

Factoring Linear Recurrence Operators

Mark van Hoeij¹

Florida State University

Braşov Romania

May 13, 2019

¹Supported by NSF 1618657

Recurrence operators with rational function coefficients

Let $a_i(n) \in \mathbb{Q}(n)$ be rational functions in n .

Recurrence relation:

$$a_k(n)u(n+k) + \cdots + a_1(n)u(n+1) + a_0(n)u(n) = 0.$$

Solutions $u(n)$ are viewed as functions on subsets of \mathbb{C} .

Recurrence operator: write the recurrence relation as $L(u) = 0$ where

$$L = a_k\tau^k + \cdots + a_0\tau^0 \in \mathbb{Q}(n)[\tau]$$

Here τ is the shift operator. It sends $u(n)$ to $u(n+1)$.

Recurrence relations come from many sources:

Zeilberger's algorithm, walks, QFT computations, OEIS, etc.

Recurrence operators with rational function coefficients

Let $a_i(n) \in \mathbb{Q}(n)$ be rational functions in n .

Recurrence relation:

$$a_k(n)u(n+k) + \cdots + a_1(n)u(n+1) + a_0(n)u(n) = 0.$$

Solutions $u(n)$ are viewed as functions on subsets of \mathbb{C} .

Recurrence operator: write the recurrence relation as $L(u) = 0$ where

$$L = a_k\tau^k + \cdots + a_0\tau^0 \in \mathbb{Q}(n)[\tau]$$

Here τ is the shift operator. It sends $u(n)$ to $u(n+1)$.

Recurrence relations come from many sources:

Zeilberger's algorithm, walks, QFT computations, OEIS, etc.

Goal: factoring recurrence operators

Factoring: if possible, write L as a composition $L_1 \circ L_2$ of lower order operators.

Computing **first order right-factors**:

Same as computing **hypergeometric solutions**, there are **algorithms** (Petkovšek 1992, vH 1999) and **implementations**.

Goal: compute **right-factors of order $d > 1$** .

Method 1: Hypergeometric solutions of a system of order $\binom{k}{d}$.

Method 2: Construct factors from special solutions.

Goal: factoring recurrence operators

Factoring: if possible, write L as a composition $L_1 \circ L_2$ of lower order operators.

Computing **first order right-factors**:

Same as computing **hypergeometric solutions**, there are **algorithms** (Petkovšek 1992, vH 1999) and **implementations**.

Goal: compute **right-factors of order $d > 1$** .

Method 1: Hypergeometric solutions of a **system of order $\binom{k}{d}$** .

Method 2: Construct factors from **special solutions**.

Example: Entry A025184 in OEIS

$$\begin{aligned}L(u) = & 33n(3n-1)(3n-2)u(n) \\ & + 11(2047n^3 - 10725n^2 + 17192n - 8520)u(n-1) \\ & - 9(4397n^3 + 10169n^2 - 110500n + 145368)u(n-2) \\ & - 54(2n-5)(5353n^2 - 33313n + 53904)u(n-3) \\ & - 115668(n-4)(2n-5)(2n-7)u(n-4) = 0.\end{aligned}$$

$L \in \mathbb{Q}(n)[\tau^{-1}]$ has order 4 and **n -degree 3**.

Our implementation finds a right-hand factor R where $R(u) =$

$$\begin{aligned}& 3n(3n-1)(3n-2)(221n^2 - 723n + 574)u(n) \\ & - 2(2n-1)(7735n^4 - 33040n^3 + 48239n^2 - 27998n + 5280)u(n-1) \\ & - 36(n-2)(2n-1)(2n-3)(221n^2 - 281n + 72)u(n-2)\end{aligned}$$

R order 2 but **n -degree 5** which is more than L !

(Explanation: R has 3 true and 2 apparent singularities).

Example: Entry A025184 in OEIS

$$\begin{aligned}L(u) = & 33n(3n-1)(3n-2)u(n) \\ & + 11(2047n^3 - 10725n^2 + 17192n - 8520)u(n-1) \\ & - 9(4397n^3 + 10169n^2 - 110500n + 145368)u(n-2) \\ & - 54(2n-5)(5353n^2 - 33313n + 53904)u(n-3) \\ & - 115668(n-4)(2n-5)(2n-7)u(n-4) = 0.\end{aligned}$$

$L \in \mathbb{Q}(n)[\tau^{-1}]$ has order 4 and **n -degree 3**.

Our implementation finds a right-hand factor R where $R(u) =$

$$\begin{aligned}& 3n(3n-1)(3n-2)(221n^2 - 723n + 574)u(n) \\ & - 2(2n-1)(7735n^4 - 33040n^3 + 48239n^2 - 27998n + 5280)u(n-1) \\ & - 36(n-2)(2n-1)(2n-3)(221n^2 - 281n + 72)u(n-2)\end{aligned}$$

R order 2 but **n -degree 5** which is more than L !

(Explanation: R has 3 true and 2 apparent singularities).

Gauss' lemma does not hold for $\mathbb{Q}[n][\tau] \subset \mathbb{Q}(n)[\tau]$

Gauss' lemma does not hold for difference operators:

- 1 Reducible operators in $\mathbb{Q}(n)[\tau]$ are often irreducible in $\mathbb{Q}[n][\tau]$.
- 2 L can have a right-factor R with higher n -degree than L (after clearing denominators).

This means:

- 1 It is not enough to factor in the τ -Weyl algebra $\mathbb{Q}[n][\tau]$.
- 2 Bounding n -degrees of right-factors is non-trivial.

Method 1: Reduce order- d factors to order-1 factors

Beke (1894) gave a method to reduce:

- order- d factors of a differential operator of order k
- to
- order-1 factors of several operators of order $\binom{k}{d}$.

Bronstein (ISSAC'1994) gave **significant improvements**:

- 1 Use only **one system** of order $\binom{k}{d}$
(instead of **several operators** of that order, whose factors had to be combined with a potentially **costly computation**)
- 2 This system has much **smaller coefficients**, which improves performance as well.

Beke 1894 / Bronstein 1994 works for recurrence operators as well.

Method 1: Reduce order- d factors to order-1 factors

Beke (1894) gave a method to reduce:

- order- d factors of a differential operator of order k
- to
- order-1 factors of several operators of order $\binom{k}{d}$.

Bronstein (ISSAC'1994) gave **significant improvements**:

- 1 Use only **one system** of order $\binom{k}{d}$
(instead of **several operators** of that order, whose factors had to be combined with a potentially **costly computation**)
- 2 This system has much **smaller coefficients**, which improves performance as well.

Beke 1894 / Bronstein 1994 works for recurrence operators as well.

Method 1: Reduce to order 1

Let $\mathcal{D} := \mathbb{Q}(n)[\tau]$.

Let $L \in \mathcal{D}$ have order k .

Suppose L has a right-factor R of order d .

Consider the \mathcal{D} -modules

$$M_L := \mathcal{D}/\mathcal{D}L \quad \text{and} \quad M_R := \mathcal{D}/\mathcal{D}R$$

and homomorphism:

$$\phi : \bigwedge^d M_L \rightarrow \bigwedge^d M_R$$

Over $\mathbb{Q}(n)$:

$$\dim \left(\bigwedge^d M_L \right) = \binom{k}{d} \quad \text{and} \quad \dim \left(\bigwedge^d M_R \right) = \binom{d}{d} = 1$$

Hence:

$\phi \rightsquigarrow$ a hypergeometric solution of the system for $\bigwedge^d M_L$

Method 1: Reduce to order 1

Let $\mathcal{D} := \mathbb{Q}(n)[\tau]$.

Let $L \in \mathcal{D}$ have order k .

Suppose L has a right-factor R of order d .

Consider the \mathcal{D} -modules

$$M_L := \mathcal{D}/\mathcal{D}L \quad \text{and} \quad M_R := \mathcal{D}/\mathcal{D}R$$

and homomorphism:

$$\phi: \bigwedge^d M_L \rightarrow \bigwedge^d M_R$$

Over $\mathbb{Q}(n)$:

$$\dim \left(\bigwedge^d M_L \right) = \binom{k}{d} \quad \text{and} \quad \dim \left(\bigwedge^d M_R \right) = \binom{d}{d} = 1$$

Hence:

$\phi \rightsquigarrow$ a **hypergeometric solution** of the system for $\bigwedge^d M_L$

System for $\bigwedge^d M_L$: Example with $k = 4$ and $d = 2$.

Let $L = \tau^4 + a_3\tau^3 + a_2\tau^2 + a_1\tau + a_0$ and $M_L := \mathcal{D}/DL$.

Action of τ on **basis** of $\bigwedge^2 M_L$ is:

$$b_1 := \tau^0 \wedge \tau^1 \mapsto \tau^1 \wedge \tau^2 = b_4$$

$$b_2 := \tau^0 \wedge \tau^2 \mapsto \tau^1 \wedge \tau^3 = b_5$$

$$b_3 := \tau^0 \wedge \tau^3 \mapsto \tau^1 \wedge \tau^4 = a_0 b_1 - a_2 b_4 - a_3 b_5$$

$$b_4 := \tau^1 \wedge \tau^2 \mapsto \tau^2 \wedge \tau^3 = b_6$$

$$b_5 := \tau^1 \wedge \tau^3 \mapsto \tau^2 \wedge \tau^4 = a_0 b_2 + a_1 b_4 - a_3 b_6$$

$$b_6 := \tau^2 \wedge \tau^3 \mapsto \tau^3 \wedge \tau^4 = a_0 b_3 + a_1 b_5 + a_2 b_6$$

($\tau^4 = -a_0\tau^0 - a_1\tau^1 - a_2\tau^2 - a_3\tau^3$ in M_L)

System: $AY = \tau(Y)$ where $A = \begin{pmatrix} 0 & 0 & a_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_0 \\ 1 & 0 & -a_2 & 0 & a_1 & 0 \\ 0 & 1 & -a_3 & 0 & 0 & a_1 \\ 0 & 0 & 0 & 1 & -a_3 & a_2 \end{pmatrix}$

System for $\bigwedge^d M_L$: Example with $k = 4$ and $d = 2$.

Let $L = \tau^4 + a_3\tau^3 + a_2\tau^2 + a_1\tau + a_0$ and $M_L := \mathcal{D}/\mathcal{D}L$.

Action of τ on **basis** of $\bigwedge^2 M_L$ is:

$$b_1 := \tau^0 \wedge \tau^1 \mapsto \tau^1 \wedge \tau^2 = b_4$$

$$b_2 := \tau^0 \wedge \tau^2 \mapsto \tau^1 \wedge \tau^3 = b_5$$

$$b_3 := \tau^0 \wedge \tau^3 \mapsto \tau^1 \wedge \tau^4 = a_0 b_1 - a_2 b_4 - a_3 b_5$$

$$b_4 := \tau^1 \wedge \tau^2 \mapsto \tau^2 \wedge \tau^3 = b_6$$

$$b_5 := \tau^1 \wedge \tau^3 \mapsto \tau^2 \wedge \tau^4 = a_0 b_2 + a_1 b_4 - a_3 b_6$$

$$b_6 := \tau^2 \wedge \tau^3 \mapsto \tau^3 \wedge \tau^4 = a_0 b_3 + a_1 b_5 + a_2 b_6$$

($\tau^4 = -a_0\tau^0 - a_1\tau^1 - a_2\tau^2 - a_3\tau^3$ in M_L)

System: $AY = \tau(Y)$ where $A = \begin{pmatrix} 0 & 0 & a_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_0 \\ 1 & 0 & -a_2 & 0 & a_1 & 0 \\ 0 & 1 & -a_3 & 0 & 0 & a_1 \\ 0 & 0 & 0 & 1 & -a_3 & a_2 \end{pmatrix}$

Hypergeometric solutions of systems

Suppose L has order k and a right-factor R of order d .

Let $N = \binom{k}{d}$ and A the $N \times N$ matrix as in the previous slide.

Then

$$AY = \tau(Y)$$

must have a **hypergeometric solution**:

$$Y = \lambda \begin{pmatrix} P_1 \\ \vdots \\ P_N \end{pmatrix} \quad \text{with } P_i \in \mathbb{Q}[n] \quad \text{and} \quad r := \frac{\tau(\lambda)}{\lambda} \in \mathbb{Q}(n)$$

Bronstein found (similar to Petkovšek's algorithm) that one can write $r = c \frac{a}{b}$ with $c \in \mathbb{Q}^*$ and $a, b \in \mathbb{Q}[n]$ monic with:

$$b \mid \text{denom}(A) \quad \text{and} \quad a \mid \text{denom}(A^{-1})$$

\rightsquigarrow almost an algorithm (still need c)

Hypergeometric solutions of systems

Suppose L has order k and a right-factor R of order d .

Let $N = \binom{k}{d}$ and A the $N \times N$ matrix as in the previous slide.

Then

$$AY = \tau(Y)$$

must have a **hypergeometric solution**:

$$Y = \lambda \begin{pmatrix} P_1 \\ \vdots \\ P_N \end{pmatrix} \quad \text{with } P_i \in \mathbb{Q}[n] \quad \text{and} \quad r := \frac{\tau(\lambda)}{\lambda} \in \mathbb{Q}(n)$$

Bronstein found (similar to Petkovšek's algorithm) that one can write $r = c \frac{a}{b}$ with $c \in \mathbb{Q}^*$ and $a, b \in \mathbb{Q}[n]$ **monic** with:

$$b \mid \text{denom}(A) \quad \text{and} \quad a \mid \text{denom}(A^{-1})$$

\rightsquigarrow almost an algorithm (**still need c**)

Computing c , improvements, implementation: Barkatou + vH.

More work in progress: Barkatou + vH + Middeke + Schneider.

If L has high order then $AY = \tau(Y)$ has high dimension $N = \binom{k}{d}$.

There is a faster method that works remarkably often even though it is not proved to work.

Another way to factor

LLL algorithm to factor $L \in \mathbb{Q}[x]$ in polynomial time:

- 1 Compute a p -adic solution α of L .
- 2 Find $M \in \mathbb{Z}[x]$ of lower degree with $M(\alpha) = 0$ if it exists.
- 3 If no such M exists, then L is irreducible, otherwise $\gcd(L, M)$ is a non-trivial factor.

In order for this to work for $L \in \mathbb{Q}(n)[\tau]$, the solution in Step 1 must meet this requirement:

Definition

A solution u of L is **order-special** if it satisfies an operator M of lower order.

Unlike the polynomial case, most solutions of most reducible operators are not order-special.

Another way to factor

LLL algorithm to factor $L \in \mathbb{Q}[x]$ in polynomial time:

- 1 Compute a p -adic solution α of L .
- 2 Find $M \in \mathbb{Z}[x]$ of lower degree with $M(\alpha) = 0$ if it exists.
- 3 If no such M exists, then L is irreducible, otherwise $\gcd(L, M)$ is a non-trivial factor.

In order for this to work for $L \in \mathbb{Q}(n)[\tau]$, the solution in Step 1 must meet this requirement:

Definition

A solution u of L is **order-special** if it satisfies an operator M of lower order.

Unlike the polynomial case, most solutions of most reducible operators are not order-special.

Factoring with a special solution

If L is reducible and u is order-special then write:

$$R := \sum_{i=0}^{k-1} \left(\sum_{j=0}^{\text{Degree bound}} c_{ij} n^j \right) \tau^i$$

Then

$$R(u) = 0 \quad \rightsquigarrow \quad \text{equations for } c_{ij} \quad \rightsquigarrow \quad R$$

We need:

- 1 Special solutions
- 2 Degree bound

(How to bound the number of apparent singularities?).

Factoring with a special solution

If L is reducible and u is order-special then write:

$$R := \sum_{i=0}^{k-1} \left(\overset{\text{Degree bound}}{\sum_{j=0}^i} c_{ij} \tau^j \right) \tau^i$$

Then

$$R(u) = 0 \rightsquigarrow \text{equations for } c_{ij} \rightsquigarrow R$$

We need:

- 1 Special solutions
- 2 Degree bound

(How to bound the number of **apparent singularities**?).

Example: Special solutions

$$\begin{aligned}L(u) &= 33n(3n-1)(3n-2)u(n) \\ &\quad + \dots \\ &\quad - 115668(n-4)(2n-5)(2n-7)u(n-4) = 0.\end{aligned}$$

$L(u) = 0$ determines $u(n)$ in terms of $u(n-1), \dots, u(n-4)$
except if n is a root of the **leading coefficient**.

Take $q \in \{0, \frac{1}{3}, \frac{2}{3}\}$. Define $u : q + \mathbb{Z} \rightarrow \mathbb{C}$ with:

$$L(u) = 0, \quad u(n) = 0 \text{ for all } n < q, \quad u(q) = 1.$$

Then u is called a **leading-special** solution. Likewise:

Roots of the **trailing coefficient** \rightsquigarrow **trailing-special** solutions.

(Leading/trailing)-special solutions are frequently order-special!

Example: Special solutions

$$\begin{aligned}L(u) &= 33n(3n-1)(3n-2)u(n) \\ &+ \dots \\ &- 115668(n-4)(2n-5)(2n-7)u(n-4) = 0.\end{aligned}$$

$L(u) = 0$ determines $u(n)$ in terms of $u(n-1), \dots, u(n-4)$
except if n is a root of the **leading coefficient**.

Take $q \in \{0, \frac{1}{3}, \frac{2}{3}\}$. Define $u : q + \mathbb{Z} \rightarrow \mathbb{C}$ with:

$$L(u) = 0, \quad u(n) = 0 \text{ for all } n < q, \quad u(q) = 1.$$

Then u is called a **leading-special** solution. Likewise:

Roots of the **trailing coefficient** \rightsquigarrow **trailing-special** solutions.

(Leading/trailing)-special solutions are frequently order-special!

Example: Special solutions

$$\begin{aligned}L(u) &= 33n(3n-1)(3n-2)u(n) \\ &\quad + \dots \\ &\quad - 115668(n-4)(2n-5)(2n-7)u(n-4) = 0.\end{aligned}$$

$L(u) = 0$ determines $u(n)$ in terms of $u(n-1), \dots, u(n-4)$
except if n is a root of the **leading coefficient**.

Take $q \in \{0, \frac{1}{3}, \frac{2}{3}\}$. Define $u : q + \mathbb{Z} \rightarrow \mathbb{C}$ with:

$$L(u) = 0, \quad u(n) = 0 \text{ for all } n < q, \quad u(q) = 1.$$

Then u is called a **leading-special** solution. Likewise:

Roots of the **trailing coefficient** \rightsquigarrow trailing-special solutions.

(Leading/trailing)-special solutions are frequently order-special!

Leading/trailing vs order special solutions

(Leading/trailing)-special solutions are frequently order-special.

We can only explain that for certain cases:

Suppose L is a Least-Common-Left-Multiple of L_1 and L_2 .

Suppose L_1 and L_2 do not have the same valuation growths at some $q + \mathbb{Z}$ for some $q \in \mathbb{C}$.

Then a (leading/trailing)-special solution² is order-special.

Valuation-growth: the valuation (root/pole order) at $q + \text{large } n$ minus the valuation at $q - \text{large } n$.

²of L or its desingularization

Leading/trailing vs order special solutions

(Leading/trailing)-special solutions are frequently order-special.

We can only explain that for certain cases:

Suppose L is a Least-Common-Left-Multiple of L_1 and L_2 .

Suppose L_1 and L_2 do not have the same **valuation growths** at some $q + \mathbb{Z}$ for some $q \in \mathbb{C}$.

Then a (leading/trailing)-special solution² is **order-special**.

Valuation-growth: the valuation (root/pole order) at $q + \text{large } n$ minus the valuation at $q - \text{large } n$.

²of L or its desingularization

Degree bound (with Yi Zhou)

Due to **apparent singularities**, a right-factor R of L can have higher n -degree than L .

A bound can be computed from **generalized exponents**.

Generalized exponents \approx asymptotic behavior of solutions.

Example: $L = \tau - r$ with $r = 7n^3(1 + 8n^{-1} + \dots n^{-2} + \dots)$.

The **dominant part** of r is $e = 7n^3(1 + 8n^{-1})$.

This e encodes the dominant part of the solution

$$u(n) = 7^n \Gamma(n)^3 n^8 (1 + \dots n^{-1} + \dots n^{-2} + \dots)$$

Definition

Let $e = c \cdot n^\nu \cdot (1 + c_1 n^{-1/r} + c_2 n^{-2/r} + \dots + c_r n^{-1})$.

Then e is called a **generalized exponent** of L if:

The operator obtained by dividing solutions of L by $\text{Sol}(\tau - e)$ has an **indicial equation** with 0 as a root.

Degree bound (with Yi Zhou)

Due to **apparent singularities**, a right-factor R of L can have higher n -degree than L .

A bound can be computed from **generalized exponents**.

Generalized exponents \approx asymptotic behavior of solutions.

Example: $L = \tau - r$ with $r = 7n^3(1 + 8n^{-1} + \dots n^{-2} + \dots)$.

The **dominant part** of r is $e = 7n^3(1 + 8n^{-1})$.

This e encodes the dominant part of the solution

$$u(n) = 7^n \Gamma(n)^3 n^8 (1 + \dots n^{-1} + \dots n^{-2} + \dots)$$

Definition

Let $e = c \cdot n^\nu \cdot (1 + c_1 n^{-1/r} + c_2 n^{-2/r} + \dots + c_r n^{-1})$.

Then e is called a **generalized exponent** of L if:

The operator obtained by dividing solutions of L by $\text{Sol}(\tau - e)$ has an **indicial equation** with 0 as a root.

Degree bound (with Yi Zhou)

Due to **apparent singularities**, a right-factor R of L can have higher n -degree than L .

A bound can be computed from **generalized exponents**.

Generalized exponents \approx asymptotic behavior of solutions.

Example: $L = \tau - r$ with $r = 7n^3(1 + 8n^{-1} + \dots n^{-2} + \dots)$.

The **dominant part** of r is $e = 7n^3(1 + 8n^{-1})$.

This e encodes the dominant part of the solution

$$u(n) = 7^n \Gamma(n)^3 n^8 (1 + \dots n^{-1} + \dots n^{-2} + \dots)$$

Definition

Let $e = c \cdot n^\nu \cdot (1 + c_1 n^{-1/r} + c_2 n^{-2/r} + \dots + c_r n^{-1})$.

Then e is called a **generalized exponent** of L if:

The operator obtained by **dividing solutions of L by $\text{Sol}(\tau - e)$** has an **indicial equation with 0 as a root**.

Degree bound (with Yi Zhou)

Let $R = r_d \tau^d + \cdots + r_0 \tau^0$ be a right-factor of L in $\mathbb{Q}(n)[\tau]$.

$$\begin{aligned} \det(R) &:= (-1)^d \frac{r_0}{r_d} \in \mathbb{Q}(n) \\ &= c n^\nu (1 + c_1 n^{-1} + c_2 n^{-2} + \cdots) \in \mathbb{Q}((n^{-1})) \end{aligned}$$

Dominant part:

$$\text{dom}(\det(R)) = c n^\nu (1 + c_1 n^{-1})$$

$c_1 =$ number of apparent singularities of R (with multiplicity)
+ a term that comes from $\{\text{true singularities of } R\}$
 $\subseteq \{\text{true singularities of } L\}$

$\{\text{gen. exp. of } L\} \supseteq \{\text{gen. exp. of } R\} \rightsquigarrow \text{dom}(\det(R)) \rightsquigarrow c_1$
 $\rightsquigarrow \text{bound}(\text{number apparent singularities}) \rightsquigarrow \text{degree bound}$

Degree bound (with Yi Zhou)

Let $R = r_d \tau^d + \cdots + r_0 \tau^0$ be a right-factor of L in $\mathbb{Q}(n)[\tau]$.

$$\begin{aligned}\det(R) &:= (-1)^d \frac{r_0}{r_d} \in \mathbb{Q}(n) \\ &= c n^\nu (1 + c_1 n^{-1} + c_2 n^{-2} + \cdots) \in \mathbb{Q}((n^{-1}))\end{aligned}$$

Dominant part:

$$\text{dom}(\det(R)) = c n^\nu (1 + c_1 n^{-1})$$

$c_1 =$ **number of apparent singularities** of R (with multiplicity)
+ a term that comes from $\{\text{true singularities of } R\}$
 $\subseteq \{\text{true singularities of } L\}$

$\{\text{gen. exp. of } L\} \supseteq \{\text{gen. exp. of } R\} \rightsquigarrow \text{dom}(\det(R)) \rightsquigarrow c_1$
 $\rightsquigarrow \text{bound}(\text{number apparent singularities}) \rightsquigarrow \text{degree bound}$

Irreducibility proof

Except for special cases, method 2 **does not prove** that the factors it finds are **irreducible**.

Suppose L is not factored by method 2.

Idea:

- Gen. exponents \rightsquigarrow finite set of potential $\text{dom}(\det(R))$
- p -curvature \rightsquigarrow conditions mod p for $\text{dom}(\det(R))$
- Incompatible? \rightsquigarrow L is irreducible.

Overview:

- 1 Factor with method 2.
- 2 Apply the above idea to the factors.
- 3 Any factor not proved irreducible: fall back on method 1.

Irreducibility proof

Except for special cases, method 2 **does not prove** that the factors it finds are **irreducible**.

Suppose L is not factored by method 2.

Idea:

- Gen. exponents \rightsquigarrow finite set of potential $\text{dom}(\det(R))$
- p -curvature \rightsquigarrow conditions mod p for $\text{dom}(\det(R))$
- Incompatible? \rightsquigarrow L is irreducible.

Overview:

- 1 Factor with method 2.
- 2 Apply the above idea to the factors.
- 3 Any factor not proved irreducible: fall back on method 1.