Seminar 6:
Polynomarithmetik: Faktorisierung

Präsentation erstellt von Stefan Hasenbanck
als Informatikseminar an der FH-Wedel
gehalten am 06.12.2007

Themenübersicht

- Der erweiterte Euklidische Algorithmus
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen

- **Der erweiterte euklidische Algorithmus**
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- Weg
- Resümee

Der erweiterte euklidische Algorithmus

- **Der erweiterte euklidische Algorithmus**
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen
- **Problem**
- Ziel
- Weg
- Resümee

Beispiel:

$(x-2) * (x-6)^2 * 4 = 4x^3-56x^2+240x-288$

$(x-2) * (x+3)*(x-7)^2 = x^4-13x^3+29x^2+133x-294$

Wenn wir nun die Formel $\frac{4x^3-56x^2+240x-288}{x^4-13x^3+29x^2+133x-294}$ haben so fragen wir uns sicherlich, ob man diese einfacher darstellen kann.

Wir wissen, dass Zähler und Nenner (x-2) enthalten und unter der Annahme, dass $x \neq 2$können wir den Bruch kürzen auf $\frac{4x^2-48x+144}{x^3-11x^2+7x+147}$

Nun ist die allgemeine Frage: wie bekommt man den größten gemeinsamen Teiler (ggT(x,y) -> gcd(x,y) im Englischen) von zwei beliebigen Polynomen?

- **Der erweiterte euklidische Algorithmus**
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- **Ziel**
- Weg
- Resümee

Mit dem euklidischen Algorithmus (der aus der Vorlesung GTI bekannt ist) den größten gemeinsamen Teiler (ggT) zweier Polynome zu finden.

Dabei gilt als Grundlage $a(x) = q(x)b(x)+r(x)$

```
ggT(a, b)
{
   /*if (a = 0 .....  alle Möglichkeiten mit 0 abfangen*/
   if (a mod b = 0) return b;
   /*else*/
   return ggT(b, a mod b);
}
```

- **Der erweiterte euklidische Algorithmus**
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Da wir die Division mit Rest auch für Polynome beherrschen und der eigentliche Algorithmus identisch ist, kann man sofort losrechnen.

Beispiel mit den Polynomen, vom Anfang:

$(4x^3-56x^2+240x-288) / (x^4-13x^3+29x^2+133x-294) = 0$ Rest $(4x^3-56x^2+240x-288)$

$(x^4-13x^3+29x^2+133x-294) / (4x^3-56x^2+240x-288) = ¼\,x + ¼$ Rest $-17x^2 + 145x - 222$

$$
\begin{array}{l}
x^4 - 14x^3 + 60x^2 - 72x \\
\hline
\quad X^3 - 31x^2 + 205x - 294 \\
\quad X^3 - 14x^2 + 60x - 72 \\
\hline
\quad\quad -17x^2 + 145x - 222
\end{array}
$$

- **Der erweiterte euklidische Algorithmus**
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

$$(x^4 - 13x^3 + 29x^2 + 133x - 294)/(4x^3 - 56x^2 + 240x - 288) = \frac{1}{4}x + \frac{1}{4} \quad \text{Rest} = -17x^2 + 145x - 222$$

$$(4x^3 - 56x^2 + 240x - 288)/(-17x^2 + 145x - 222) = -\frac{4}{17}x + \frac{372}{289} \quad \text{Rest} = \frac{324}{289}x - \frac{648}{289}$$

$$(-17x^2 + 145x - 222)/(\frac{324}{289}x - \frac{648}{289}) = -\frac{4913}{324}x + \frac{10693}{108} \quad \text{Rest} = 0$$

=> ggT($4x^3-56x^2+240x-288$, $x^4-13x^3+29x^2+133x-294$) = $\frac{324}{289}x - \frac{648}{289}$

ggT($(x-2)*(x-6)^2*4$, $(x-2)*(x+3)*(x-7)^2$) = $\frac{324}{289}x - \frac{648}{289}$

- **Der erweiterte euklidische Algorithmus**
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

ggT((x-2)*(x-6)²*4 , (x-2)*(x+3)*(x-7)²) = $\frac{324}{289}x - \frac{648}{289}$

Leider liefert der erweiterte euklidische Algorithmus für Polynome ein Ergebnis, welches bis auf einen konstanten Faktor eindeutig ist.

$$\frac{324}{289}(x-2) = \frac{324}{289}x - \frac{648}{289}$$

Ein eindeutigen ggT erhalten wir durch Normierung.

Für die Polynomdivision mit Rest empfehle ich:
„http://www.arndt-bruenner.de/mathe/scripts/polynomdivision.htm“
da sie alle Zwischenergebnissen darstellt.

- **Der erweiterte euklidische Algorithmus**
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Wenn man schreibt: ggT(f(x), g(x)) = 1 meint man, dass die Polynome keinen gemeinsamen nicht trivialen Teiler haben – unter trivialen Teilern versteht man an dieser Stelle konstante Teiler.

Da wir den euklidischen Algorithmus für Polynome anwenden können, ist ersichtlich, dass auch der erweiterte euklidische Algorithmus zur Ermittlung der Bézoutkoeffizienten funktioniert.

Die Bézoutkoeffizienten sind gegeben durch (vollständiges Beispiel in der Ausarbeitung):

$$(x-2) = (-\frac{17}{324}x^2 + \frac{19}{81}x + \frac{191}{162}) * (4x^3 - 56x^2 + 240x - 288) - (-\frac{17}{81}x + \frac{31}{27}) * (x^4 - 13x^3 + 29x^2 + 133x - 294)$$

Das Ermitteln des ggT bei mehreren Polynomen funktioniert genauso wie bei das Ermitteln des ggT bei mehreren ganzen Zahlen.

- **Der erweiterte euklidische Algorithmus**
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- Weg
- **Resümee**

Der euklidische Algorithmus ist schneller als die vollständige Faktorisierung, wenn es darum geht, alle gemeinsamen Teiler von zwei Polynomen zu finden.

Problem: intermediate expression swell

$$(-17x^2 + 145x - 222)/(\frac{324}{289}x - \frac{648}{289}) = -\frac{4913}{324}x + \frac{10693}{108}\text{Rest} = 0$$

Unter der Problemklasse des „expression swells“ versteht man alle Probleme, bei denen die Länge der Zahl(en) stark anwächst.
Dieses kann zu Speicherproblemen führen und wie in dem Seminar *„Langzahlarithmetik: Addition und Multiplikation“* zu sehen ist, ist die Komplexität der Berechnung auch abhängig von der Länge der Zahl.

Da der ggT normiert wird, handelt es sich hier um ein Teil-Problem, welches man als „intermediate expression swell“ bezeichnet -> sprich die Werte wachsen nur während der Berechnung stark an.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- Weg
- Resümee

Eindeutige Faktorzerlegung

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- **Problem**
- Ziel
- Weg
- Resümee

Beispiel:

$(x-2) * (x-6)^2 * 4 = 4x^3-56x^2+240x-288$

$(x-2) * (x+3)*(x-7)^2 = x^4-13x^3+29x^2+133x-294$

Wir haben $x^4-13x^3+29x^2+133x-294$ und wollen wissen, welche Nullstellen das Polynom hat und ob es sich um einfache oder um vielfache Nullstellen handelt.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- **Ziel**
- Weg
- Resümee

Wir wollen nun ein beliebiges Polynom zerlegen und alle irreduziblen Teilpolynome zu bekommen.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Einfachste Idee:
Wir probieren einfach alle möglichen Polynome als Teiler.

Problem: es sind unendlich viele!!!

Nun müssen wir überlegen, wie wir die Anzahl der möglichen Polynome (Kandidatenpolynome) beschränken.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Zuerst kann man ähnlich wie bei ganzen Zahlen annehmen, dass man nur irreduzible Teiler ausprobieren muss, welche kleiner gleich der Wurzel des zu untersuchenden Polynoms sind.

Die Wurzel eines Polynoms mit dem Grad n, ist hierbei ein Polynom mit dem Grad n/2.

$$\sqrt{(x^n)} = (x^n)^{\frac{1}{2}} = x^{n*\frac{1}{2}} = x^{\frac{n}{2}}$$

Des weiteren kann man annehmen, dass es maximal einen irreduziblen Teiler gibt, dessen Grad größer ist als n/2.

Dieses ergibt sich, daraus, dass $x^n * x^m = x^{n+m}$ ist.

Man sieht, gäbe es zwei irreduzible Teiler mit einem Grad größer als n/2, so müsste der Grad des Polynoms größer als n sein.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Leider sind die möglichen Koeffizienten immer noch unendlich viel.

1. Ansatz: Beschränkung der Polynome indem man eine Restklasse ($\mathbb{Z}_p$)betrachtet.

Wie man in dem Seminar „*Vorstellung des Computer-Algebra-Systems Mathematica*“ an einen Beispiel gesehen hat kommen für $\mathbb{Z}_p$ andere Teiler als für $\mathbb{Z}$ heraus.

Ein kurzes Beispiel wieso dieses so ist:
$(x + 3)^2 = x^2 + 6x + 9$
$(x + 3)^2$ in $\mathbb{Z}_6 = x^2 + 0x + 3 = x^2 + 3$

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Um nun die Teiler herauszufinden, muss man alle Kandidatenpolynome zuerst erfassen.
Beispiel für $(x + 3)^2$ in $\mathbb{Z}_7$:

1, 2, 3, 4, 5, 6,
x, 2x, 3x, 4x, 5x, 6x,
x+1, x+2, x+3, x+4, x+5, x+6,
2x+1, 2x+2, 2x+3, 2x+4, 2x+5, 2x+6,
...
6x+1, 6x+2, 6x+3, 6x+4, 6x+5, 6x+6

Nun enthält diese Menge viele doppelte Kandidatenpolynome, denn man sieht, dass
x und 2x und ...
x+1 und 2x+2 und ...
bis auf einen Faktor identisch sind.

Zudem kann es noch weiter Elemente in der Liste geben, die per Multiplikation durch andere Elementen erzeugt werden können.
Bevor man jedoch solche Elemente sucht, würde man einfach ausprobieren.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Alle übriggebliebenen kann man nun testen und erhält dann alle Teiler des zu untersuchenden Polynoms (wenn man mit den kleinsten Elementen beginnt werden die erzeugbaren Elemente auch ausgeschlossen).

Man stellt sofort zwei Sachverhalte fest:
1. Es ist ein enorm aufwendiges Verfahren
2. Es funktioniert nur in jeweiligen Restklassen und ist somit je nach Problem nicht immer geeignet

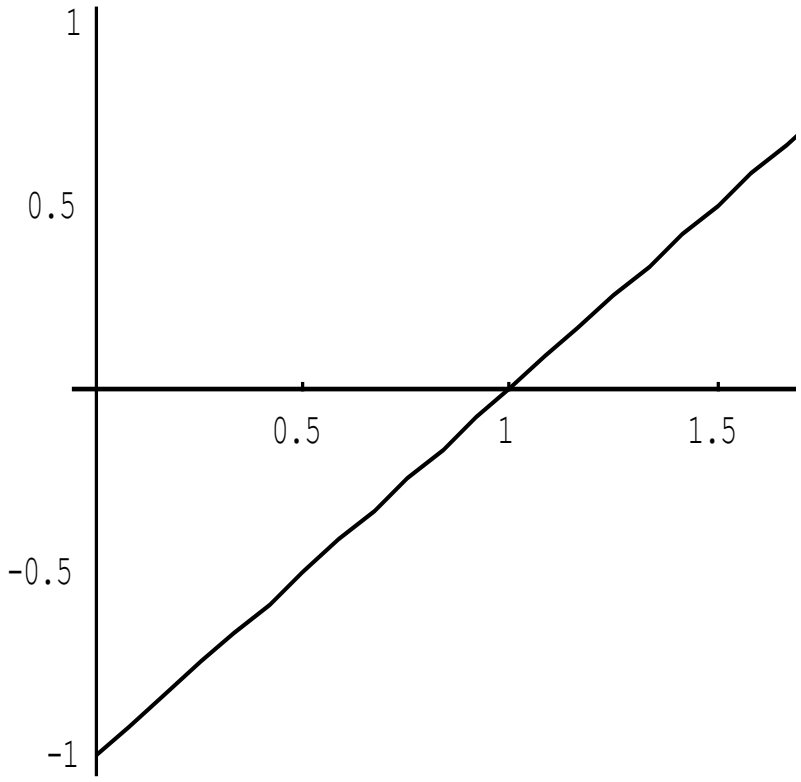
- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

2. Ansatz: Untersuchung von Eigenschaften der Polynome (in $\mathbb{Z}$) und mögliche Rückschlüsse (Grundlagen von dem Kronecker Algorithmus)

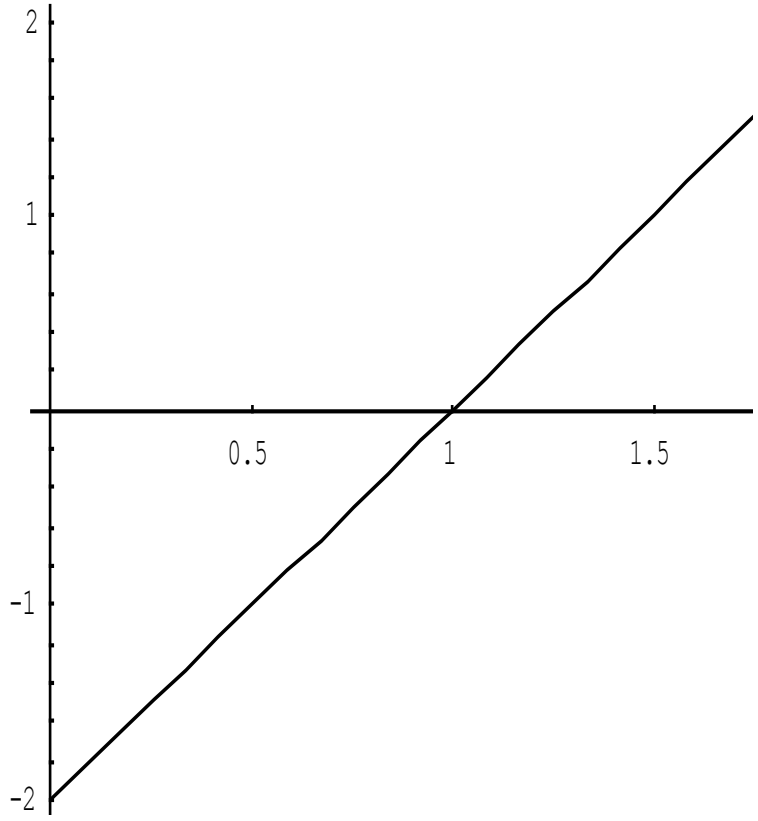
Wenn man ein Polynom mit einem Faktor multipliziert, so verändert sich der Graf in der Form, dass jeder Abstand zur x-Achse mit dem Faktor multipliziert wird.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

(x-1)



2*(x-1)

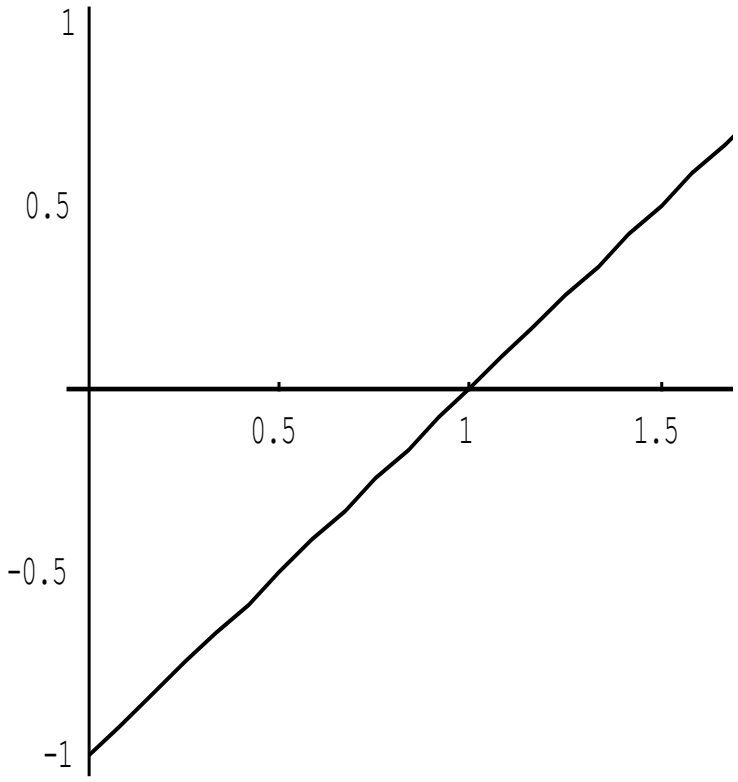


- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

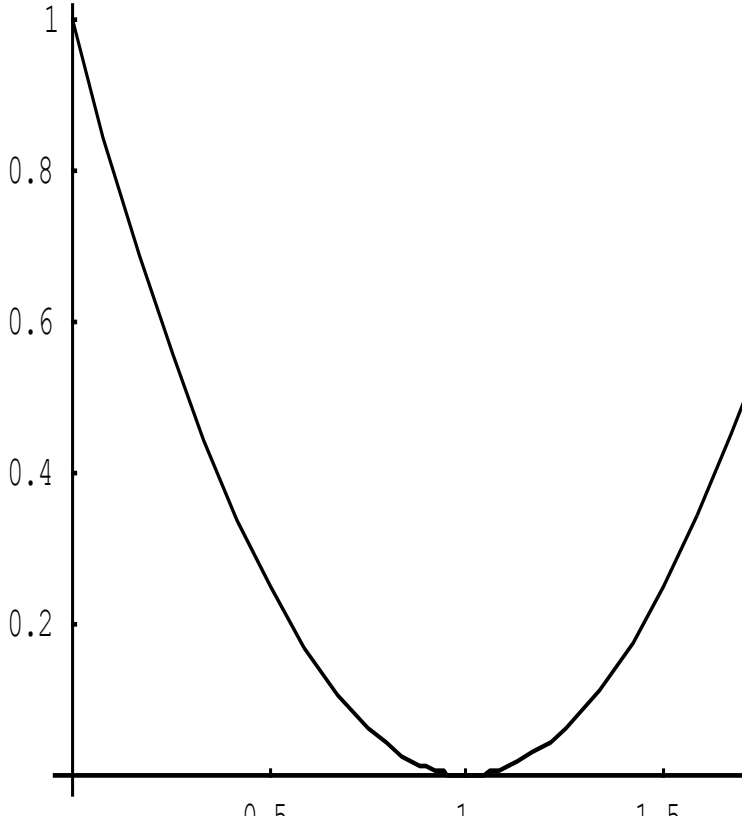
Wenn man ein Polynom mit einem anderen Polynom multipliziert, wird der Abstand zwischen Graf(Polynom1) und x-Achse mit dem Abstand zur x-Achse von Graf(Polynom2) multipliziert.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

(x-1)



(x-1)*(x-1)



- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Wenn man nun ein Polynom so ändert, dass es für jedes ganzzahliges x eine ganze Zahl liefert, dann muss jedes Kandidatenpolynom an dieser Stelle einen Teiler der ganzen Zahl liefern.

$$b(x) \mid a(x) \rightarrow b(x_i) \mid a(x_i) \quad \forall i \in \mathbb{Z}$$

Des weiteren wissen wir (spätestens) seit dem letzten Seminar, dass ein Polynom eindeutig bestimmt werden kann, wenn es vom Grad n ist und man mindestens n+1 Wertepaare (x,f(x)) kennt.

Das bedeutet mit n/2+1 Werten des zu untersuchenden Polynoms, kann man alle Kandidatenpolynome ermitteln mit einem Grad <= n/2.
Da es nur ein Polynom mit dem Grad > n/2 geben kann, finden wir es, indem wir die Kandidatenpolynome von dem zu untersuchenden Polynom dividieren.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Indem man dieses Wissen verwendet, kann man die Menge der Kandidatenpolynome auch in $\mathbb{Z}$ auf eine endliche Menge einschränken.

Kronecker Algorithmus:

1. Schritt: Umwandeln eines Polynoms in ein Polynom, welches ganzzahlige Werte liefert.

Man multipliziert es mit einem Faktor
Beispiel:
$1/7x^4-13/7x^3+29/7x^2+19x-42 * 7 = x^4-13x^3+29x^2+133x-294$

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

2. Schritt: Nun setzen wir (n/2+1) mal beliebige ganzzahlige x ein und notieren das Ergebnis.
Beispiel:
Wir haben ein Polynom des Grades 4, also müssen wir 3 x-Werte einsetzen.
{(6,36), (3,96) , (5,96)}

3. Schritt: Nun müssen wir Polynome ermitteln die Kandidatenpolynome sind.
Dafür müssen wir erst ermitteln, welche Zahlen die ermittelten Werte ohne Rest Teilen.
36 = 1,2,3,4,6,9,12,18,36
96 = 1,2,3,4,6,8,12,16,24,32,48,96
96 = 1,2,3,4,6,8,12,16,24,32,48,96

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

4 Schritt: Nun bildet man alle möglichen Wertekombinationen und ermittelt für alle Wertekombinationen das eindeutige Polynom per Interpolation:

(6)	(3)	(5)	Kandidatenpolynom
1	1	1	1
1	1	2	1+1/2*(3-x)*(-6+x)
...	...	...	...
36	96	96	36+(-20 (-20 *(-3+x))) *(-6+x)

9*12*12=**1296**

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

5. Schritt: Nun testen man wieder, ob ein Kandidatenpolynom das zu untersuchende Polynom ohne Rest teilt und wie häufig es dieses macht.
Wenn das Polynom während der Berechnung 1 wird, ist man fertig.
Wenn man alle Kandidatenpolynome durchprobiert hat und das Polynom nicht 1 geworden ist, dann steht fest, dass das Polynom, welches man überbehält genau das eine Teil-Polynom ist, welches einen Grad über n/2 hat.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Es gilt zu beachten beim Kronecker Algorithmus:

- Man kann den größten gemeinsamen Teiler aller Koeffizienten ausklammern, um unnötige Teiler zu vermeiden

- Wenn a(0) = 0 dann kann mindestens ein x ausgeklammert werden, dieses kann die Anzahl der Werte verringern, die zur Berechnung einer Interpolation benötigt werden.

- Bei der Wahl der x_i sollte man versuchen, Zahlen mit wenigen Teilern zu finden. Bei $a(x_i) = 0$ kann man $(x-x_i)$ aus a(x) ausklammern. Allerdings darf man die 0 als ermittelten Wert nicht zulassen, da alle Zahlen ein Teiler von 0 sind.

- Der erweiterte euklidische Algorithmus
- **Eindeutige Faktorzerlegung**
- Quadratfreie Faktorisierung
- Rationale Funktionen
- Problem
- Ziel
- Weg
- **Resümee**

Nun kann man Polynome in $\mathbb{Z}$ und Polynome in $\mathbb{Z}_p$ in ihre irreduziblen Teiler zerlegen.

Allerdings sind beide Algorithmen sehr aufwändig und daher nur begrenzt zu verwenden.

Es gibt bessere Algorithmen.
Mindestens einer wird in den kommenden Seminaren vorgestellt.

Und es gibt Möglichkeiten, vor der Faktorisierung ein Polynom so zu bearbeiten, dass manchmal die hier vorgestellten Algorithmen ausreichen.

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- Weg
- Resümee

Quadratfreie Faktorisierung

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- **Problem**
- Ziel
- Weg
- Resümee

Wir suchen die Faktorisierung eines Polynoms:

$(x-2)(x-5)(x+2)^2x^2(x-11)^2(x+17)^3 =$

$x^{11}+26x^{10}-235x^9-7982x^8+23055x^7+715422x^6-1840153x^5$

$-8680370x^4+7006516x^3+23778920x^2$

Dieses Polynom könnte man mit den bisher behandelten Mitteln lösen, jedoch wäre der Zeitaufwand in der Praxis zu groß.

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- **Ziel**
- Weg
- Resümee

Man will erreichen, dass man in bestimmten Fällen auch größere Polynome lösen kann.

Und man wäre glücklich, wenn man das Problem vereinfachen könnte, z.B. in der Form, dass man nicht $(x-2)(x-5)(x+2)^2x^2(x-11)^2(x+17)^3$ zerlegen muss, sondern nur drei Zerlegungen machen müsste und zwar von

$(x-2)(x-5)$ und
$(x+2)x(x-11)$ und
$(x+17)$

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Einen Weg bietet uns die Quadratfreie Faktorisierung, welche die eben gezeigte Zerlegung vornimmt.

Das bedeutet anstelle von einen großen Polynom bekommt man Polynome, deren Teilpolynome vorher den gleichen Exponenten hatten. Zudem erfahren wir gleichzeitig, um welchen Exponenten es sich gehandelt hat.

Hierfür muss man wieder zunächst die Eigenschaften von Polynomen betrachten und zwar im Hinblick auf eine Ableitung des Polynoms.

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Ableitungsregeln:

(Konstantenregel)
$f(x) = c \rightarrow f'(x) = 0$

(Potenzregel)
$f(x) = x^n \rightarrow f'(x) = n*x^{n-1}$

(Potenzregel)
$f(x) = (a(x))^n \rightarrow f'(x) = a(x)' * n * (a(x))^{n-1}$

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Ableitungsregeln:

(Produktregel)

$$f(x) = (a(x)*b(x)) \rightarrow f'(x) = a'(x)*b(x) + a(x)*b'(x)$$

(Produktregel)

$$f(x) = (a(x)*b(x)*c(x)) \rightarrow f'(x) = a'(x)*b(x)*c(x) + a(x)*b'(x)*c(x) + a(x)*b(x)*c'(x)$$

und so weiter …

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Nimmt man nun ein Beispiel Polynom:

$f(x) = (x-2) * (x+3)*x^2*(x-7)^2 *(x^2+11)^3$

$$
\begin{aligned}
f'(x) = \quad & 1 * (x+3)*x^2*(x-7)^2 *(x^2+11)^3 \\
& +(x-2) * 1*x^2*(x-7)^2 *(x^2+11)^3 \\
& +(x-2) * (x+3)*2x*(x-7)^2 *(x^2+11)^3 \\
& +(x-2) * (x+3)*x^2*2*(x-7) *(x^2+11)^3 \\
& +(x-2) * (x+3)*x^2*(x-7)^2 *2x*3*(x^2+11)^2
\end{aligned}
$$

$$
\begin{aligned}
f'(x) = \quad & x*(x-7)*(x^2+11)^2 * \\
& (\\
& \quad 1 * (x+3)*x*(x-7) *(x^2+11) \\
& +(x-2) * 1*x*(x-7) *(x^2+11) \\
& +(x-2) * (x+3)*2*(x-7) *(x^2+11) \\
& +(x-2) * (x+3)*x*2 *(x^2+11) \\
& +(x-2) * (x+3)*x*(x-7) *2x*3 \\
&)
\end{aligned}
$$

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

$f(x) = (x-2) * (x+3)*x^2*(x-7)^2 *(x^2+11)^3$

$f'(x) =$ $x*(x-7)*(x^2+11)^2 *$
(
$1 * (x+3)*x*(x-7) *(x^2+11)$
$+(x-2) * 1*x*(x-7) *(x^2+11)$
$+(x-2) * (x+3)*2*(x-7) *(x^2+11)$
$+(x-2) * (x+3)*x*2 *(x^2+11)$
$+(x-2) * (x+3)*x*(x-7) *2x*3$
)

Wenn man f(x) und f‘(x) vergleicht, sieht man, dass n-fache Nullstellen zu (n-1)-fachen Nullstellen geworden sind. Zudem gibt es keine weiteren Nullstellen, die mit den (n-1)-fachen Nullstellen zusammenfallen können.

ACHTUNG:
Wenn man nicht ein Polynom aus $\mathbb{Z}[x]$ sondern aus $\mathbb{Z}_p[x]$ hat, dann gilt für $(a(x))^p$
$f(x) = (a(x))^p$ -> $f'(x) = a(x)' * p * (a(x))^{p-1}$
da aber p mod p = 0 ist, gilt auch f’(x) = 0.
Da es einfacher ist betrachten wir hier nur Polynome aus $\mathbb{Z}[x]$!

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Nun kann man aus dem Wissen einen Algorithmus entwickeln.

1. Schritt
Man belegt eine Variable mit einem Polynom.

$f = (x-2) * (x+3)*x^2*(x-7)^2 *(x^2+11)^3$

2. Schritt
Man bildet die Ableitung und legt diese auf eine andere Variable.

$df = f' = x*(x-7)*(x^2+11)^2 *((x+3)*x*(x-7) *(x^2+11)+(x-2) * x*(x-7) *(x^2+11)+(x-2) * (x+3)*2*(x-7) *(x^2+11)+(x-2) * (x+3)*x*2 *(x^2+11)+(x-2) * (x+3)*x*(x-7) *2x*3)$

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

3. Schritt
Man bestimmt den größten gemeinsamen Teiler von dem Polynom und der Ableitung des Polynoms und speichert ihn zwischen.

ggTeiler = ggT(f, df) = $x*(x-7)*(x^2+11)^2$

4. Schritt
Man bestimmt den quadratfreien Teil von dem Polynom.

quadFrei = f / ggTeiler = $(x-2) * (x+3)*x*(x-7) *(x^2+11)$

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

5. Schritt
Man bestimmt nun ein Polynom, welches alle einfachen Nullstellen enthält.

polEinfacheNullstellen = quadFrei / ggT(quadFrei, ggTeiler) =

$$\frac{(x-2) * (x+3)*x*(x-7) *(x^2+11)}{x*(x-7)*(x^2+11)} = (x-2)*(x+3)$$

6. Schritt
Nun will man auch alle Polynome finden, welche mehrfache Nullstellen beinhalten.
$f = (x-2) * (x+3)*x^2*(x-7)^2 *(x^2+11)^3$
$ggTeiler = x*(x-7)*(x^2+11)^2$
Man kann sehen, dass man f = ggTeiler setzen kann und die Schritte nur wiederholen muss.

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- **Weg**
- Resümee

Beispiel:

$f = ggTeiler = x*(x-7)*(x^2+11)^2$
$df = f' = (x^2+11) * ((x-7)*(x^2+11) + x*(x^2+11) + x * (x-7) * 2x * 2)$
$ggTeiler = ggT(f, df) = (x^2+11)$
$quadFrei = f / ggTeiler = x*(x-7) *(x^2+11)$
$polZweifacheNullstellen = quadFrei / ggT(quadFrei, ggTeiler) = x*(x-7)$

$f = ggTeiler = (x^2+11)$
$df = f' = 2x$
$ggTeiler = ggT(f, df) = 1$
$quadFrei = f / ggTeiler = (x^2+11)$
$polDreifacheNullstellen = quadFrei / ggT(quadFrei, ggTeiler) = (x^2+11)$

$f = ggTeiler = 1$
$df = f' = 0$ -> Abbruch des Algorithmus

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- Weg
- **Resümee**

Es treten die bekannten Schwierigkeiten der Teilschritte auf (ggT – intermediate expression swell).

Funktioniert nur bei Polynomen aus $\mathbb{Z}[x]$.
Erweiterung auf $\mathbb{Z}_p[x]$ gibt es in einen späteren Seminar.

Wenn der Grad aller Nullstellen = 1 ist, gibt der Algorithmus keine Verbesserung, kostet jedoch Zeit.

Wenn der Grad der Nullstellen unterschiedlich ist oder > 1, erleichtert der Algorithmus die Faktorisierung immens.

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- **Quadratfreie Faktorisierung**
- Rationale Funktionen
- Problem
- Ziel
- Weg
- **Resümee**

Bei einem Polynom $(x-1)*(x-2)^{14}$ bekommen wir für die 2-fachen bis 13-fachen Nullstellen die Konstante 1.
So zu sagen die Zerlegung von $(x-1)*1^2*1^3*1^4*1^5*1^6*1^7*1^8*1^9*1^{10}*1^{11}*1^{12}*1^{13}*(x-2)^{14}$.

Hinweis:
Die Quadratfreie Faktorisierung kann auch bei der Integration verwendet werden, leider fällt dieser Vortrag aus.

Es gibt eine Verbesserung von diesem Algorithmus welche von Yun entwickelt wurde, welcher vor allem auf Verbesserung der Komplexität des ggT ausgerichtet ist.

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- **Rationale Funktionen**
- Grundlagen
- Resümee

Rationale Funktionen

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- **Rationale Funktionen**
- **Grundlagen**
- Resümee

Wie wir im Seminar „*Langzahlarithmetik: Vereinfachen von Brüchen*“ gesehen haben, liegen Brüche nach der Addition/Subtraktion oder Multiplikation/Division zweier Brüche nicht zwingend in einer gekürzten Form vor.
Daher kann man nach solchen Operationen den ggT auf den Nenner und Zähler anwenden. Das Ergebnis kann man benutzen, um Nenner und Zähler zu kürzen.

Das gleiche gilt für Funktionen.

Beispiel: $\frac{x^3 - 2x^2 - 5x + 6}{x - 1} = x^2 - x - 6$

Wobei wir x^2-x-6 als Standarddarstellung bezeichnen.

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- **Rationale Funktionen**
- Grundlagen
- **Resümee**

Wenn wir die Standarddarstellung wählen, so können Informationen verloren gehen, denn es wird eine hebbare Lücke entfernt.

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen

Gesamt Resümee

Wir suchen die Faktorisierung eines Polynoms:

$x^{11}+26x^{10}-235x^9-7982x^8+23055x^7+715422x^6-1840153x^5$
$-8680370x^4+7006516x^3+23778920x^2$

$=(x-2)(x-5)(x+2)^2x^2(x-11)^2(x+17)^3$

Man kann einiges verbessern an den Algorithmen und es gibt auch Bessere,

ABER wir haben Algorithmen und müssen sie uns nicht selbst ausdenken!!!

- Der erweiterte euklidische Algorithmus
- Eindeutige Faktorzerlegung
- Quadratfreie Faktorisierung
- Rationale Funktionen

Vielen Dank für eure Aufmerksamkeit