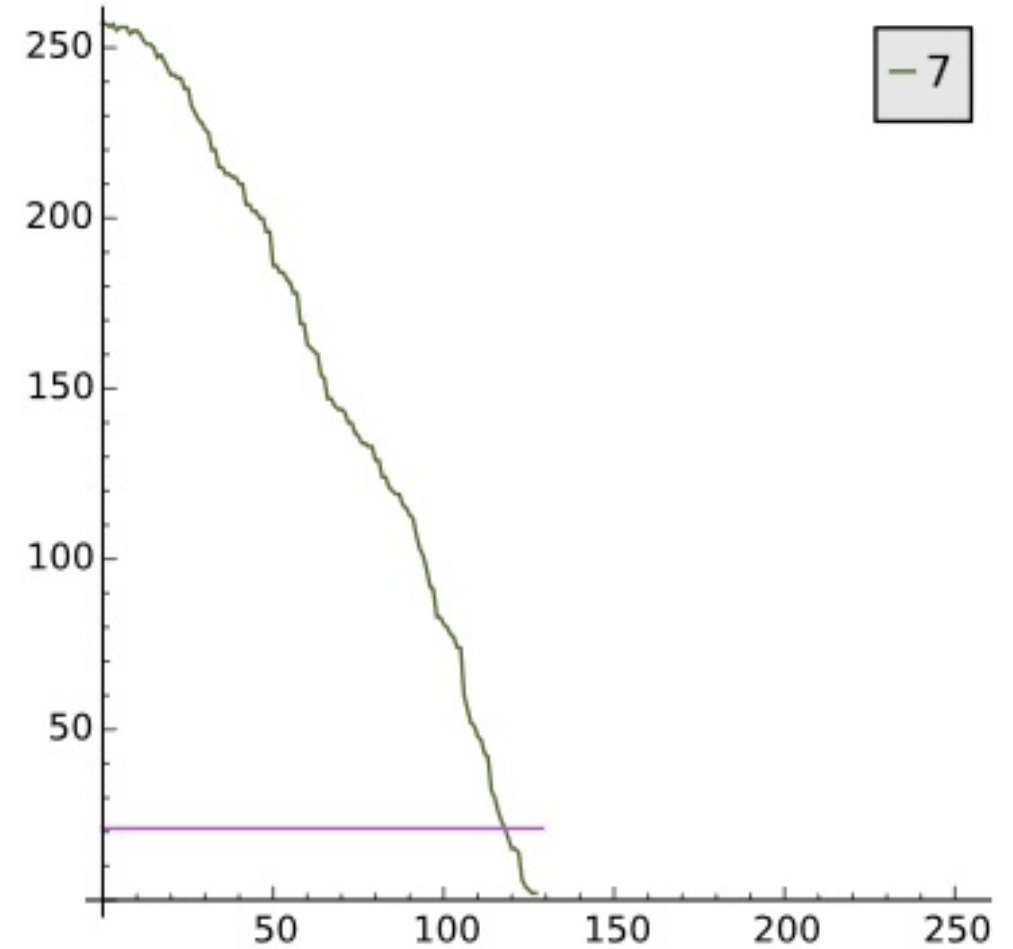


Figure: Precision over the output

Table of contents

Different way of representing the p-adics

Another take on the computation

Different way of representing the p-adics

Another take on the computation

- In the previous computation, we start with some given approximations of g, h, u_0 and try **to follow** the algorithm for the exact counterparts of g, h, u_0.

Different way of representing the p-adics

Another take on the computation

- In the previous computation, we start with some given approximations of g, h, u_0 and try **to follow** the algorithm for the exact counterparts of g, h, u_0. This is somehow **much stronger** than our desire: computing a good approximate solution.

Different way of representing the p-adics

Another take on the computation

- In the previous computation, we start with some given approximations of g, h, u_0 and try **to follow** the algorithm for the exact counterparts of g, h, u_0. This is somehow **much stronger** than our desire: computing a good approximate solution.
- Another way is then to modify the current g, h, u_0 **at each step**, in a consistent way, so as to keep on getting better approximate solutions.

Different way of representing the p-adics

Another take on the computation

- In the previous computation, we start with some given approximations of g, h, u_0 and try **to follow** the algorithm for the exact counterparts of g, h, u_0. This is somehow **much stronger** than our desire: computing a good approximate solution.
- Another way is then to modify the current g, h, u_0 **at each step**, in a consistent way, so as to keep on getting better approximate solutions.
- A third way here will be to work entirely in $\mathbb{Z}/p^\kappa\mathbb{Z}$.

Table of contents

New framework

In this new computation, we consider h as given, and not varying for the lemma.

Lemma

Let $Y : g \mapsto y$ *such that* $y(0) = 0$ *and* $y' = gh(y)$. *Then,*

$$Y'(g) \cdot (\delta g) = h(y) \int \delta g.$$

Consequence

Small modification of g corresponds to small modification of y (and conversely).

In concrete terms

A new take on the iteration

In concrete terms

A new take on the iteration

- $u_0' = g_0 h(u_0) \mod (p^k, t^1)$
- $g_0 = g \mod p^k$

In concrete terms

A new take on the iteration

- $u_0' = g_0 h(u_0) \mod (p^k, t^1)$
- $u_1' = g_1 h(u_1) \mod (p^k, t^2)$

- $g_0 = g \mod p^k$
- $g_1 = g_0 \mod p^k$

In concrete terms

A new take on the iteration

- $u_0' = g_0 h(u_0) \mod (p^k, t^1)$
- $u_1' = g_1 h(u_1) \mod (p^k, t^2)$
- $u_2' = g_2 h(u_2) \mod (p^k, t^4)$

- $g_0 = g \mod p^k$
- $g_1 = g_0 \mod p^k$
- $g_2 = g_1 \mod p^k$

In concrete terms

A new take on the iteration

- $u'_0 = g_0 h(u_0) \mod (p^k, t^1)$
- $u'_1 = g_1 h(u_1) \mod (p^k, t^2)$
- $u'_2 = g_2 h(u_2) \mod (p^k, t^4)$
- $\ldots$

- $g_0 = g \mod p^k$
- $g_1 = g_0 \mod p^k$
- $g_2 = g_1 \mod p^k$
- $\ldots$

In concrete terms

A new take on the iteration

- $u_0' = g_0 h(u_0) \mod (p^k, t^1)$
- $u_1' = g_1 h(u_1) \mod (p^k, t^2)$
- $u_2' = g_2 h(u_2) \mod (p^k, t^4)$
- ...
- ...

- $g_0 = g \mod p^k$
- $g_1 = g_0 \mod p^k$
- $g_2 = g_1 \mod p^k$
- ...
- ...

In concrete terms

A new take on the iteration

- $u'_0 = g_0 h(u_0) \mod (p^k, t^1)$
- $u'_1 = g_1 h(u_1) \mod (p^k, t^2)$
- $u'_2 = g_2 h(u_2) \mod (p^k, t^4)$
- $\ldots$
- $\ldots$
- $u'_l = g_l h(u_l) \mod (p^k, t^{2^l})$

- $g_0 = g \mod p^k$
- $g_1 = g_0 \mod p^k$
- $g_2 = g_1 \mod p^k$
- $\ldots$
- $\ldots$
- $g_l = g_{l-1} \mod p^k$

In concrete terms

A new take on the iteration

- $u'_0 = g_0 h(u_0) \mod (p^k, t^1)$
- $u'_1 = g_1 h(u_1) \mod (p^k, t^2)$
- $u'_2 = g_2 h(u_2) \mod (p^k, t^4)$
- $\dots$
- $\dots$
- $u'_l = g_l h(u_l) \mod (p^k, t^{2^l})$

- $g_0 = g \mod p^k$
- $g_1 = g_0 \mod p^k$
- $g_2 = g_1 \mod p^k$
- $\dots$
- $\dots$
- $g_l = g_{l-1} \mod p^k$

In the end

- $u'_l = gh(u_l) \mod (p^k, t^{2^l})$

- $g_l = g \mod p^k$

Final take on the Newton scheme

As a consequence, we can prove that it is harmless to work in $\mathbb{Z}/p^k\mathbb{Z}$ for our computation.

Proposition

We can obtain the solution $\Phi(g,h) \mod (p, t^{n+1})$ *knowing* $g, h \mod (p^{\lfloor \log_p n \rfloor + 1}, t^{n+1})$ *and applying the following iteration:*

$$N_{g,h}(u) \leftarrow u - h(u) \int \left(\frac{u'}{h(u)} - g \right),$$

Final take on the Newton scheme

As a consequence, we can prove that it is harmless to work in $\mathbb{Z}/p^k\mathbb{Z}$ for our computation.

Proposition

We can obtain the solution $\Phi(g,h) \mod (p, t^{n+1})$ *knowing* $g, h \mod (p^{\lfloor \log_p n \rfloor + 1}, t^{n+1})$ *and applying the following iteration:*

$$N_{g,h}(u) \leftarrow u - h(u) \int \left(\frac{u'}{h(u)} - g \right),$$

modulo $p^{\lfloor \log_p n \rfloor + 1}$ *and growing order of truncation.*

In other words

We achieve **optimal loss** in precision: **linear** in the number of iteration for the Newton method.

Timings

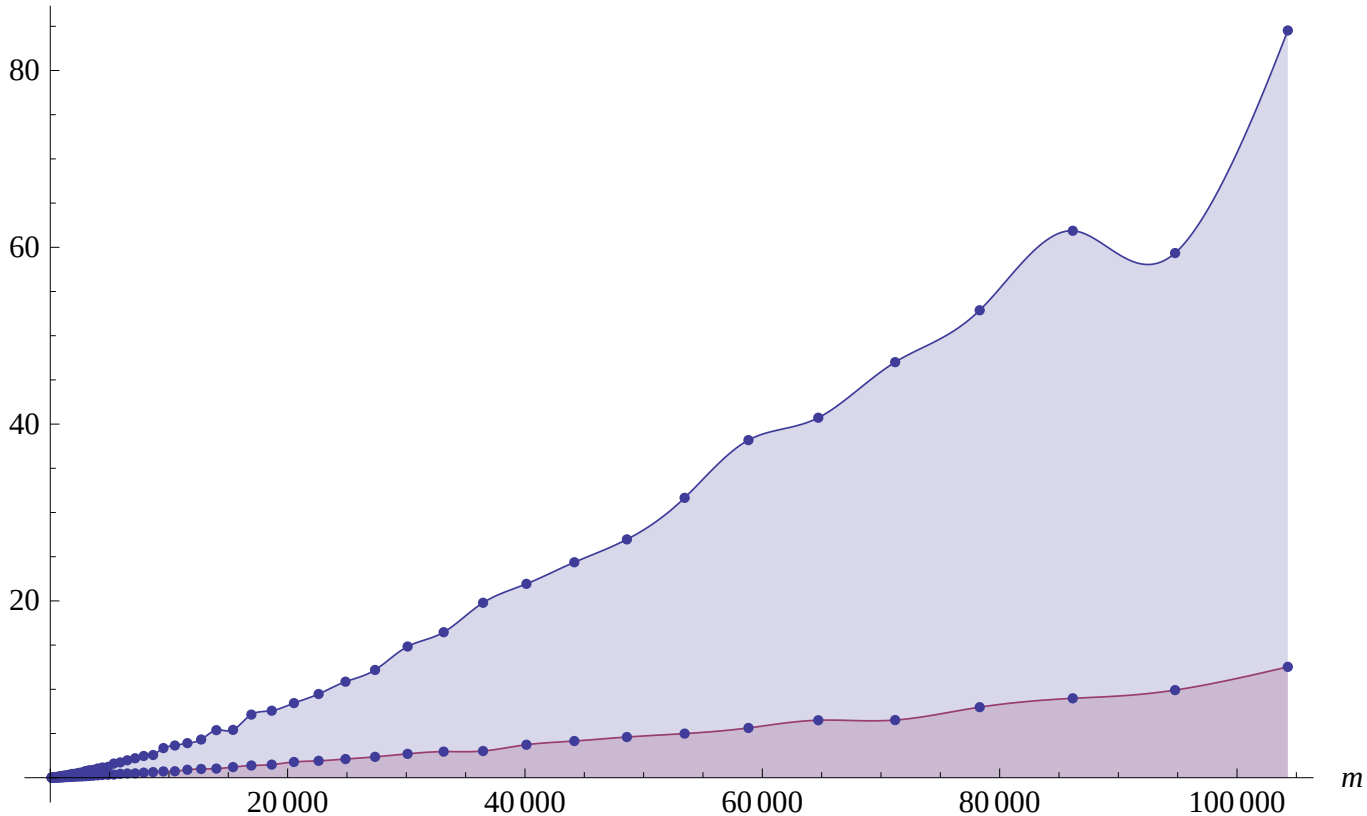


Figure: Timings in seconds, measured on a laptop, of our Algorithm run at precision λ_{old} (upper curve) and λ_{new} (lower curve) in order to compute an approximation modulo $(5, t^{4m+1})$ of some given m-isogenies.

Speedup

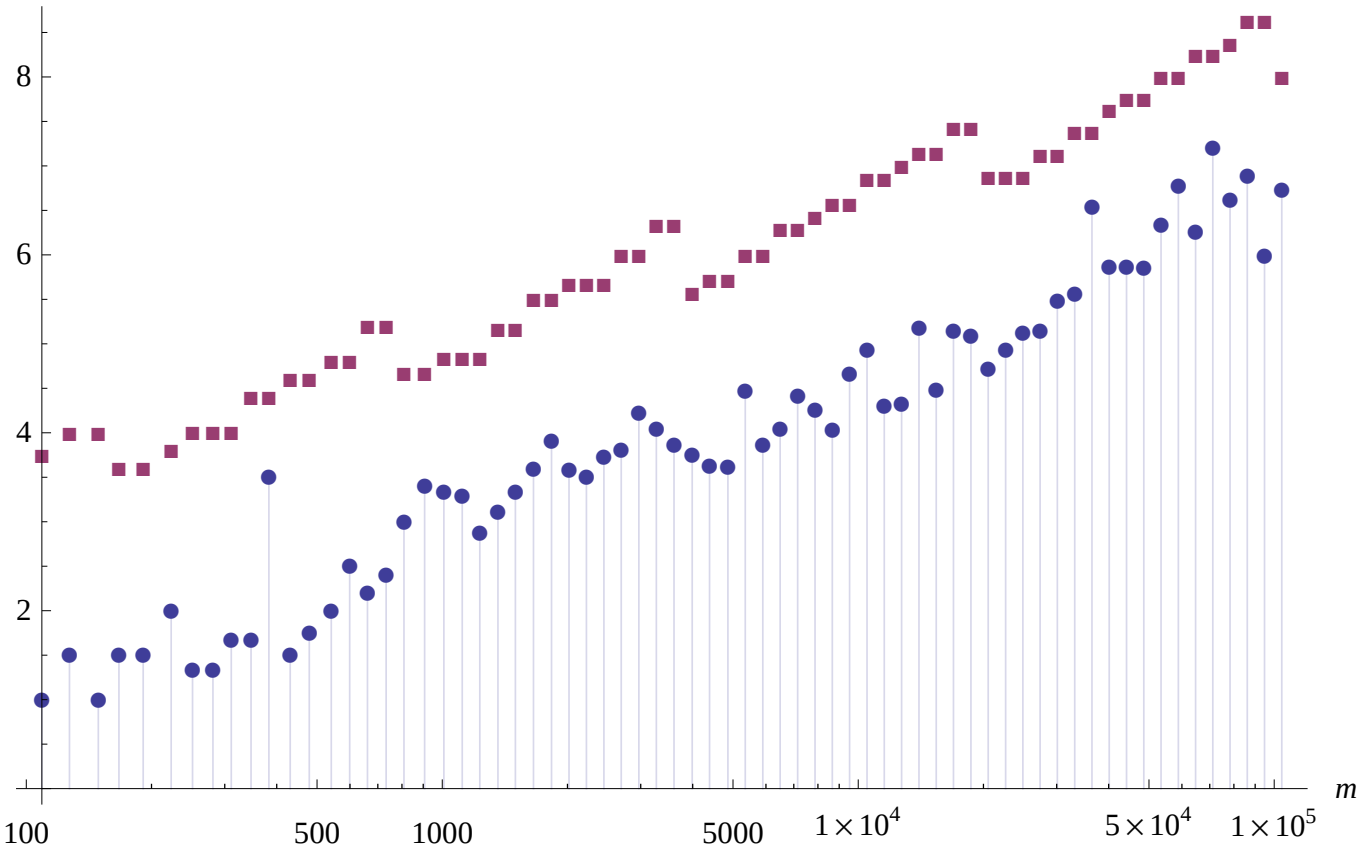


Figure: Practical speedup obtained with the new precision analysis compared with the theoretical improvement (m-axis in logarithmic scale). (■) is the ratio on precisions, (•) is the actual speedup.

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**.
- Can stabilize and attain **optimal** precision, even though naïve computation lose too much 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**.
- Can stabilize and attain **optimal** precision, even though naïve computation lose too much precision.

On differential equations

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**.
- Can stabilize and attain **optimal** precision, even though naïve computation lose too much precision.

On differential equations

- Can attain **optimal loss** in precision for differential equations with separation of variables.

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**.
- Can stabilize and attain **optimal** precision, even though naïve computation lose too much precision.

On differential equations

- Can attain **optimal loss** in precision for differential equations with separation of variables.
- Future works: higher order and $p = 2$.

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.

Differential equations, this current work

- Pierre Lairez and Tristan Vaccon On p-adic differential equations with separation of variables, ISSAC 2016.

Thank you for your attention

Thanks