Eine Implementierung des Zahlkörpersiebes

Johannes Lippmann

September 14, 2023

Was wird gesucht?

Sei $n \in \mathbb{N}$ ungerade. Gesucht sind $p, q \in \mathbb{Z}$, so dass nichttrivial gilt:

$$n = p \cdot q$$

Was wird gesucht?

Sei $n \in \mathbb{N}$ ungerade. Gesucht sind $p, q \in \mathbb{Z}$, so dass nichttrivial gilt:

$$n = p \cdot q$$

Sei $n \in \mathbb{N}$ ungerade. Gesucht sind $x, y \in \mathbb{Z}$, so dass nichttrivial gilt:

$$n = x^2 - y^2$$

Was wird gesucht?

Sei $n \in \mathbb{N}$ ungerade. Gesucht sind $p, q \in \mathbb{Z}$, so dass nichttrivial gilt:

$$n = p \cdot q$$

Sei $n \in \mathbb{N}$ ungerade. Gesucht sind $x, y \in \mathbb{Z}$, so dass nichttrivial gilt:

$$\begin{aligned} n &= x^2 - y^2 \\ &= (x + y) \cdot (x - y) \end{aligned}$$

Das Problem relaxieren

$$n = x^2 - y^2$$

Das Problem relaxieren

$$
\begin{aligned}
& & n &= x^2 - y^2 \\
\Rightarrow & & 0 &\equiv x^2 - y^2 \pmod{n}
\end{aligned}
$$

Das Problem relaxieren

$$
\begin{aligned}
& & n &= x^2 - y^2 \\
\Rightarrow & & 0 &\equiv x^2 - y^2 \pmod{n} \\
\Leftrightarrow \exists k \in \mathbb{Z}: & & n \cdot k &= (x+y) \cdot (x-y)
\end{aligned}
$$

Die Chance, dass die Faktoren von n gesplittet werden ist etwa $\frac{2}{3}$.

Faktoren von n finden mit Quadraten

Example

Ein Faktor von $n = 221$ wird gesucht und wir kennen die Beziehung:

$$0 \equiv 910^2 - 637^2 \pmod{221}$$

Faktoren von n finden mit Quadraten

Example

Ein Faktor von $n = 221$ wird gesucht und wir kennen die Beziehung:

$$0 \equiv 910^2 - 637^2 \pmod{221}$$

Diese Zahlen sind dann Kandidaten für Faktoren:

$$\gcd(221, 910 + 637)$$
$$\gcd(221, 910 - 637)$$

Faktoren von n finden mit Quadraten

Example

Ein Faktor von $n = 221$ wird gesucht und wir kennen die Beziehung:

$$0 \equiv 910^2 - 637^2 \pmod{221}$$

Diese Zahlen sind dann Kandidaten für Faktoren:

$$\gcd(221, 910 + 637) = 221$$
$$\gcd(221, 910 - 637) = 13$$

Faktor gefunden: 13

Zusammenfassung: Faktoren von n finden mit Quadraten

1. Finde $x, y \in \mathbb{Z}$ so dass $x^2 \equiv y^2 \pmod{n}$
2. Teste, ob $\gcd(n, x + y)$ oder $\gcd(n, x - y)$ Faktoren sind (etwa $\frac{2}{3}$ Chance)
3. Falls nötig, gehe zurück zu 1.

Smoothe Zahlen

Definition

Eine Faktorbasis P ist eine Menge von Primzahlen.

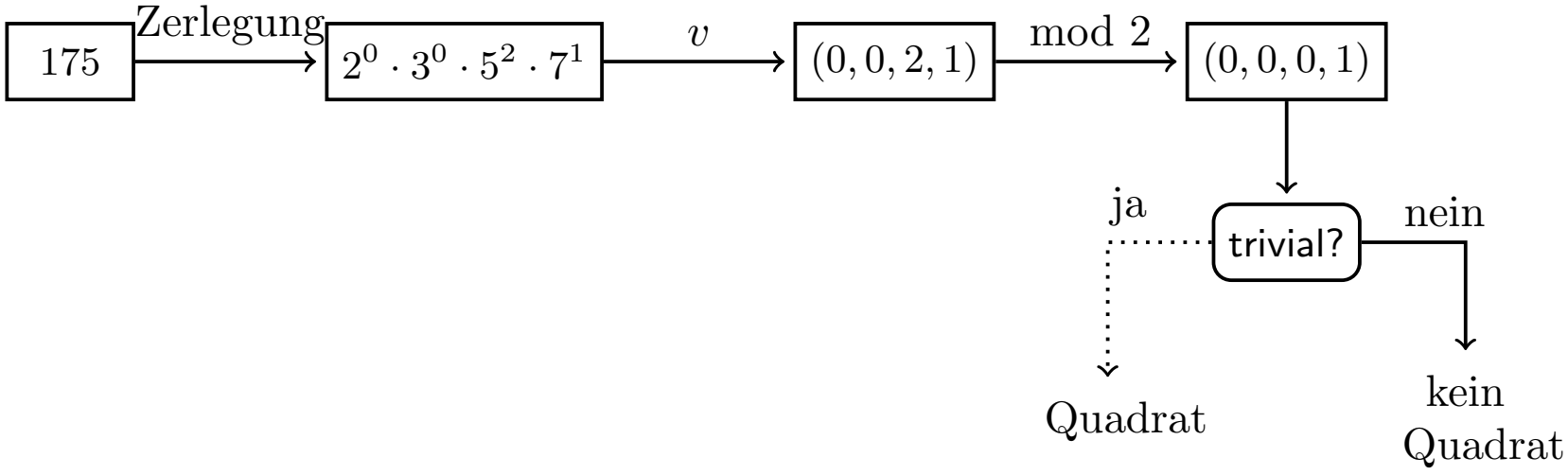
Definition

Eine Zahl x heißt smooth über einer Faktorbasis P, wenn alle Primfaktoren von x in P enthalten sind.

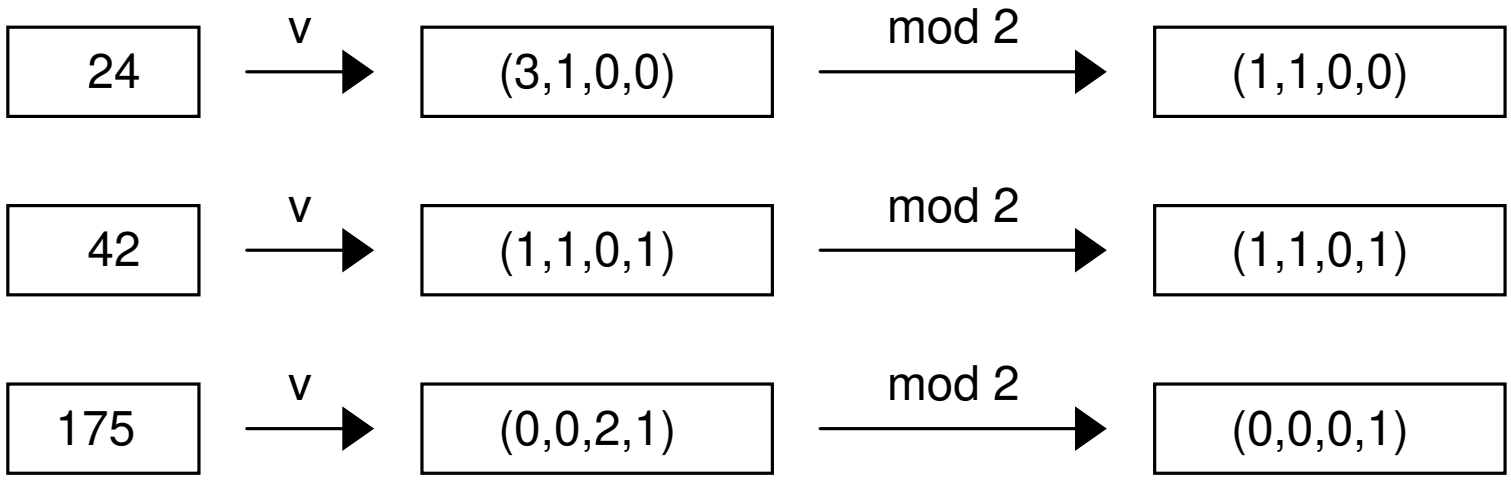
Example

$175 = 5 \cdot 5 \cdot 7$ ist smooth über der Faktorbasis $\{2, 3, 5, 7\}$.

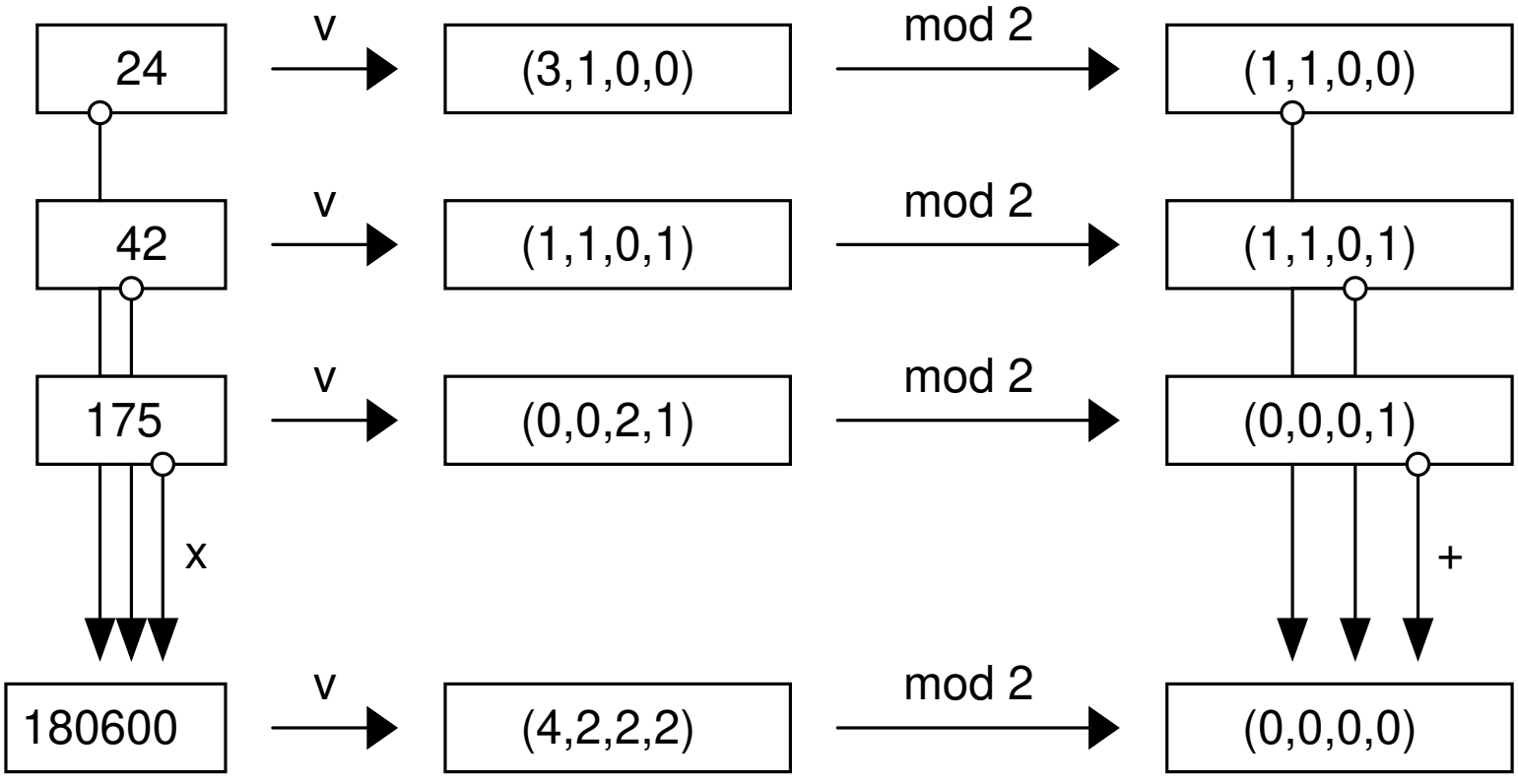
Smoothe Zahlen als Quadrate erkennen



Smoothe Zahlen multiplizieren



Smoothe Zahlen zu Quadraten multiplizieren



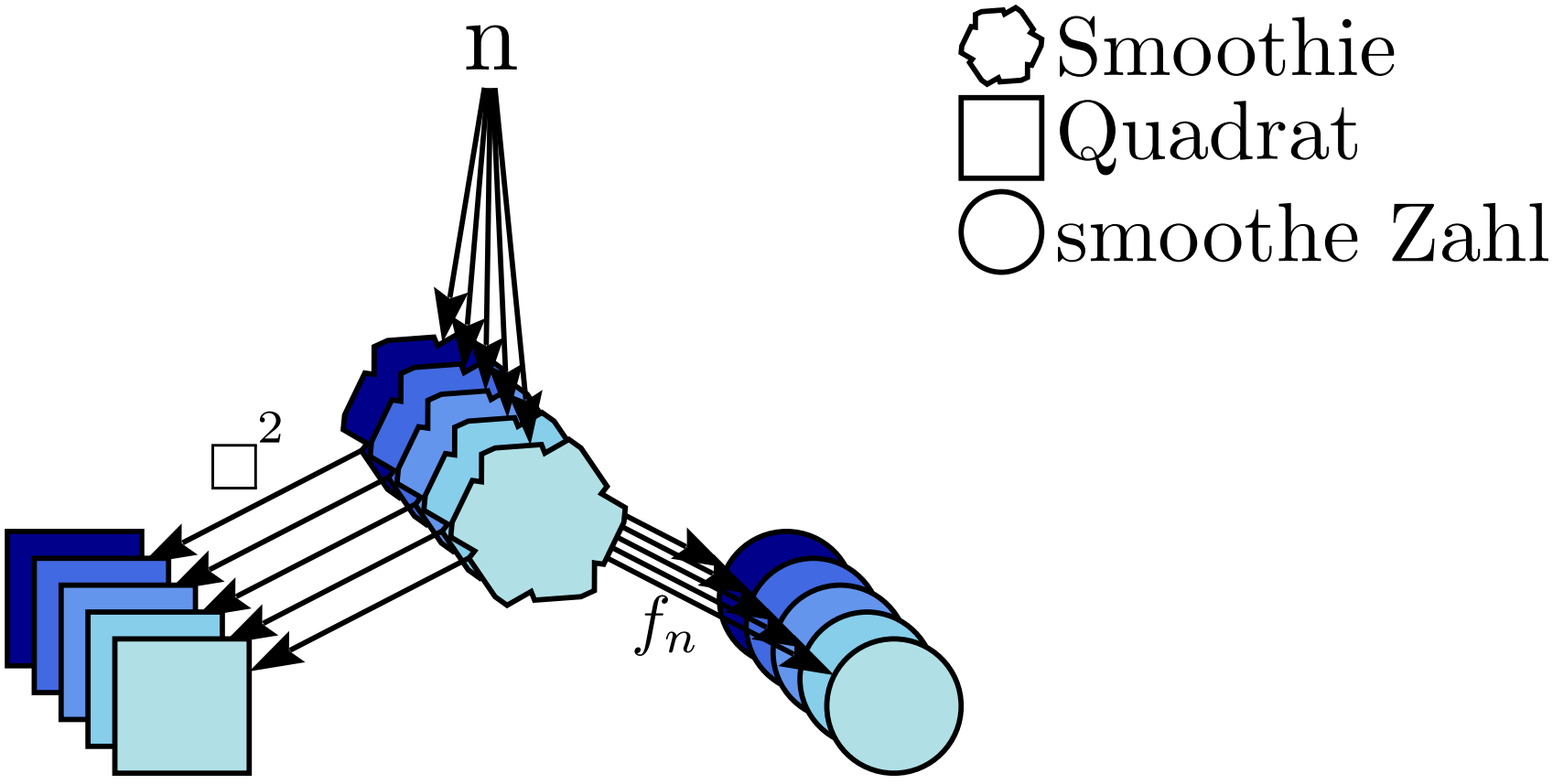
Smoothies

Definition

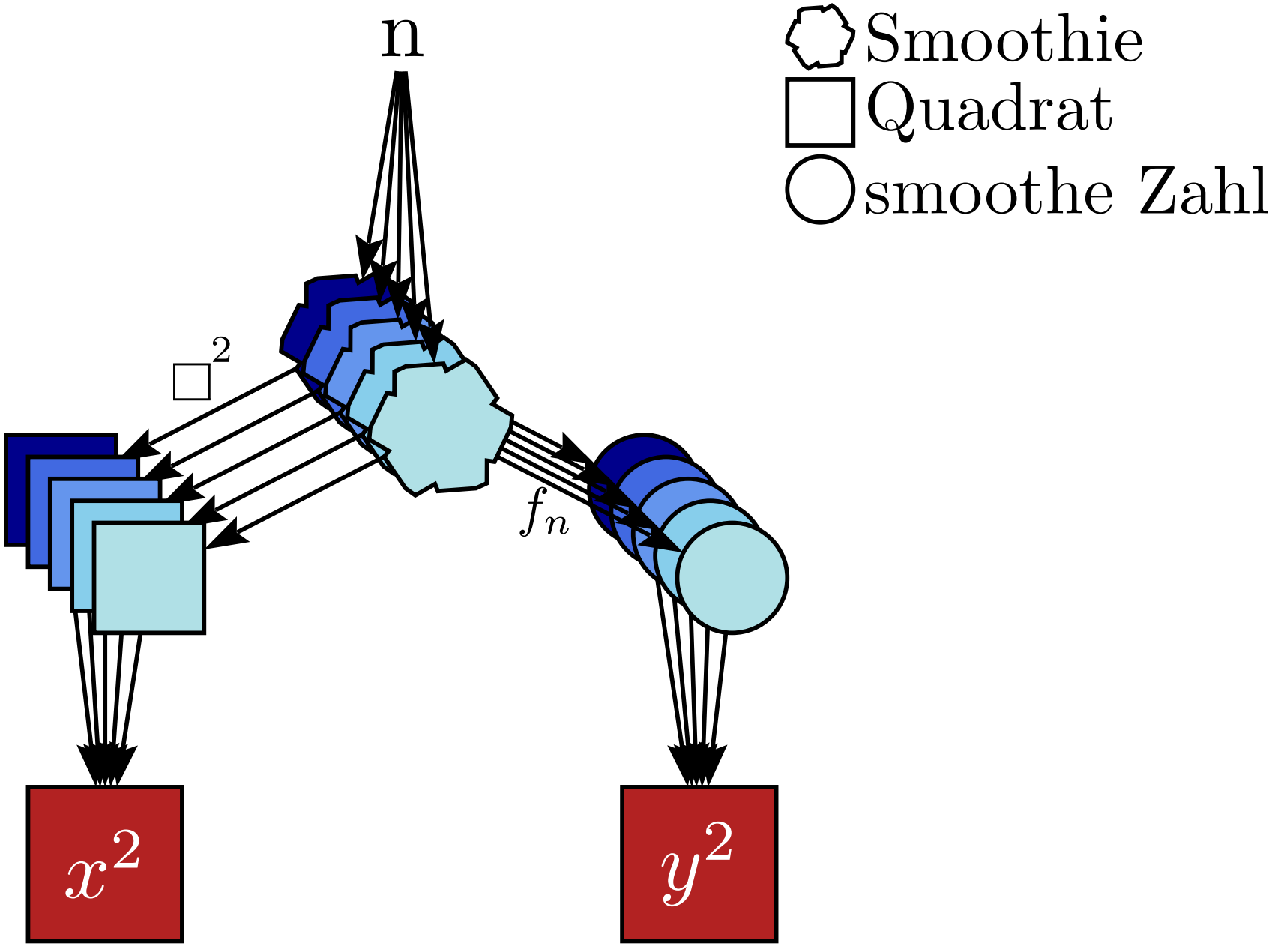
Sei S eine Menge, $f : S \to \mathbb{Z}$ eine Funktion und P eine Faktorbasis. Dann nennen wir $s \in S$ einen Smoothie, wenn $f(s) \in \mathbb{Z}$ smooth über P ist. f nennen wir dann die Smoothiefunktion.

Das sind eigentlich keine Fachbegriffe, aber Worte dafür zu haben macht vieles einfacher.

Dixons Algorithmus: Plan zum Faktorisieren



Dixons Algorithmus: Plan zum Faktorisieren



Dixons Algorithmus: Plan zum Faktorisieren

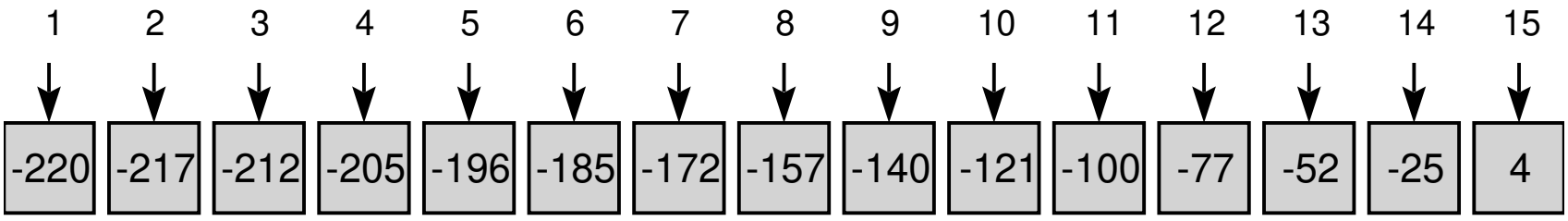
$$y^2 = \prod_{s \in S_d} f_n(s) \equiv \prod_{r \in S_s} s^2 = \left(\prod_{s \in S_s} s \right)^2 = x^2 \pmod{n}$$

Dixons Algorithmus: Beispielhafter Verlauf

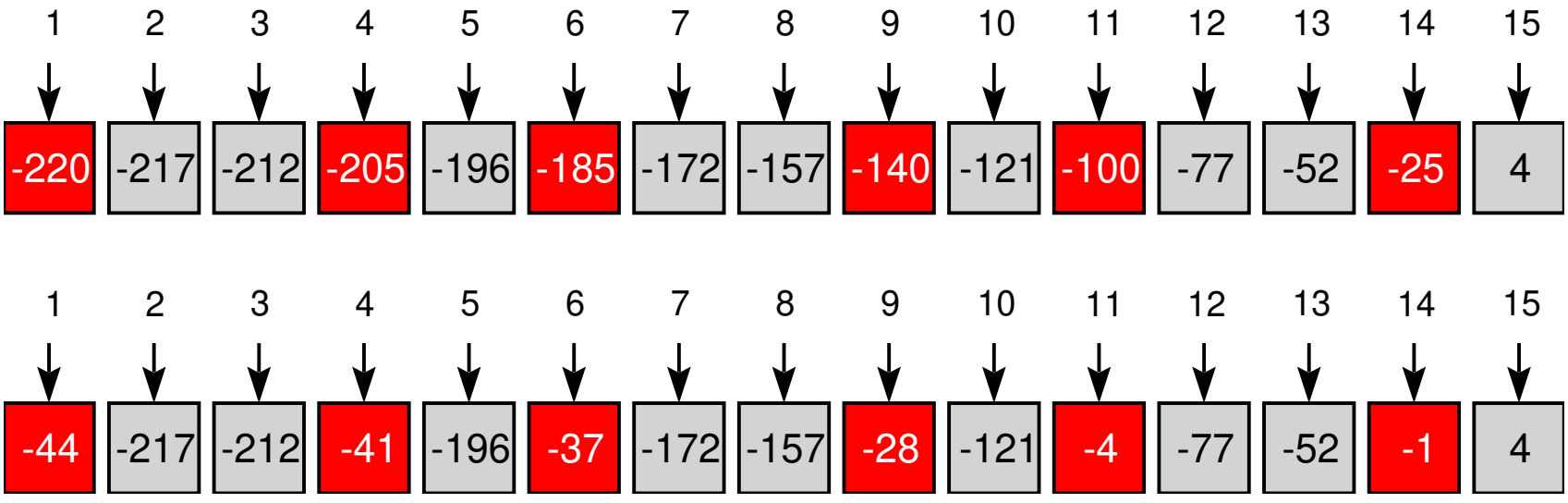
Das Quadratische Sieb

Idee: Smoothies schneller finden durch die schlauere Smoothiefunktion $f_n(x) = x^2 - n$

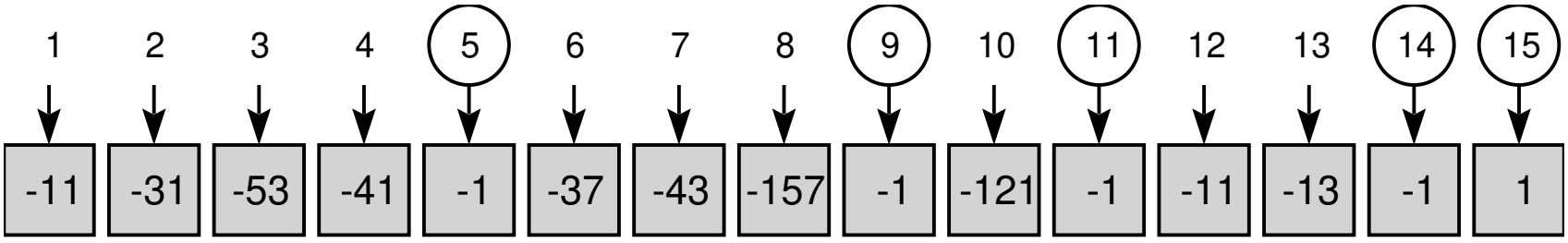
Quadratisches Sieb: Array intialisiert



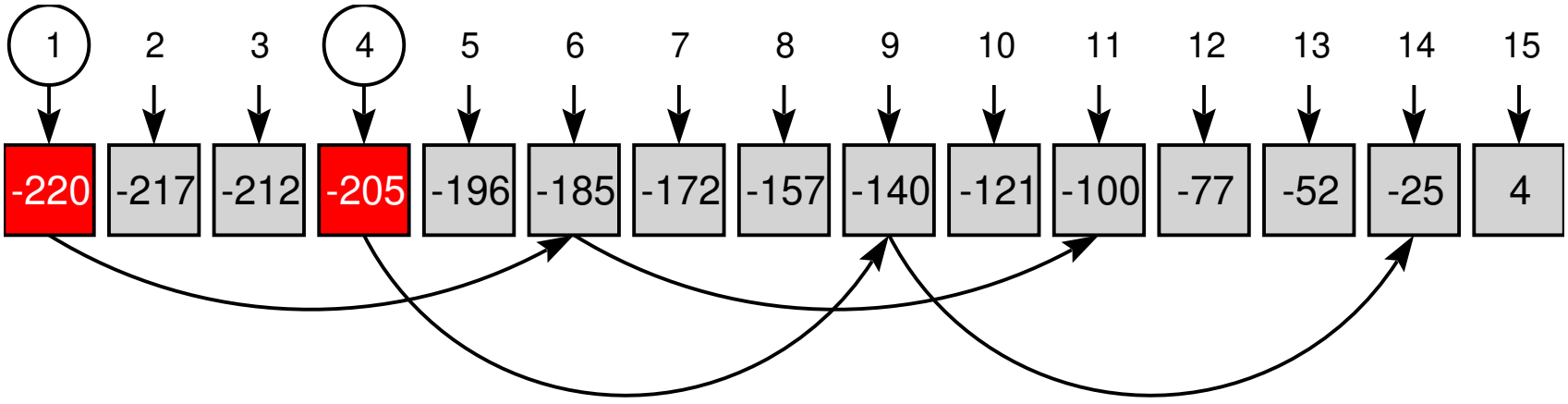
Quadratisches Sieb: 5 herausdividieren



Quadratisches Sieb: Smoothies ernten



Quadratisches Sieb: Divisionen durch 5 einsparen



Quadratisches Sieb: Beispielhafter Verlauf

Das Zahlkörpersieb

Ideen:

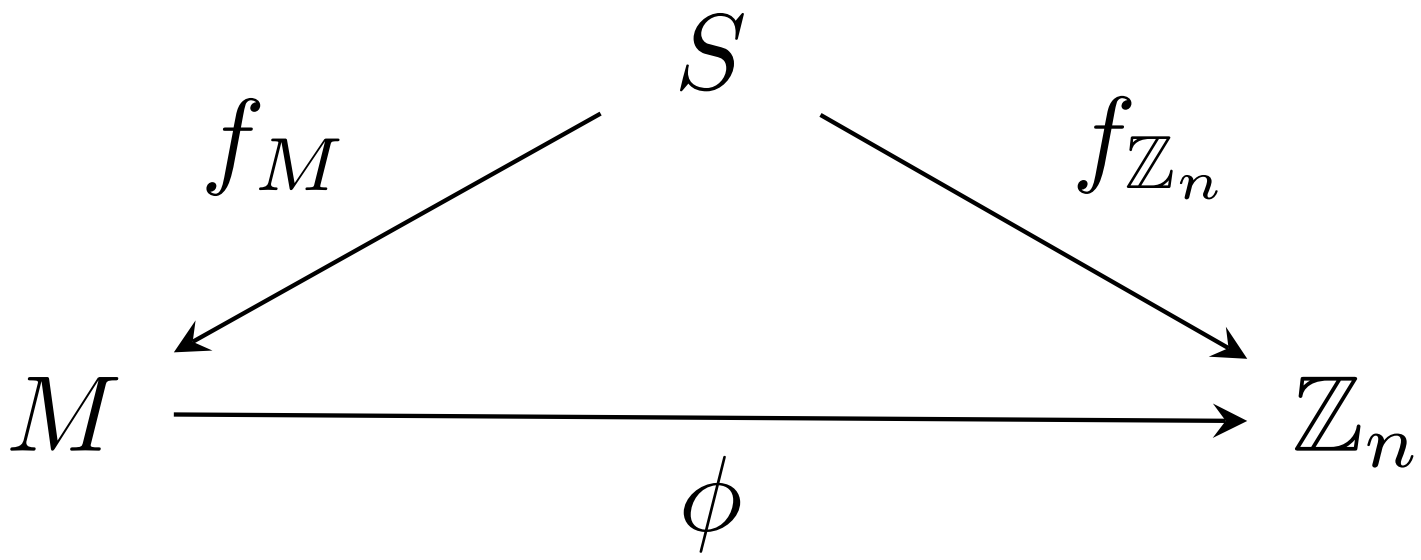
- Vielleicht können Polynome höheren Grades mehr Smoothies erzeugen.

Das Zahlkörpersieb

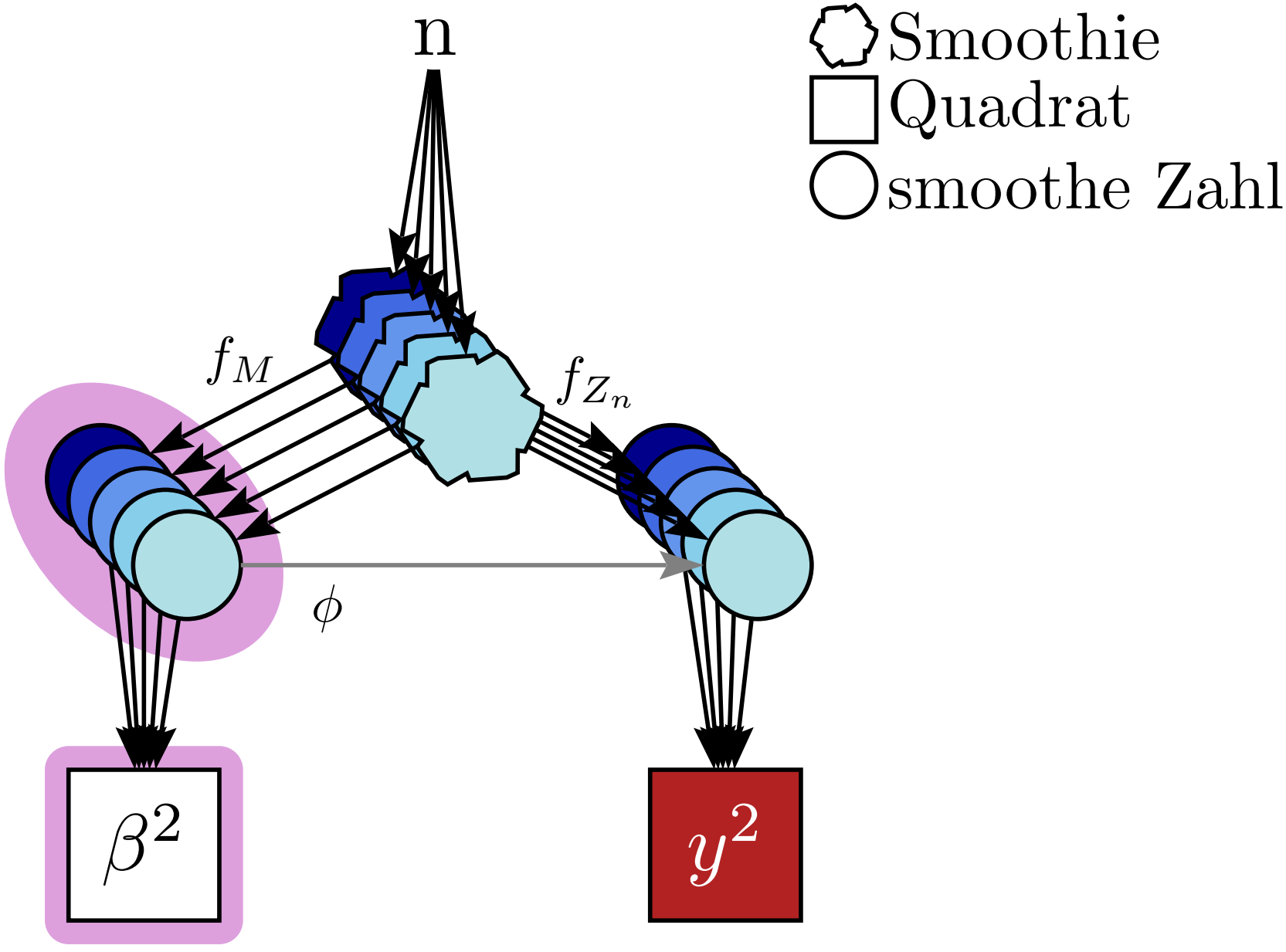
Ideen:

- Vielleicht können Polynome höheren Grades mehr Smoothies erzeugen.
- Smoothe Elemente treten vielleicht in anderen Monoiden als $(\mathbb{Z}, \cdot)$ häufiger auf

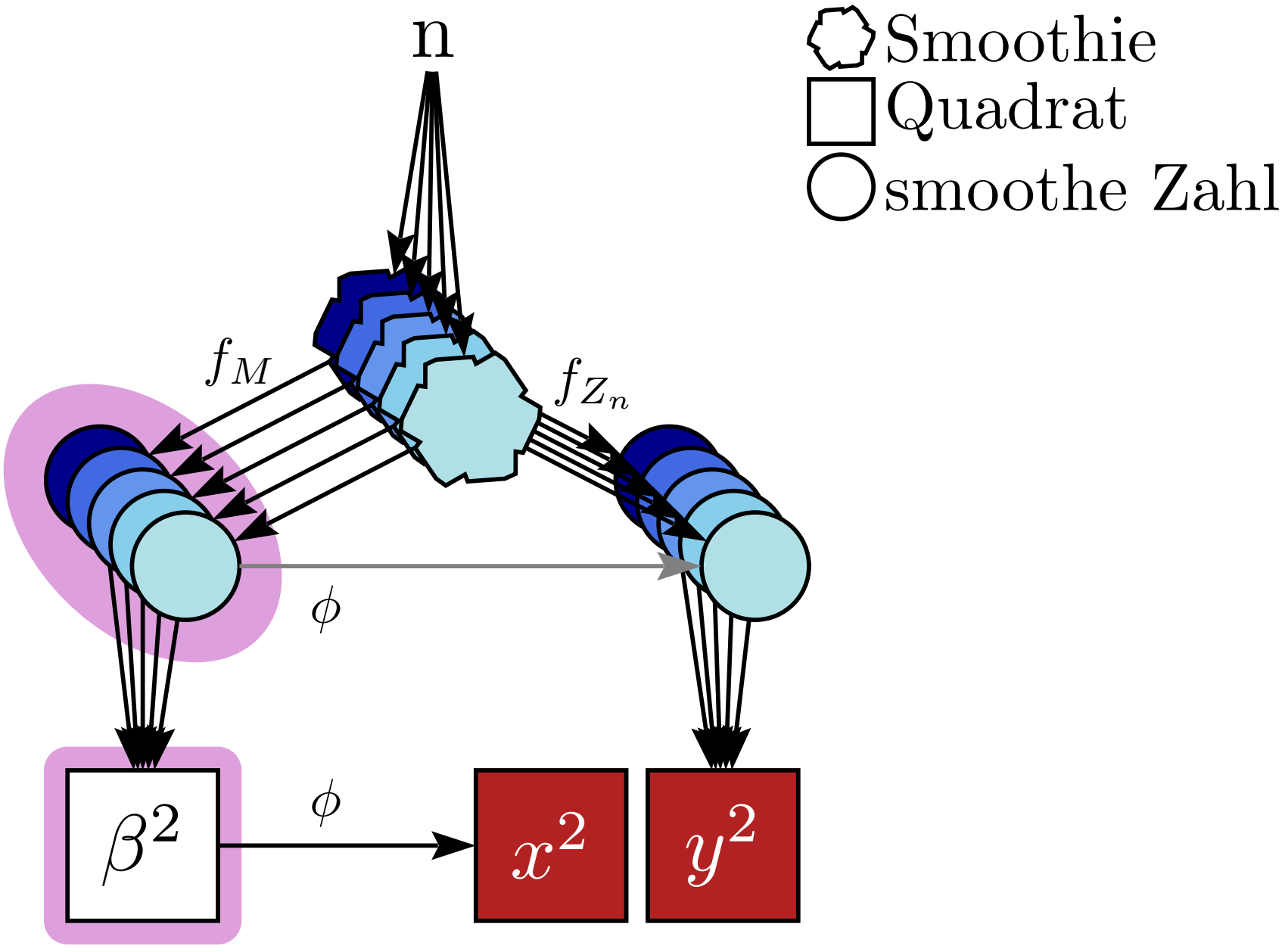
Zahlkörpersieb: Zwei Smoothiefunktionen



Zahlkörpersieb: Plan zum Faktorisieren

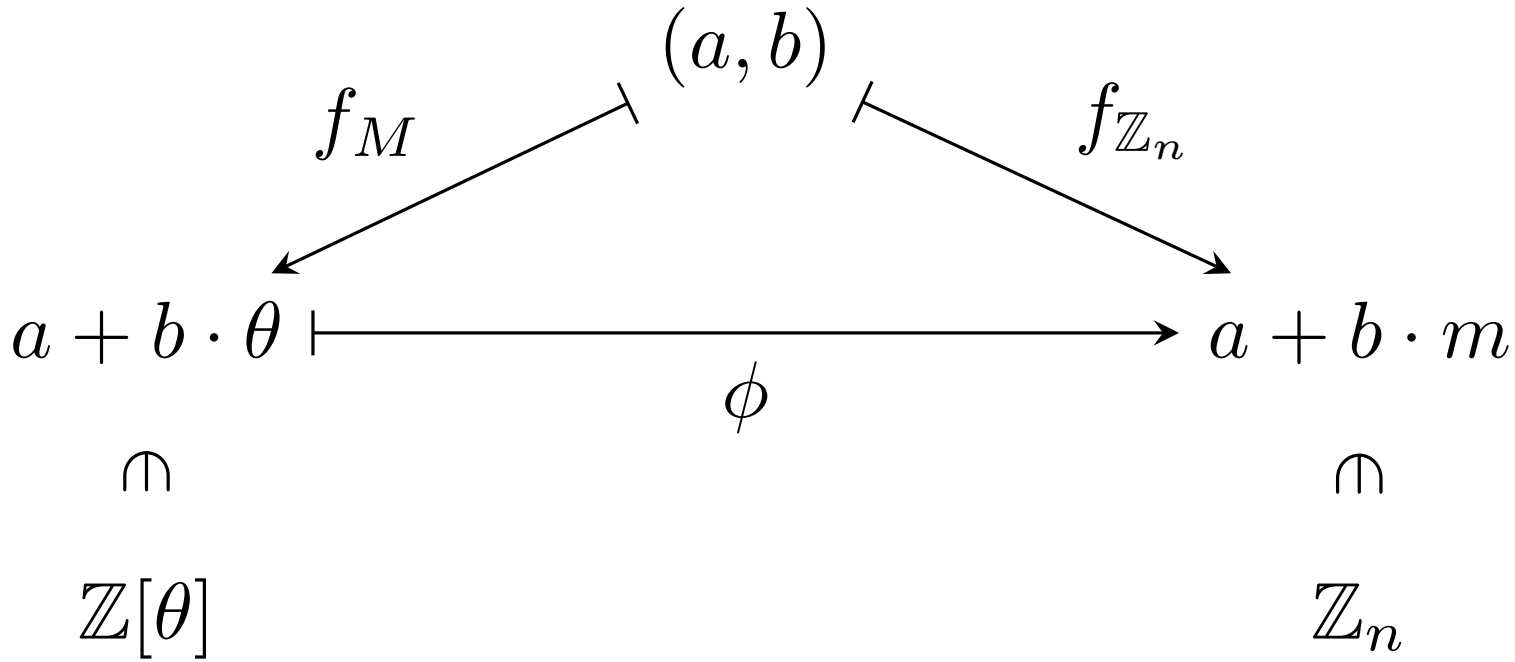


Zahlkörpersieb: Plan zum Faktorisieren



Zahlkörpersieb: Zwei Smoothiefunktionen konkret

Sei $\theta \in \mathbb{C}$ Nullstelle eines normierten, irreduziblen Polynoms $\texttt{poly} \in \mathbb{Z}[\theta]$ und $m \in \mathbb{Z}$, so dass $\texttt{poly}(m) \equiv 0 \pmod{n}$.



Algebraische Integer $\mathfrak{O}_{\mathbb{Q}(\theta)}$

Definition

(Komplexe) Nullstellen von irreduziblen, normierten Polynomen mit ganzzahligen Koeffizienten heißen algebraische Integer und bilden mit Addition und Multiplikation den (kommutativen) Ring A. Ist $\mathbb{Q}(\theta)$ ein Zahlkörper so bezeichnet $\mathfrak{O}_{\mathbb{Q}(\theta)} := A \cap \mathbb{Q}(\theta)$ die algebraischen Integer in $\mathbb{Q}(\theta)$.

Example

$\sqrt[5]{3} \in A$ wegen $x^5 - 3$.
$\frac{2}{3} \notin A$.

Example

$\frac{1+\sqrt{5}}{2} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{5})}$, wegen $x^2 - x + 1$.

Eigenschaften von $\mathfrak{D}_{\mathbb{Q}(\theta)}$

Sei θ ein algebrischer Integer

Eigenschaften von $\mathfrak{O}_{\mathbb{Q}(\theta)}$

Sei θ ein algebrischer Integer

- $\mathbb{Z}[\theta] \subset \mathfrak{O}_{\mathbb{Q}(\theta)} \subset \mathbb{Q}(\theta)$

Eigenschaften von $\mathfrak{O}_{\mathbb{Q}(\theta)}$

Sei θ ein algebrischer Integer

- $\mathbb{Z}[\theta] \subset \mathfrak{O}_{\mathbb{Q}(\theta)} \subset \mathbb{Q}(\theta)$
- $\mathfrak{O}_{\mathbb{Q}(\theta)}$ ist ein Dedekindring. Ideale in $\mathfrak{O}_{\mathbb{Q}(\theta)}$ haben eine eindeuige Zerlegung in Primideale.

Eigenschaften von $\mathfrak{O}_{\mathbb{Q}(\theta)}$

Sei θ ein algebrischer Integer

- $\mathbb{Z}[\theta] \subset \mathfrak{O}_{\mathbb{Q}(\theta)} \subset \mathbb{Q}(\theta)$
- $\mathfrak{O}_{\mathbb{Q}(\theta)}$ ist ein Dedekindring. Ideale in $\mathfrak{O}_{\mathbb{Q}(\theta)}$ haben eine eindeuige Zerlegung in Primideale.
- Primideale erster Ordnung von $\mathfrak{O}_{\mathbb{Q}(\theta)}$ können im Computer repräsentiert werden.

Eigenschaften von $\mathfrak{O}_{\mathbb{Q}(\theta)}$

Sei θ ein algebrischer Integer

- $\mathbb{Z}[\theta] \subset \mathfrak{O}_{\mathbb{Q}(\theta)} \subset \mathbb{Q}(\theta)$
- $\mathfrak{O}_{\mathbb{Q}(\theta)}$ ist ein Dedekindring. Ideale in $\mathfrak{O}_{\mathbb{Q}(\theta)}$ haben eine eindeuige Zerlegung in Primideale.
- Primideale erster Ordnung von $\mathfrak{O}_{\mathbb{Q}(\theta)}$ können im Computer repräsentiert werden.
- Es gibt ein Äquivalent zum Legendresymbol auf den Idealen von $\mathfrak{O}_{\mathbb{Q}(\theta)}$.

Quadrate in $\mathfrak{O}_{\mathbb{Q}(\theta)}$ mit Hauptidealen erkennen

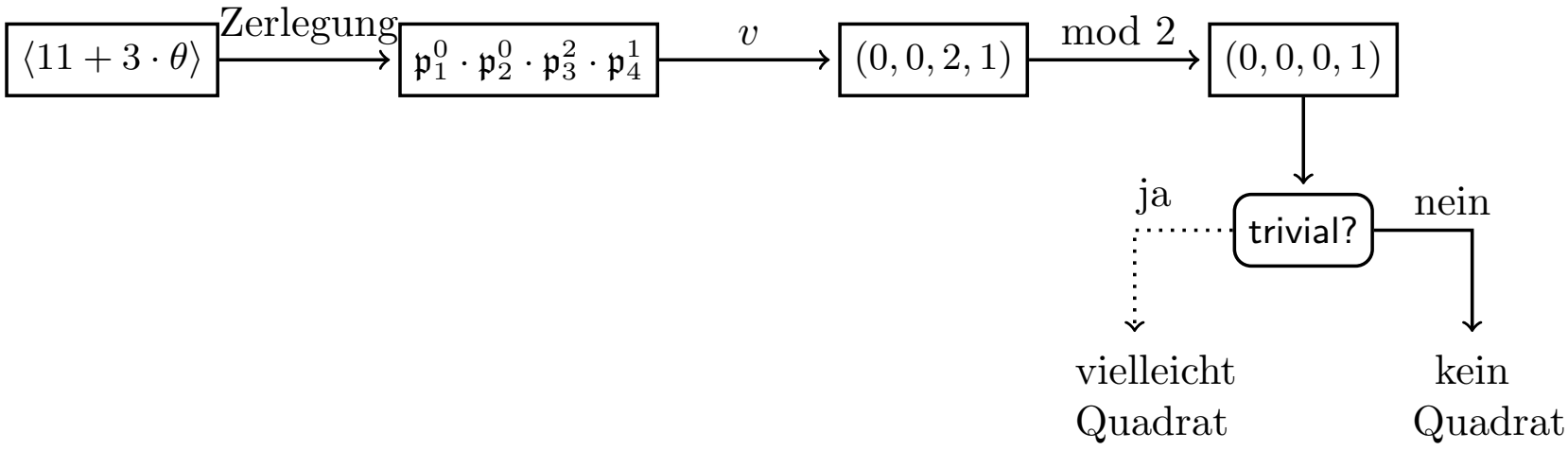
γ ist ein Quadrat in $\mathbb{Z}[\theta]$

$\Rightarrow$ γ ist ein Quadrat in $\mathfrak{O}_{\mathbb{Q}(\theta)}$

$\Rightarrow$ $\langle\gamma\rangle$ ist ein Quadrat von Idealen in $\mathfrak{O}_{\mathbb{Q}(\theta)}$

$\Rightarrow$ In der eindeutigen Primidealzerlegung von $\langle\gamma\rangle$ kommt jeder Faktor doppelt vor

Ideale von $\mathfrak{O}_{\mathbb{Q}(\theta)}$ als Quadrate erkennen



Quadrate in $\mathbb{Z}$ erkennen mit Legendresymbolen

$$
\begin{aligned}
& a \text{ ist ein Quadrat in } \mathbb{Z} \\
\Rightarrow \quad & a \text{ ist ein Quadrat in } \mathbb{Z}_p \quad \forall p \in \mathbb{P} \\
\Rightarrow \quad & \left(\frac{a}{p}\right) = 1
\end{aligned}
$$

Example

Ist 46 eine Quadratzahl? Wir testen für verschiedene Primzahlen:
$\left(\frac{46}{2}\right) = 1$;

Quadrate in $\mathbb{Z}$ erkennen mit Legendresymbolen

$$
\begin{aligned}
& a \text{ ist ein Quadrat in } \mathbb{Z} \\
\Rightarrow \quad & a \text{ ist ein Quadrat in } \mathbb{Z}_p \quad \forall p \in \mathbb{P} \\
\Rightarrow \quad & \left(\frac{a}{p}\right) = 1
\end{aligned}
$$

Example

Ist 46 eine Quadratzahl? Wir testen für verschiedene Primzahlen:
$\left(\frac{46}{2}\right) = 1$; $\left(\frac{46}{3}\right) = 1$;

Quadrate in $\mathbb{Z}$ erkennen mit Legendresymbolen

$$
\begin{aligned}
& a \text{ ist ein Quadrat in } \mathbb{Z} \\
\Rightarrow \quad & a \text{ ist ein Quadrat in } \mathbb{Z}_p \quad \forall p \in \mathbb{P} \\
\Rightarrow \quad & \left(\frac{a}{p}\right) = 1
\end{aligned}
$$

Example

Ist 46 eine Quadratzahl? Wir testen für verschiedene Primzahlen:
$\left(\frac{46}{2}\right) = 1$; $\left(\frac{46}{3}\right) = 1$; $\left(\frac{46}{5}\right) = 1$;

Quadrate in $\mathbb{Z}$ erkennen mit Legendresymbolen

$$
\begin{aligned}
& a \text{ ist ein Quadrat in } \mathbb{Z} \\
\Rightarrow \quad & a \text{ ist ein Quadrat in } \mathbb{Z}_p \quad \forall p \in \mathbb{P} \\
\Rightarrow \quad & \left(\frac{a}{p}\right) = 1
\end{aligned}
$$

Example

Ist 46 eine Quadratzahl? Wir testen für verschiedene Primzahlen:
$\left(\frac{46}{2}\right) = 1$; $\left(\frac{46}{3}\right) = 1$; $\left(\frac{46}{5}\right) = 1$; $\left(\frac{46}{7}\right) = 1$;

Quadrate in $\mathbb{Z}$ erkennen mit Legendresymbolen

$$
\begin{aligned}
& a \text{ ist ein Quadrat in } \mathbb{Z} \\
\Rightarrow \quad & a \text{ ist ein Quadrat in } \mathbb{Z}_p \quad \forall p \in \mathbb{P} \\
\Rightarrow \quad & \left(\frac{a}{p}\right) = 1
\end{aligned}
$$

Example

Ist 46 eine Quadratzahl? Wir testen für verschiedene Primzahlen:
$\left(\frac{46}{2}\right) = 1$; $\left(\frac{46}{3}\right) = 1$; $\left(\frac{46}{5}\right) = 1$; $\left(\frac{46}{7}\right) = 1$; $\left(\frac{46}{11}\right) = -1$

Zusammenfassung: Quadrate konstruieren in $\mathbb{Z}[\theta]$

Ist $\gamma \in \mathbb{Z}[x]$ ein Quadrat, dann

- lässt sich $\langle\gamma\rangle \in \mathfrak{O}_{\mathbb{Q}(\theta)}$ in Paare von Primidealen zerteilen.
- ist $\left(\frac{\gamma}{\mathfrak{p}}\right) = 1$ für alle Primideale $\mathfrak{p}$ von $\mathfrak{O}_{\mathbb{Q}(\theta)}$

Wie zuvor werden jedem Kandidaten s binäre Vektoren zugeordnet. Eine linear abhängige Menge dieser Vektoren deutet auf ein Quadrat hin.

Funktioniert die Implementierung?

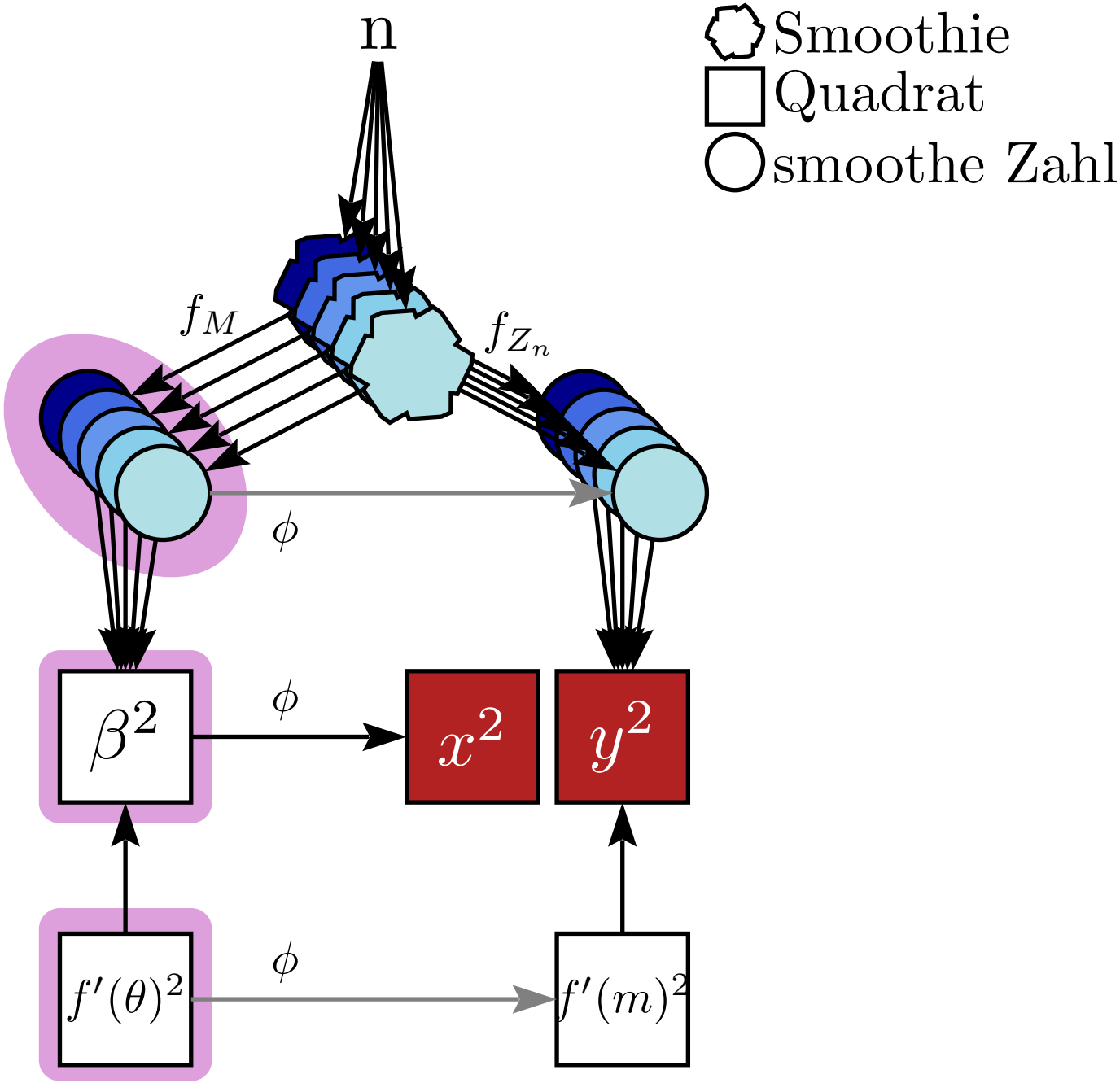
Mit den voreingestellten Parametern findet man kleine Faktoren relativ zuverlässig, große Faktoren relativ zuverlässig nicht.

Das waren die Grundlagen. Worauf soll ich näher eingehen?

- Teilmengen der Smoothiemenge S finden, die ein Quadrat ergeben.
- Wurzeln ziehen in $\frac{\mathbb{Z}[x]}{\langle f \rangle}$
- Das dunkle Geheimnis von $\mathfrak{O}_{\mathbb{Q}(\theta)}$
- Nullstellen von Polynomen in $\mathbb{Z}_p[x]$
- Beispielhafter Verlauf des Zahlkörpersiebes
- Etwas anderes?

Zusatzmaterial

Das dunkle Geheimnis des Zahlkörpersiebes



Nullstellen von Polynomen in $\mathbb{Z}_p[x]$

Wir suchen die Nullstellen von $f \in \mathbb{Z}_p[x]$.

Nullstellen von Polynomen in $\mathbb{Z}_p[x]$

Wir suchen die Nullstellen von $f \in \mathbb{Z}_p[x]$.

$$f(x) = \underbrace{(x-n_1)^{e_1} \cdot (x-n_2)^{e_2} \cdot \ldots \cdot (x-n_k)^{e_k}}_{\text{Linearfaktoren}} \cdot \underbrace{f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_l(x)}_{\text{irreduzible Anteile}} \cdot a$$

Nullstellen von Polynomen in $\mathbb{Z}_p[x]$

Wir suchen die Nullstellen von $f \in \mathbb{Z}_p[x]$.

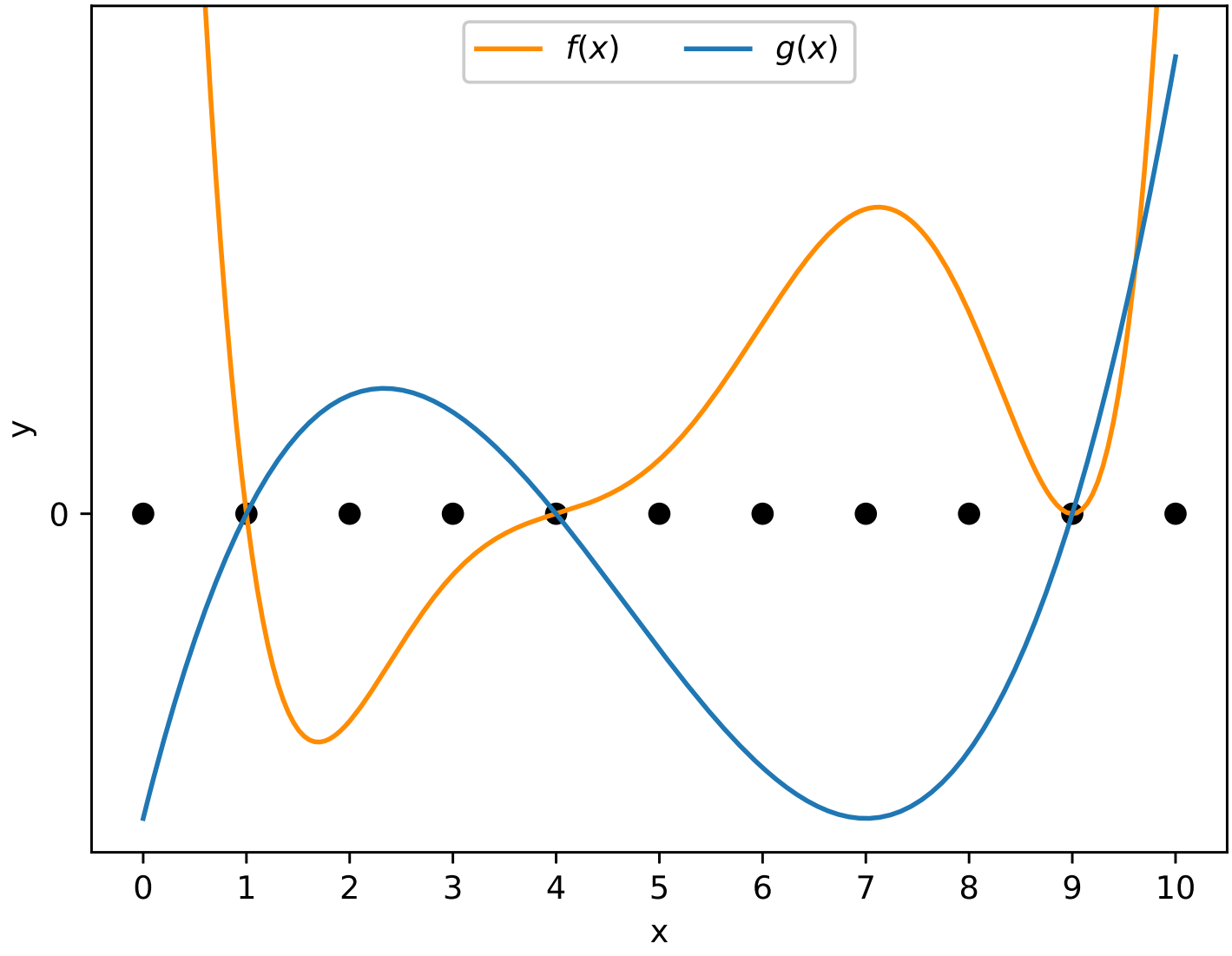
$$f(x) = \underbrace{(x-n_1)^{e_1} \cdot (x-n_2)^{e_2} \cdot \ldots \cdot (x-n_k)^{e_k}}_{\text{Linearfaktoren}} \cdot \underbrace{f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_l(x)}_{\text{irreduzieble Anteile}} \cdot a$$

In $\mathbb{Z}_p$ gilt

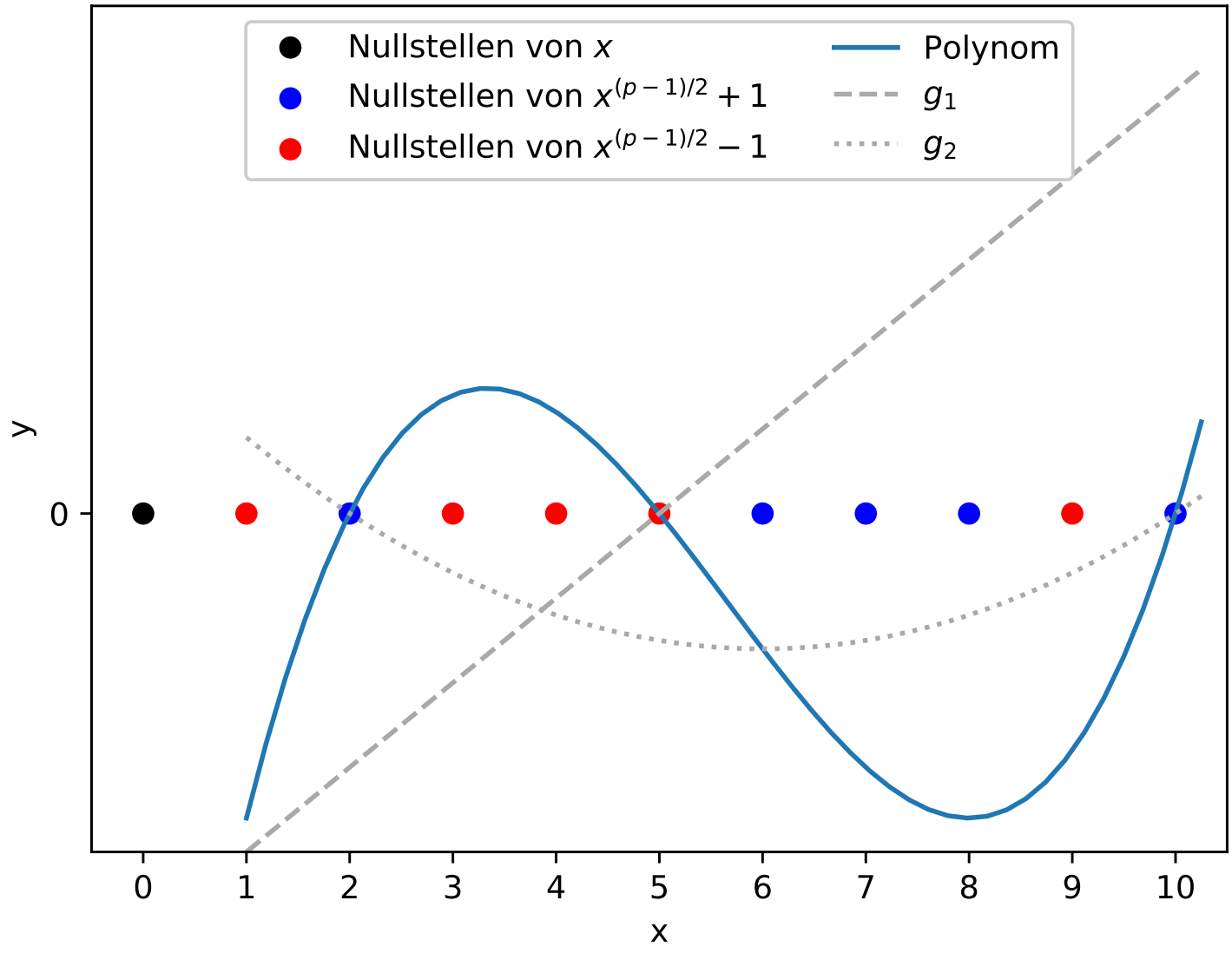
$$x^p - x = \prod_{i=0}^{p-1} (x-i)$$

Um die Nullstellen von f zu finden, genügt es deshalb $\gcd(f, x^p - x)$ zu betrachten.

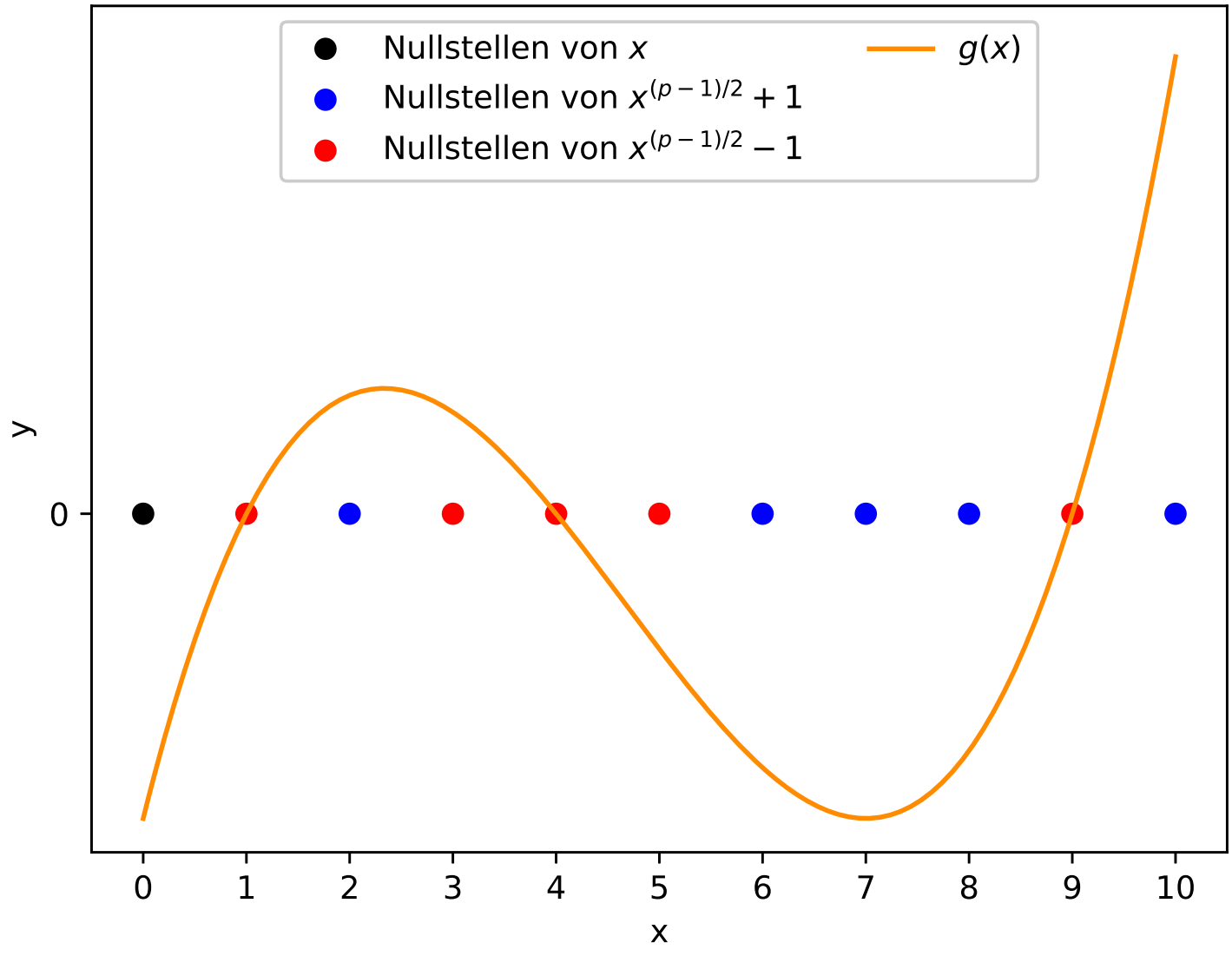
Unnötige Faktoren herausdividieren



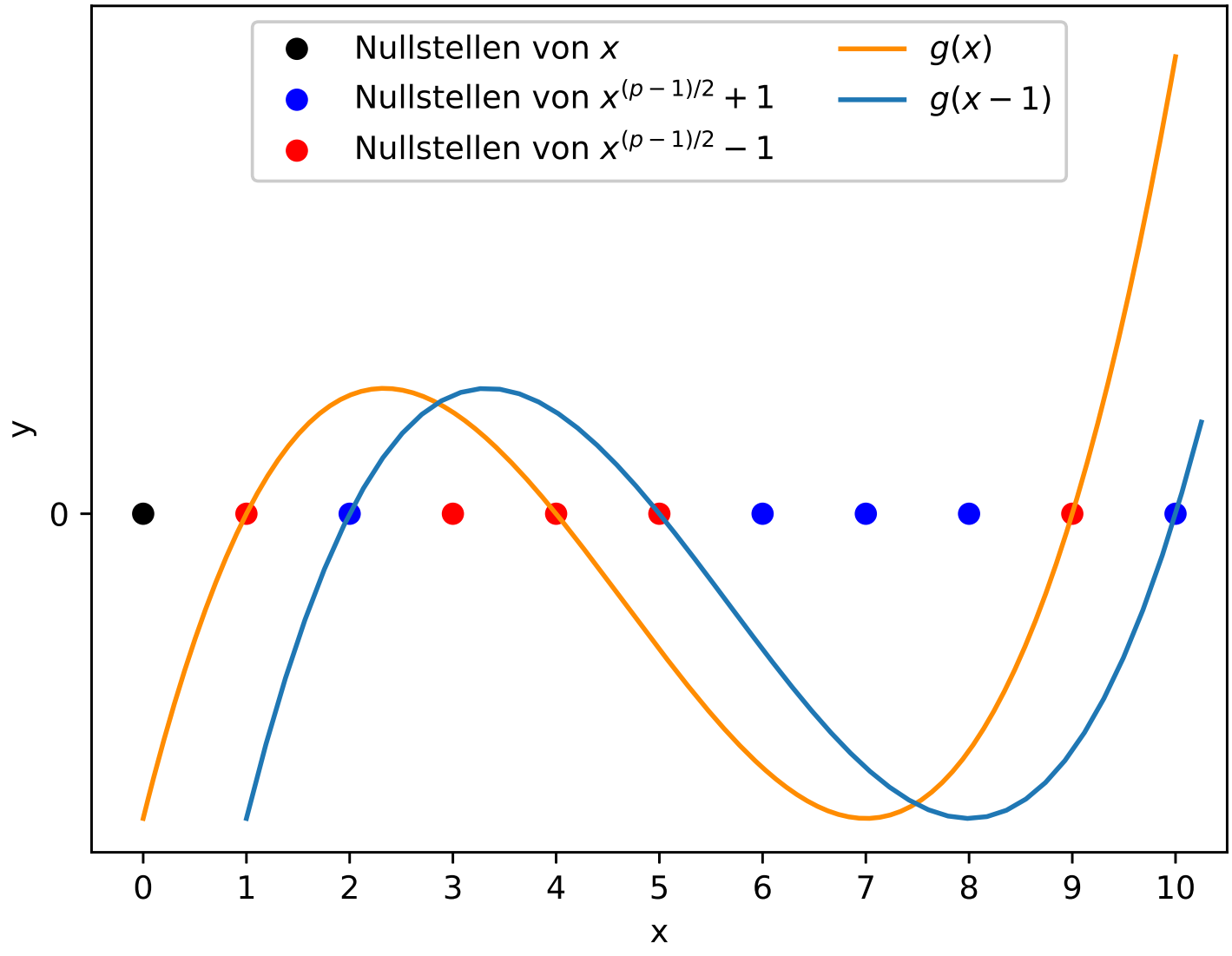
Polynom splitten



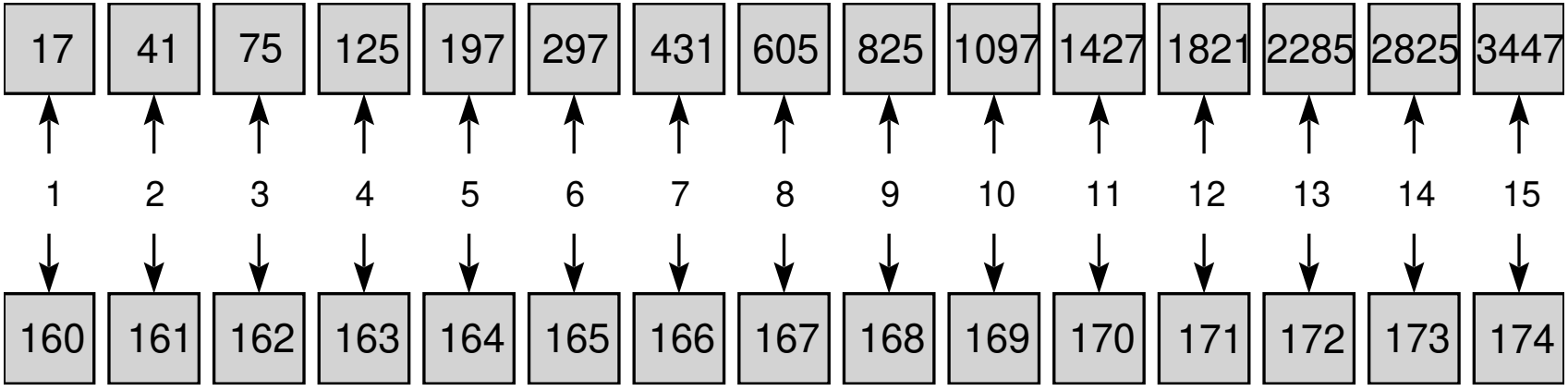
Polynom kann nicht gesplittet werden



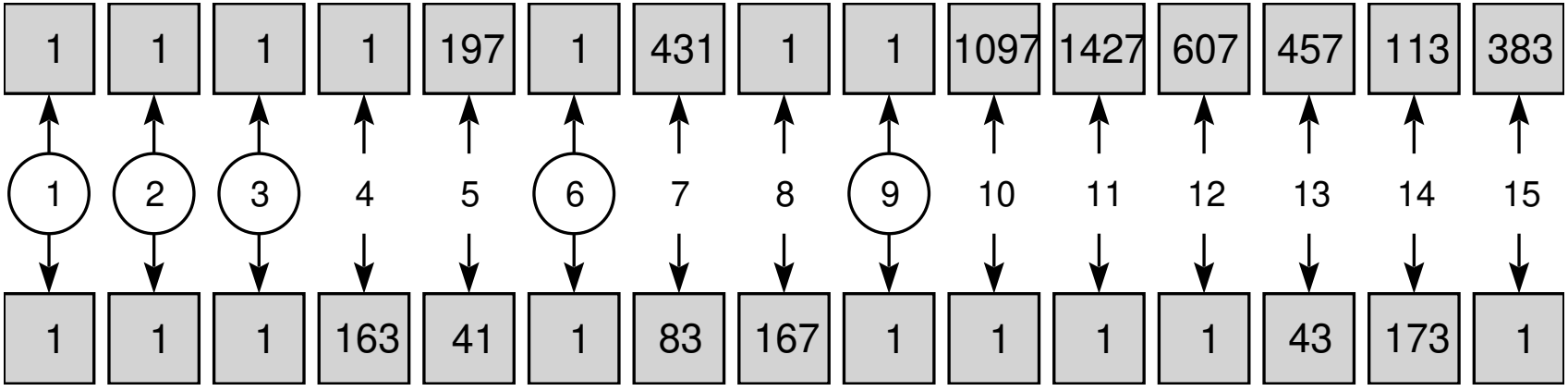
Polynom wird verschoben, um gesplittet zu werden



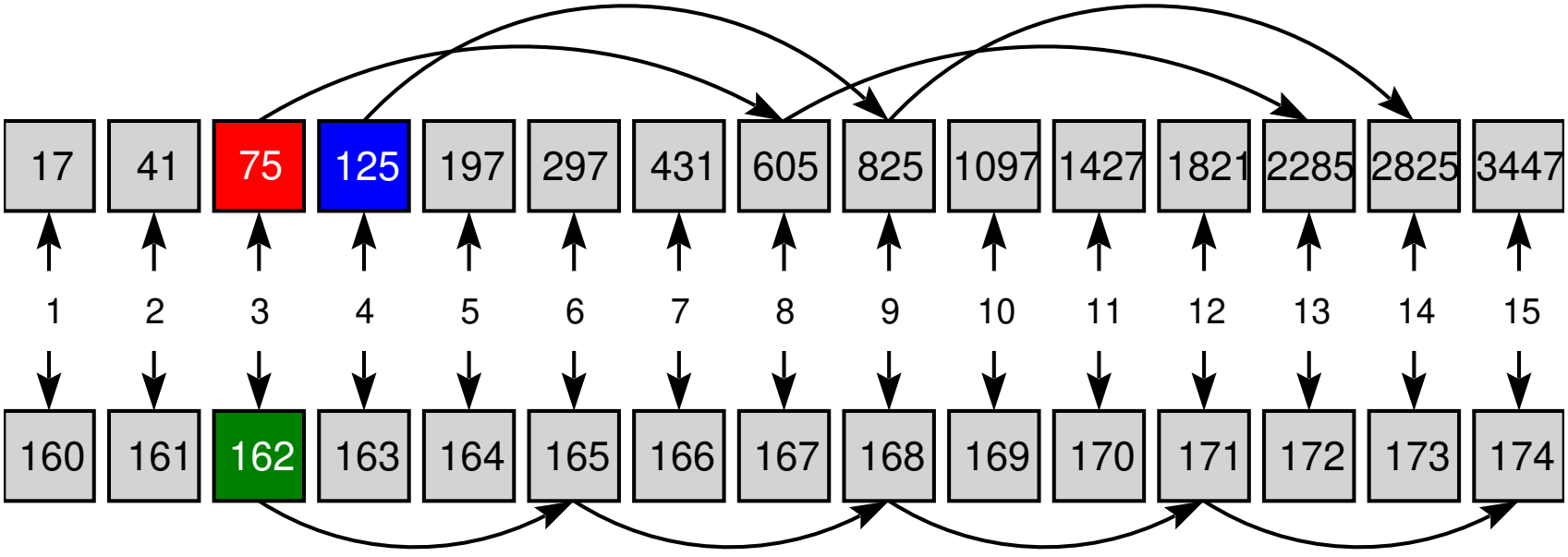
GNFS: Sieben


17 41 75 125 197 297 431 605 825 1097 1427 1821 2285 2825 3447
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
160 161 162 163 164 165 166 167 168 169 170 171 172 173 174

GNFS: Sieben


1 1 1 1 197 1 431 1 1 1097 1427 607 457 113 383
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
1 1 1 163 41 1 83 167 1 1 1 1 43 173 1

GNFS: Sieben


17 41 75 125 197 297 431 605 825 1097 1427 1821 2285 2825 3447
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
160 161 162 163 164 165 166 167 168 169 170 171 172 173 174