Secret Sharing

P. Amrein, A. Lägeler, M. Schwagenscheidt

ETH Zürich D-MATH / Ubique Innovations AG

ETH Studienwoche 2022

8. Juni 2022

Ein geheimes Projekt

Problem: Drei Wissenschaftler*innen arbeiten an einem geheimen Projekt. Die Dokumente dazu legen sie in einem Tresor, den sie mit Vorhängeschlössern verschliessen. Sie möchten den Tresor nur dann öffnen können, wenn mindestens zwei der drei Wissenschaftler*innen zugegen sind. Wie viele Schlösser brauchen sie mindestens dafür und wie viele Schlüssel bekommt jede Wissenschaftler*in?

Ein geheimes Projekt

Problem: Drei Wissenschaftler*innen arbeiten an einem geheimen Projekt. Die Dokumente dazu legen sie in einem Tresor, den sie mit Vorhängeschlössern verschliessen. Sie möchten den Tresor nur dann öffnen können, wenn mindestens zwei der drei Wissenschaftler*innen zugegen sind. Wie viele Schlösser brauchen sie mindestens dafür und wie viele Schlüssel bekommt jede Wissenschaftler*in?

Lösung: Mindestens drei Schlösser. Jede Wissenschaftler*in bekommt zwei Schlüssel.

Ein geheimes Projekt

Problem: Elf Wissenschaftler*innen arbeiten an einem geheimen Projekt. Die Dokumente dazu legen sie in einem Tresor, den sie mit Vorhängeschlössern verschliessen. Sie möchten den Tresor nur dann öffnen können, wenn mindestens sechs der elf Wissenschaftler*innen zugegen sind. Wie viele Schlösser brauchen sie mindestens dafür und wie viele Schlüssel bekommt jede Wissenschaftler*in?

Ein geheimes Projekt

Problem: Elf Wissenschaftler*innen arbeiten an einem geheimen Projekt. Die Dokumente dazu legen sie in einem Tresor, den sie mit Vorhängeschlössern verschliessen. Sie möchten den Tresor nur dann öffnen können, wenn mindestens sechs der elf Wissenschaftler*innen zugegen sind. Wie viele Schlösser brauchen sie mindestens dafür und wie viele Schlüssel bekommt jede Wissenschaftler*in?

Lösung: Es sind mindestens 462 Schlösser und 252 Schlüssel pro Wissenschaftler*in nötig!

Ein geheimes Projekt

Problem: Elf Wissenschaftler*innen arbeiten an einem geheimen Projekt. Die Dokumente dazu legen sie in einem Tresor, den sie mit Vorhängeschlössern verschliessen. Sie möchten den Tresor nur dann öffnen können, wenn mindestens sechs der elf Wissenschaftler*innen zugegen sind. Wie viele Schlösser brauchen sie mindestens dafür und wie viele Schlüssel bekommt jede Wissenschaftler*in?

Lösung: Es sind mindestens 462 Schlösser und 252 Schlüssel pro Wissenschaftler*in nötig!

Das ist offensichtlich unpraktisch!

Ein geheimes Projekt

Alternativer Lösungsvorschlag: Sie kaufen einen Tresor, der sich mittels einer Zahlenkombination öffnen lässt und teilen sich das Passwort auf, so dass sich das Passwort nur rekonstruieren lässt, wenn genug Leute dabei sind.

Nehmen wir wieder an, dass 11 Personen am Projekt beteiligt sind und das Passwort nur mit mindestens 6 einverstandenen Personen rekonstruiert werden kann.

Ein geheimes Projekt

Alternativer Lösungsvorschlag: Sie kaufen einen Tresor, der sich mittels einer Zahlenkombination öffnen lässt und teilen sich das Passwort auf, so dass sich das Passwort nur rekonstruieren lässt, wenn genug Leute dabei sind.

Nehmen wir wieder an, dass 11 Personen am Projekt beteiligt sind und das Passwort nur mit mindestens 6 einverstandenen Personen rekonstruiert werden kann.

Vorteile:

1. Selbst wenn eine Person ihr Passwort verliert, kann das tatsächliche Passwort rekonstruiert werden. Wenn z.B. eine neutrale Person das Passwort hätte, könnte diese es verlieren, vergessen oder plötzlich sterben.

Ein geheimes Projekt

Alternativer Lösungsvorschlag: Sie kaufen einen Tresor, der sich mittels einer Zahlenkombination öffnen lässt und teilen sich das Passwort auf, so dass sich das Passwort nur rekonstruieren lässt, wenn genug Leute dabei sind.

Nehmen wir wieder an, dass 11 Personen am Projekt beteiligt sind und das Passwort nur mit mindestens 6 einverstandenen Personen rekonstruiert werden kann.

Vorteile:

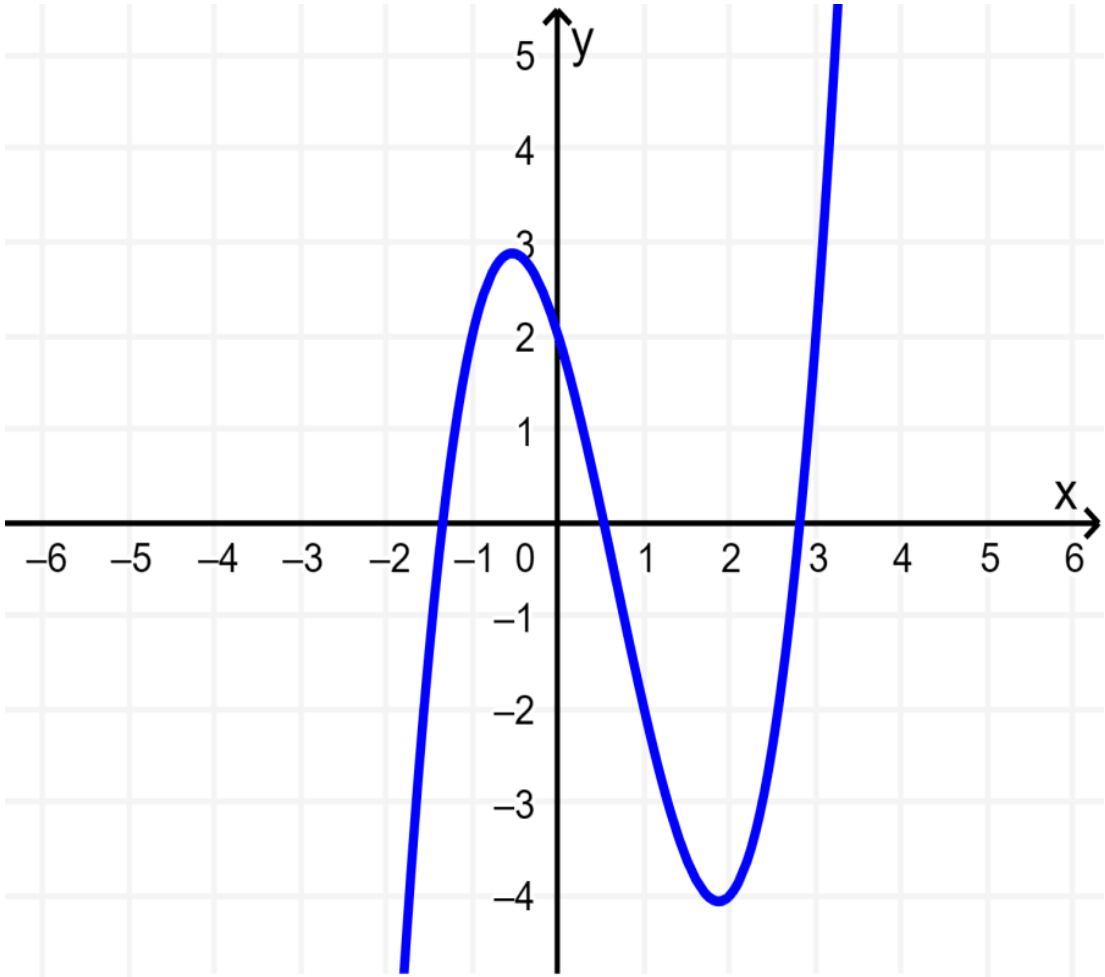
1. Selbst wenn eine Person ihr Passwort verliert, kann das tatsächliche Passwort rekonstruiert werden. Wenn z.B. eine neutrale Person das Passwort hätte, könnte diese es verlieren, vergessen oder plötzlich sterben.
2. Eine gewisse Anzahl muss einverstanden sein (tatsächliche Anwendungen finden sich z.B. in digitalen Signaturen oder Abschusscodes von Raketen).

Shamir's Secret Sharing

Heute werden wir uns mit einem Ansatz zur Verschlüsselung von Passwörtern beschäftigen, der von Adi Shamir (1979) entwickelt wurde.

Die Methode basiert auf Polynominterpolation. Dazu müssen wir zuerst einige Dinge über Polynome lernen.

Polynome



$$f(x) = x^3 - 2\,x^2 - 3\,x + 2$$

Polynome

Sei $n \geq 0$ eine ganze Zahl. Ein Polynom vom Grad n mit Koeffizienten in $\mathbb{R}$ ist eine Funktion von der Form

$$a_0 + a_1 x + a_2 x^2 + ... + a_n x^n,$$

wobei $a_0, a_1, ..., a_n \in \mathbb{R}$ und x die Variable ist.

Polynome

Sei $n \geq 0$ eine ganze Zahl. Ein Polynom vom Grad n mit Koeffizienten in $\mathbb{R}$ ist eine Funktion von der Form

$$a_0 + a_1 x + a_2 x^2 + ... + a_n x^n,$$

wobei $a_0, a_1, ..., a_n \in \mathbb{R}$ und x die Variable ist.

Beispiel: Die Funktion $p(x) = x^2 - x + 1$ ist ein Polynom vom Grad 2.

Rechenregeln

Für ein Polynom

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

mit $a_n \neq 0$ bezeichnen wir n als den *Grad* von $p(x)$ und schreiben $n = \mathrm{Grad}(p)$.

Zum Beispiel ist $\mathrm{Grad}(x^2 - x + 1) = 2$.

Rechenregeln

Für ein Polynom

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

mit $a_n \neq 0$ bezeichnen wir n als den *Grad* von $p(x)$ und schreiben $n = \mathrm{Grad}(p)$.

Zum Beispiel ist $\mathrm{Grad}(x^2 - x + 1) = 2$.

Rechenregeln für den Grad der Polynome.
Seien p, q zwei Polynome. Dann gelten die folgenden Regeln:

1. $\mathrm{Grad}(p) = \mathrm{Grad}(q) \Rightarrow \mathrm{Grad}(p + q) \leq \mathrm{Grad}(p)$
2. $\mathrm{Grad}(p \cdot q) = \mathrm{Grad}(p) \cdot \mathrm{Grad}(q)$

Aufgabe: Beweise die Rechenregeln für Grad.

Eindeutigkeit der Polynomdarstellung

Frage: Sei $n \geq 0$. Seien $a_0, a_1, ..., a_n, b_0, b_1, ..., b_n \in \mathbb{R}$. Angenommen, dass

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0 \qquad (1)$$

für alle $x \in \mathbb{R}$ gilt. Gilt dann auch $a_0 = b_0$, $a_1 = b_1$, ..., $a_n = b_n$?

Eindeutigkeit der Polynomdarstellung

Frage: Sei $n \geq 0$. Seien $a_0, a_1, ..., a_n, b_0, b_1, ..., b_n \in \mathbb{R}$. Angenommen, dass

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0 \qquad (1)$$

für alle $x \in \mathbb{R}$ gilt. Gilt dann auch $a_0 = b_0$, $a_1 = b_1$, ..., $a_n = b_n$?

Ja!

Eindeutigkeit der Polynomdarstellung

Frage: Sei $n \geq 0$. Seien $a_0, a_1, ..., a_n, b_0, b_1, ..., b_n \in \mathbb{R}$. Angenommen, dass

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0 \qquad (1)$$

für alle $x \in \mathbb{R}$ gilt. Gilt dann auch $a_0 = b_0$, $a_1 = b_1$, ..., $a_n = b_n$?

Ja! Betrachten wir die Gleichung (1) an $x = 0$. Daraus folgt unmittelbar, dass $a_0 = b_0$.

Eindeutigkeit der Polynomdarstellung

Frage: Sei $n \geq 0$. Seien $a_0, a_1, ..., a_n, b_0, b_1, ..., b_n \in \mathbb{R}$. Angenommen, dass

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0 \qquad (1)$$

für alle $x \in \mathbb{R}$ gilt. Gilt dann auch $a_0 = b_0$, $a_1 = b_1$, ..., $a_n = b_n$?

Ja! Betrachten wir die Gleichung (1) an $x = 0$. Daraus folgt unmittelbar, dass $a_0 = b_0$.
Also haben wir

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x$$

für alle $x \in \mathbb{R}$.

Eindeutigkeit der Polynomdarstellung

Beide Seiten nach x ableiten:

$$n \cdot a_n x^{n-1} + (n-1) \cdot a_{n-1} x^{n-2} + \ldots + a_1 = n \cdot b_n x^{n-1} + (n-1) \cdot b_{n-1} x^{n-2} + \ldots + b_1 \quad (2)$$

für alle $x \in \mathbb{R}$.

Eindeutigkeit der Polynomdarstellung

Beide Seiten nach x ableiten:

$$n \cdot a_n x^{n-1} + (n-1) \cdot a_{n-1} x^{n-2} + \ldots + a_1 = n \cdot b_n x^{n-1} + (n-1) \cdot b_{n-1} x^{n-2} + \ldots + b_1 \quad (2)$$

für alle $x \in \mathbb{R}$.
Jetzt schauen wir uns die Gleichung (2) wieder an $x = 0$ an und bekommen $a_1 = b_1$.

Eindeutigkeit der Polynomdarstellung

Beide Seiten nach x ableiten:

$$n \cdot a_n x^{n-1} + (n-1) \cdot a_{n-1} x^{n-2} + \ldots + a_1 = n \cdot b_n x^{n-1} + (n-1) \cdot b_{n-1} x^{n-2} + \ldots + b_1 \quad (2)$$

für alle $x \in \mathbb{R}$.
Jetzt schauen wir uns die Gleichung (2) wieder an $x = 0$ an und bekommen $a_1 = b_1$.

Wieder beide Seiten nach x ableiten:

$$\begin{aligned} & n \cdot (n-1) \cdot a_n x^{n-2} + (n-1) \cdot (n-2) \cdot a_{n-1} x^{n-3} + \ldots + 2 \cdot a_2 \\ & = n \cdot (n-1) \cdot b_n x^{n-2} + (n-1) \cdot (n-2) \cdot b_{n-1} x^{n-3} + \ldots + 2 \cdot b_2 \end{aligned} \quad (3)$$

und die Gleichung (3) an $x = 0$ auswerten gibt $2 \cdot a_2 = 2 \cdot b_2 \Rightarrow a_2 = b_2$.

Eindeutigkeit der Polynomdarstellung

Beide Seiten nach x ableiten:

$$n \cdot a_n x^{n-1} + (n-1) \cdot a_{n-1} x^{n-2} + \ldots + a_1 = n \cdot b_n x^{n-1} + (n-1) \cdot b_{n-1} x^{n-2} + \ldots + b_1 \quad (2)$$

für alle $x \in \mathbb{R}$.
Jetzt schauen wir uns die Gleichung (2) wieder an $x = 0$ an und bekommen $a_1 = b_1$.

Wieder beide Seiten nach x ableiten:

$$\begin{aligned} & n \cdot (n-1) \cdot a_n x^{n-2} + (n-1) \cdot (n-2) \cdot a_{n-1} x^{n-3} + \ldots + 2 \cdot a_2 \\ & = n \cdot (n-1) \cdot b_n x^{n-2} + (n-1) \cdot (n-2) \cdot b_{n-1} x^{n-3} + \ldots + 2 \cdot b_2 \end{aligned} \quad (3)$$

und die Gleichung (3) an $x = 0$ auswerten gibt $2 \cdot a_2 = 2 \cdot b_2 \Rightarrow a_2 = b_2$.

Und so weiter ...

Eindeutigkeit der Polynomdarstellung

Wir halten also fest:

Theorem 1

Sei $n \geq 0$. Seien $a_0, a_1, ..., a_n, b_0, b_1, ..., b_n \in \mathbb{R}$. Angenommen, dass

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0$$

für alle $x \in \mathbb{R}$ gilt. Dann gilt $a_0 = b_0$, $a_1 = b_1$, ..., $a_n = b_n$.

Euklidische Division für Polynome

Euklidische Division ganzer Zahlen: Wir haben heute Morgen gesehen, dass für ganze Zahlen n und q immer $a, r \in \mathbb{Z}$ existiert mit $0 \leq r < |q|$, so dass

$$n = aq + r.$$

Euklidische Division für Polynome

Euklidische Division ganzer Zahlen: Wir haben heute Morgen gesehen, dass für ganze Zahlen n und q immer $a, r \in \mathbb{Z}$ existiert mit $0 \leq r < |q|$, so dass

$$n = aq + r.$$

Dasselbe gilt für Polynome! Seien $P(x)$, $Q(x)$ zwei Polynome. Dann existieren Polynome $A(x)$ und $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass

$$P(x) = A(x)Q(x) + R(x).$$

Aufgabe: Beweise die Aussage.

Euklidische Division für Polynome

Falls $\mathrm{Grad}(Q) > \mathrm{Grad}(P)$ können wir $A(x) = 0$ und $R(x) = P(x)$ wählen und wir sind fertig.

Euklidische Division für Polynome

Falls $\mathrm{Grad}(Q) > \mathrm{Grad}(P)$ können wir $A(x) = 0$ und $R(x) = P(x)$ wählen und wir sind fertig.

Also nehmen wir an, dass $\mathrm{Grad}(Q) \leq \mathrm{Grad}(P)$.

Euklidische Division für Polynome

Falls $\mathrm{Grad}(Q) > \mathrm{Grad}(P)$ können wir $A(x) = 0$ und $R(x) = P(x)$ wählen und wir sind fertig.

Also nehmen wir an, dass $\mathrm{Grad}(Q) \leq \mathrm{Grad}(P)$. Schreiben wir

$$Q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0 \text{ und}$$
$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

wobei $n \geq m$ und $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{R}$ und $a_n, b_m \neq 0$.

Euklidische Division für Polynome

Falls $\mathrm{Grad}(Q) > \mathrm{Grad}(P)$ können wir $A(x) = 0$ und $R(x) = P(x)$ wählen und wir sind fertig.

Also nehmen wir an, dass $\mathrm{Grad}(Q) \leq \mathrm{Grad}(P)$. Schreiben wir

$$Q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0 \text{ und}$$
$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

wobei $n \geq m$ und $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{R}$ und $a_n, b_m \neq 0$.

Wähle das Polynom $A_n(x) = \frac{a_n}{b_m} x^{n-m}$. Dann ist

$$P(x) - A_n(x)Q(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots - \frac{a_n}{b_m} x^{n-m}(b_m x^m + b_{m-1} x^{m-1} + \ldots)$$
$$= (a_n x^n - a_n x^n) + \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) x^{n-1} + \ldots$$

ein Polynom vom Grad $\leq n - 1$.
Wiederhole diesen Vorgang mit $P(x) \leftarrow P(x) - A_n(x)Q(x)$ und $Q(x) \leftarrow Q(x)$.
Der Vorgang geht so lange gut, bis wir ein Polynom mit Grad $< \mathrm{Grad}(Q)$ haben.

Euklidische Division für Polynome

Falls $\mathrm{Grad}(Q) > \mathrm{Grad}(P)$ können wir $A(x) = 0$ und $R(x) = P(x)$ wählen und wir sind fertig.

Also nehmen wir an, dass $\mathrm{Grad}(Q) \leq \mathrm{Grad}(P)$. Schreiben wir

$$Q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0 \text{ und}$$
$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

wobei $n \geq m$ und $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{R}$ und $a_n, b_m \neq 0$.

Wähle das Polynom $A_n(x) = \frac{a_n}{b_m} x^{n-m}$. Dann ist

$$P(x) - A_n(x)Q(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots - \frac{a_n}{b_m} x^{n-m}(b_m x^m + b_{m-1} x^{m-1} + \ldots)$$
$$= (a_n x^n - a_n x^n) + \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) x^{n-1} + \ldots$$

ein Polynom vom Grad $\leq n - 1$.

Euklidische Division für Polynome

Falls $\mathrm{Grad}(Q) > \mathrm{Grad}(P)$ können wir $A(x) = 0$ und $R(x) = P(x)$ wählen und wir sind fertig.

Also nehmen wir an, dass $\mathrm{Grad}(Q) \leq \mathrm{Grad}(P)$. Schreiben wir

$$Q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0 \text{ und}$$
$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

wobei $n \geq m$ und $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{R}$ und $a_n, b_m \neq 0$.

Wähle das Polynom $A_n(x) = \frac{a_n}{b_m} x^{n-m}$. Dann ist

$$P(x) - A_n(x)Q(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots - \frac{a_n}{b_m} x^{n-m}(b_m x^m + b_{m-1} x^{m-1} + \ldots)$$
$$= (a_n x^n - a_n x^n) + \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) x^{n-1} + \ldots$$

ein Polynom vom Grad $\leq n - 1$.
Wiederhole diesen Vorgang mit $P(x) \leftarrow P(x) - A_n(x)Q(x)$ und $Q(x) \leftarrow Q(x)$.
Der Vorgang geht so lange gut, bis wir ein Polynom mit Grad $< \mathrm{Grad}(Q)$ haben.

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$.

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$.

Schritt 1: Ist $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$?

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$.

Schritt 1: Ist $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$? $\rightarrow$ Nein!

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$.

Schritt 1: Ist $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$? $\rightarrow$ Nein!

Schritt 2: Wähle $A_3(x) = \frac{3}{2}x^{3-1} = \frac{3}{2}x^2$. Dann ist

$$P(x) - A_3(x)Q(x) = 3x^3 + 1 - \frac{3}{2}x^2(2x+1)$$

$$= 3x^3 + 1 - \left(3x^3 + \frac{3}{2}x^2\right)$$

$$= -\frac{3}{2}x^2 + 1.$$

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$.

Schritt 1: Ist $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$? $\rightarrow$ Nein!

Schritt 2: Wähle $A_3(x) = \frac{3}{2}x^{3-1} = \frac{3}{2}x^2$. Dann ist

$$P(x) - A_3(x)Q(x) = 3x^3 + 1 - \frac{3}{2}x^2(2x+1)$$

$$= 3x^3 + 1 - \left(3x^3 + \frac{3}{2}x^2\right)$$

$$= -\frac{3}{2}x^2 + 1.$$

Schritt 3: Ersetze $P(x)$ mit $-\frac{3}{2}x^2 + 1$, das jetzt Grad 2 hat (anstatt Grad 3) und wiederhole.

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$. Gefunden: $A_3(x) = \frac{3}{2}x^2$.

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$. Gefunden: $A_3(x) = \frac{3}{2}x^2$.

Schritt 4: Sei $A_2(x) = -\frac{4}{3}x$, so dass

$$\begin{aligned} P(x) - A_3(x)Q(x) - A_2(x)Q(x) &= \left(-\frac{3}{2}x^2 + 1\right) + \frac{4}{3}x(2x+1) \\ &= \frac{3}{4}x + 1 \end{aligned}$$

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$. Gefunden: $A_3(x) = \frac{3}{2}x^2$.

Schritt 4: Sei $A_2(x) = -\frac{4}{3}x$, so dass

$$\begin{aligned} P(x) - A_3(x)Q(x) - A_2(x)Q(x) &= \left(-\frac{3}{2}x^2 + 1\right) + \frac{4}{3}x(2x+1) \\ &= \frac{3}{4}x + 1 \end{aligned}$$

Schritt 5: Sei $A_1(x) = \frac{3}{8}$, so dass

$$\begin{aligned} P(x) - A_3(x)Q(x) - A_2(x)Q(x) - A_1(x)Q(x) &= \left(\frac{3}{4}x + 1\right) + \frac{3}{8}(2x+1) \\ &= \frac{5}{8}. \end{aligned}$$

Euklidische Division für Polynome: Zahlenbeispiel

Sei $P(x) = 3x^3 + 1$ und $Q(x) = 2x + 1$. Gefunden: $A_3(x) = \frac{3}{2}x^2$.

Schritt 4: Sei $A_2(x) = -\frac{4}{3}x$, so dass

$$\begin{aligned} P(x) - A_3(x)Q(x) - A_2(x)Q(x) &= \left(-\frac{3}{2}x^2 + 1\right) + \frac{4}{3}x(2x+1) \\ &= \frac{3}{4}x + 1 \end{aligned}$$

Schritt 5: Sei $A_1(x) = \frac{3}{8}$, so dass

$$\begin{aligned} P(x) - A_3(x)Q(x) - A_2(x)Q(x) - A_1(x)Q(x) &= \left(\frac{3}{4}x + 1\right) + \frac{3}{8}(2x+1) \\ &= \frac{5}{8}. \end{aligned}$$

D.h. wir haben $P(x) = (A_3(x) + A_2(x) + A_1(x))Q(x) + \frac{5}{8}$ und die gesuchten Polynome sind $A(x) = A_3(x) + A_2(x) + A_1(x) = \frac{3}{2}x^2 - \frac{4}{3}x + \frac{3}{8}$ und $R(x) = \frac{5}{8}$.

Euklidische Division für Polynome

Algorithmus:
Input: Polynome $P(x)$, $Q(x)$.
Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

Euklidische Division für Polynome

Algorithmus:
Input: Polynome $P(x)$, $Q(x)$.
Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

1. Setze $A(x) = 0$.

Euklidische Division für Polynome

Algorithmus:
Input: Polynome $P(x)$, $Q(x)$.
Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

1. Setze $A(x) = 0$.
2. $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$?

Euklidische Division für Polynome

Algorithmus:
Input: Polynome $P(x)$, $Q(x)$.
Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

1. Setze $A(x) = 0$.
2. $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$?
    1. Ja: Ausgabe von $A(x)$ und $R(x) = P(x)$. Fertig.

Euklidische Division für Polynome

Algorithmus:
Input: Polynome $P(x)$, $Q(x)$.
Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

1. Setze $A(x) = 0$.
2. $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$?
   1. Ja: Ausgabe von $A(x)$ und $R(x) = P(x)$. Fertig.
   2. Nein: Continue.

Euklidische Division für Polynome

Algorithmus:
Input: Polynome $P(x)$, $Q(x)$.
Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

1. Setze $A(x) = 0$.
2. $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$?
   1. Ja: Ausgabe von $A(x)$ und $R(x) = P(x)$. Fertig.
   2. Nein: Continue.
3. Sei $B(x) = \frac{\mathrm{Lead}(P)}{\mathrm{Lead}(Q)} x^{\mathrm{Grad}(P)-\mathrm{Grad}(Q)}$.

Euklidische Division für Polynome

Algorithmus:
Input: Polynome $P(x)$, $Q(x)$.
Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

1. Setze $A(x) = 0$.
2. $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$?
   1. Ja: Ausgabe von $A(x)$ und $R(x) = P(x)$. Fertig.
   2. Nein: Continue.
3. Sei $B(x) = \frac{\mathrm{Lead}(P)}{\mathrm{Lead}(Q)} x^{\mathrm{Grad}(P)-\mathrm{Grad}(Q)}$.
4. $P(x) \leftarrow P(x) - B(x)Q(x)$.

Euklidische Division für Polynome

Algorithmus:
Input: Polynome $P(x)$, $Q(x)$.
Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

1. Setze $A(x) = 0$.
2. $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$?
   1. Ja: Ausgabe von $A(x)$ und $R(x) = P(x)$. Fertig.
   2. Nein: Continue.
3. Sei $B(x) = \frac{\mathrm{Lead}(P)}{\mathrm{Lead}(Q)} x^{\mathrm{Grad}(P)-\mathrm{Grad}(Q)}$.
4. $P(x) \leftarrow P(x) - B(x)Q(x)$.
5. $A(x) \leftarrow A(x) + B(x)$.

Euklidische Division für Polynome

Algorithmus:

Input: Polynome $P(x)$, $Q(x)$.

Output: $A(x)$, $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q)$, so dass $P(x) = A(x)Q(x) + R(x)$.

1. Setze $A(x) = 0$.
2. $\mathrm{Grad}(P) < \mathrm{Grad}(Q)$?
   1. Ja: Ausgabe von $A(x)$ und $R(x) = P(x)$. Fertig.
   2. Nein: Continue.
3. Sei $B(x) = \frac{\mathrm{Lead}(P)}{\mathrm{Lead}(Q)} x^{\mathrm{Grad}(P)-\mathrm{Grad}(Q)}$.
4. $P(x) \leftarrow P(x) - B(x)Q(x)$.
5. $A(x) \leftarrow A(x) + B(x)$.
6. Zurück zu Schritt 2.

Nullstellen von Polynomen

Sei $P(x)$ ein Polynom vom Grad n, das am Punkt $x = x_1$ eine Nullstelle hat, d.h. $P(x_1) = 0$.

Nullstellen von Polynomen

Sei $P(x)$ ein Polynom vom Grad n, das am Punkt $x = x_1$ eine Nullstelle hat, d.h. $P(x_1) = 0$.

Nach der euklidischen Division für die Polynome $P(x)$ und $Q(x) = x - x_1$ gibt es Polynome $A(x)$ und $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q) = 1$, so dass

$$P(x) = A(x)(x - x_1) + R(x).$$

Nullstellen von Polynomen

Sei $P(x)$ ein Polynom vom Grad n, das am Punkt $x = x_1$ eine Nullstelle hat, d.h. $P(x_1) = 0$.

Nach der euklidischen Division für die Polynome $P(x)$ und $Q(x) = x - x_1$ gibt es Polynome $A(x)$ und $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q) = 1$, so dass

$$P(x) = A(x)(x - x_1) + R(x).$$

Bemerke: $R(x_1) = P(x_1) - A(x_1) \cdot (x_1 - x_1) = 0$. Aber da das Polynom $R(x)$ den Grad 0 hat, muss es die Form $R(x) = a_0$ haben, also $R(x) = 0$.

Nullstellen von Polynomen

Sei $P(x)$ ein Polynom vom Grad n, das am Punkt $x = x_1$ eine Nullstelle hat, d.h. $P(x_1) = 0$.

Nach der euklidischen Division für die Polynome $P(x)$ und $Q(x) = x - x_1$ gibt es Polynome $A(x)$ und $R(x)$ mit $\mathrm{Grad}(R) < \mathrm{Grad}(Q) = 1$, so dass

$$P(x) = A(x)(x - x_1) + R(x).$$

Bemerke: $R(x_1) = P(x_1) - A(x_1) \cdot (x_1 - x_1) = 0$. Aber da das Polynom $R(x)$ den Grad 0 hat, muss es die Form $R(x) = a_0$ haben, also $R(x) = 0$.

Nach den Rechenregeln für den Grad von Polynomen gilt:

$$n = \mathrm{Grad}(P) = \mathrm{Grad}(A(x) \cdot (x - x_1)) = \mathrm{Grad}(A) + \mathrm{Grad}(x - x_1),$$

also $\mathrm{Grad}(A) = n - 1$.

Nullstellen von Polynomen

Wir halten also fest:

Theorem 2

Sei $P(x)$ ein Polynom vom Grad $n \geq 1$ und $x_1 \in \mathbb{R}$ so, dass $P(x_1) = 0$. Dann gibt es ein Polynom $A(x)$ mit $\mathrm{Grad}(A) = n - 1$ mit

$$P(x) = A(x) \cdot (x - x_1).$$

Fundamentalsatz der Algebra

Frage: Wie viele Nullstellen kann ein Polynom $P(x)$ vom Grad $n \geq 1$ höchstens haben?

Fundamentalsatz der Algebra

Frage: Wie viele Nullstellen kann ein Polynom $P(x)$ vom Grad $n \geq 1$ höchstens haben?

Höchstens n Nullstellen!

Fundamentalsatz der Algebra

Frage: Wie viele Nullstellen kann ein Polynom $P(x)$ vom Grad $n \geq 1$ höchstens haben?

Höchstens n Nullstellen!

Betrachten wir den Fall $n = 1$. Dann ist $P(x) = a_1 x + a_0$ für gewisse $a_0, a_1 \in \mathbb{R}$. Offenbar hat $a_1 x + a_0 = 0$ nur eine Lösung, nämlich $x = -\frac{a_0}{a_1}$.

Fundamentalsatz der Algebra

Frage: Wie viele Nullstellen kann ein Polynom $P(x)$ vom Grad $n \geq 1$ höchstens haben?

Höchstens n Nullstellen!

Betrachten wir den Fall $n = 1$. Dann ist $P(x) = a_1 x + a_0$ für gewisse $a_0, a_1 \in \mathbb{R}$. Offenbar hat $a_1 x + a_0 = 0$ nur eine Lösung, nämlich $x = -\frac{a_0}{a_1}$.

Betrachten wir nun $n = 2$ und nehmen wir an, dass $P(x)$ mehr als zwei Nullstellen hat. Seien $x_1, x_2, x_3 \in \mathbb{R}$ paarweise verschiedene Punkte, so dass $P(x_i) = 0$.

Fundamentalsatz der Algebra

Frage: Wie viele Nullstellen kann ein Polynom $P(x)$ vom Grad $n \geq 1$ höchstens haben?

Höchstens n Nullstellen!

Betrachten wir den Fall $n = 1$. Dann ist $P(x) = a_1 x + a_0$ für gewisse $a_0, a_1 \in \mathbb{R}$. Offenbar hat $a_1 x + a_0 = 0$ nur eine Lösung, nämlich $x = -\frac{a_0}{a_1}$.

Betrachten wir nun $n = 2$ und nehmen wir an, dass $P(x)$ mehr als zwei Nullstellen hat. Seien $x_1, x_2, x_3 \in \mathbb{R}$ paarweise verschiedene Punkte, so dass $P(x_i) = 0$.

Dann gilt

$$P(x) = A(x)(x - x_3)$$

für ein Polynom $\mathrm{Grad}(A) = 1$.

Fundamentalsatz der Algebra

Frage: Wie viele Nullstellen kann ein Polynom $P(x)$ vom Grad $n \geq 1$ höchstens haben?

Höchstens n Nullstellen!

Betrachten wir den Fall $n = 1$. Dann ist $P(x) = a_1 x + a_0$ für gewisse $a_0, a_1 \in \mathbb{R}$. Offenbar hat $a_1 x + a_0 = 0$ nur eine Lösung, nämlich $x = -\frac{a_0}{a_1}$.

Betrachten wir nun $n = 2$ und nehmen wir an, dass $P(x)$ mehr als zwei Nullstellen hat. Seien $x_1, x_2, x_3 \in \mathbb{R}$ paarweise verschiedene Punkte, so dass $P(x_i) = 0$.

Dann gilt

$$P(x) = A(x)(x - x_3)$$

für ein Polynom $\mathrm{Grad}(A) = 1$. Bemerke, dass

$$0 = P(x_1) = A(x_1)(x_1 - x_3) \text{ und } 0 = P(x_2) = A(x_2)(x_2 - x_3)$$

gilt, also auch $A(x_1) = A(x_2) = 0$. Aber ein Polynom vom Grad 1 hat höchstens eine Nullstelle.

Fundamentalsatz der Algebra

Frage: Wie viele Nullstellen kann ein Polynom $P(x)$ vom Grad $n \geq 1$ höchstens haben?

Höchstens n Nullstellen!

Betrachten wir den Fall $n = 1$. Dann ist $P(x) = a_1 x + a_0$ für gewisse $a_0, a_1 \in \mathbb{R}$. Offenbar hat $a_1 x + a_0 = 0$ nur eine Lösung, nämlich $x = -\frac{a_0}{a_1}$.

Betrachten wir nun $n = 2$ und nehmen wir an, dass $P(x)$ mehr als zwei Nullstellen hat. Seien $x_1, x_2, x_3 \in \mathbb{R}$ paarweise verschiedene Punkte, so dass $P(x_i) = 0$.

Dann gilt

$$P(x) = A(x)(x - x_3)$$

für ein Polynom $\mathrm{Grad}(A) = 1$. Bemerke, dass

$$0 = P(x_1) = A(x_1)(x_1 - x_3) \text{ und } 0 = P(x_2) = A(x_2)(x_2 - x_3)$$

gilt, also auch $A(x_1) = A(x_2) = 0$. Aber ein Polynom vom Grad 1 hat höchstens eine Nullstelle.
$\Rightarrow$ Es kann auch kein Polynom vom Grad $n = 2$ geben, das mehr als n Nullstellen hat!
Und so weiter...

Fundamentalsatz der Algebra

Wir halten also fest:

Theorem 3 (Fundamentalsatz der Algebra)

Ein Polynom $P(x)$ vom Grad $n \geq 0$, das nicht konstant Null ist, hat höchstens n Nullstellen.

Exkurs: Induktionsprinzip

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik.

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik. Sie formalisiert das Argument "und so weiter...".

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik. Sie formalisiert das Argument "und so weiter...".
Sei $A(n)$ eine Aussage, die von einer Zahl n abhängt (z.B. $A(n)$: Für alle n gilt, dass $1 + 2 + ... + n = \frac{1}{2} \cdot n \cdot (n + 1)$.)

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik. Sie formalisiert das Argument "und so weiter...".
Sei $A(n)$ eine Aussage, die von einer Zahl n abhängt (z.B. $A(n)$: Für alle n gilt, dass $1 + 2 + ... + n = \frac{1}{2} \cdot n \cdot (n + 1)$.) Die vollständige Induktion beweist die Aussage in zwei Schritten:

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik. Sie formalisiert das Argument "und so weiter...".
Sei $A(n)$ eine Aussage, die von einer Zahl n abhängt (z.B. $A(n)$: Für alle n gilt, dass $1 + 2 + ... + n = \frac{1}{2} \cdot n \cdot (n + 1)$.) Die vollständige Induktion beweist die Aussage in zwei Schritten:

1. Beweise, dass $A(1)$ stimmt.

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik. Sie formalisiert das Argument "und so weiter...".
Sei $A(n)$ eine Aussage, die von einer Zahl n abhängt (z.B. $A(n)$: Für alle n gilt, dass $1 + 2 + ... + n = \frac{1}{2} \cdot n \cdot (n + 1)$.) Die vollständige Induktion beweist die Aussage in zwei Schritten:

1. Beweise, dass $A(1)$ stimmt.
2. Beweise, dass für alle $n \geq 2$ die Korrektheit der Aussage $A(n-1)$, die Korrektheit von $A(n)$ impliziert.

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik. Sie formalisiert das Argument "und so weiter...".
Sei $A(n)$ eine Aussage, die von einer Zahl n abhängt (z.B. $A(n)$: Für alle n gilt, dass $1 + 2 + ... + n = \frac{1}{2} \cdot n \cdot (n + 1)$.) Die vollständige Induktion beweist die Aussage in zwei Schritten:

1. Beweise, dass $A(1)$ stimmt.
2. Beweise, dass für alle $n \geq 2$ die Korrektheit der Aussage $A(n-1)$, die Korrektheit von $A(n)$ impliziert.

An unserem Beispiel:

1. $A(1)$ ist korrekt: $1 = \frac{1}{2} \cdot 1 \cdot (1 + 1)$.

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik. Sie formalisiert das Argument "und so weiter...".
Sei $A(n)$ eine Aussage, die von einer Zahl n abhängt (z.B. $A(n)$: Für alle n gilt, dass $1 + 2 + ... + n = \frac{1}{2} \cdot n \cdot (n + 1)$.) Die vollständige Induktion beweist die Aussage in zwei Schritten:

1. Beweise, dass $A(1)$ stimmt.
2. Beweise, dass für alle $n \geq 2$ die Korrektheit der Aussage $A(n-1)$, die Korrektheit von $A(n)$ impliziert.

An unserem Beispiel:

1. $A(1)$ ist korrekt: $1 = \frac{1}{2} \cdot 1 \cdot (1 + 1)$.
2. $A(n-1)$ impliziert $A(n)$:

Exkurs: Induktionsprinzip

Bei der "vollständigen Induktion" handelt es sich um eine Beweismethode in der Mathematik. Sie formalisiert das Argument "und so weiter...".
Sei $A(n)$ eine Aussage, die von einer Zahl n abhängt (z.B. $A(n)$: Für alle n gilt, dass $1 + 2 + ... + n = \frac{1}{2} \cdot n \cdot (n + 1)$.) Die vollständige Induktion beweist die Aussage in zwei Schritten:

1. Beweise, dass $A(1)$ stimmt.
2. Beweise, dass für alle $n \geq 2$ die Korrektheit der Aussage $A(n-1)$, die Korrektheit von $A(n)$ impliziert.

An unserem Beispiel:

1. $A(1)$ ist korrekt: $1 = \frac{1}{2} \cdot 1 \cdot (1 + 1)$.
2. $A(n-1)$ impliziert $A(n)$:

$$\begin{aligned} 1 + 2 + ... + (n-1) + n &= (1 + 2 + ... + (n-1)) + n \\ &= \frac{1}{2} \cdot (n-1) \cdot n + n \\ &= \frac{1}{2} \cdot (n+1) \cdot n. \end{aligned}$$

Polynominterpolation

Sei $P(x)$ ein Polynom vom Grad n, von dem wir aber nur die Werte an bestimmten Puntken $x = x_1, x_2, ..., x_k$ kennen. Wie gross muss k mindestens sein, damit wir das Polynom $P(x)$ rekonstruieren können?

Polynominterpolation

Sei $P(x)$ ein Polynom vom Grad n, von dem wir aber nur die Werte an bestimmten Puntken $x = x_1, x_2, ..., x_k$ kennen. Wie gross muss k mindestens sein, damit wir das Polynom $P(x)$ rekonstruieren können?

Mindestens $k = n + 1$!

Polynominterpolation

Sei $P(x)$ ein Polynom vom Grad n, von dem wir aber nur die Werte an bestimmten Puntken $x = x_1, x_2, ..., x_k$ kennen. Wie gross muss k mindestens sein, damit wir das Polynom $P(x)$ rekonstruieren können?

Mindestens $k = n + 1$!

Gegeben seien Datenpunkte $(x_1, y_1), ..., (x_{n+1}, y_{n+1})$ mit $x_i \neq x_j$ für $i \neq j$ und $y_i = P(x_i)$.

Polynominterpolation

Idee: Finde Polynome $L_i(x)$ vom Grad n, so dass

$$L_i(x_i) = 1 \text{ und}$$
$$L_i(x_j) = 0 \text{ falls } i \neq j.$$

Das Polynom $Q(x) = y_1 L_1(x) + ... + y_{n+1} L_{n+1}(x)$ hat Grad $\leq n$ und hat die Eigenschaft

$$Q(x_i) = y_1 L_1(x_i) + ... + y_i L_i(x_i) + ... + y_n L_n(x_i) = y_i.$$

D.h. das Polynom $P(x) - Q(x)$ vom Grad $\leq n$ hat $n+1$ verschiedene Nullstellen an $x = x_1, x_2, ..., x_{n+1}$, muss also kosntant Null sein nach dem Fundamentalsatz der Algebra.

Lagrange-Polynome

Für Punkte $x_1, x_2, ..., x_k$ und Werte $y_1 = P(x_1), y_2 = P(x_2), ..., y_{n+1} = P(x_{n+1})$ definieren wir die sogenannten Lagrange-Polynome.
Sei

$$L_1(x) = \frac{(x - x_2)(x - x_3) \cdots (x - x_k)}{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_{n+1})}.$$

Dann gilt

$$L_1(x_i) = 0 \text{ falls } i \neq 1$$

und

$$L_1(x_1) = \frac{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_k)}{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_k)} = 1.$$

Genauso können wir $L_2(x), ..., L_{n+1}(x)$ definieren.
Der Grad von $L_i(x)$ ist gleich n.

Lagrange-Polynome

Für Punkte $x_1, x_2, ..., x_k$ und Werte $y_1 = P(x_1), y_2 = P(x_2), ..., y_{n+1} = P(x_{n+1})$ definieren wir die sogenannten Lagrange-Polynome.
Sei

$$L_1(x) = \frac{(x - x_2)(x - x_3) \cdots (x - x_k)}{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_{n+1})}.$$

Dann gilt

$$L_1(x_i) = 0 \text{ falls } i \neq 1$$

und

$$L_1(x_1) = \frac{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_k)}{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_k)} = 1.$$

Genauso können wir $L_2(x), ..., L_{n+1}(x)$ definieren.
Der Grad von $L_i(x)$ ist gleich n.

Übung: Finde ein Polynom $P(x)$ vom Grad 2, das folgende Werte annimmt:

$$P(1) = 6, \ P(2) = 11, \ P(3) = 18.$$

Polynominterpolation

Frage: Was passiert, wenn wir ein Polynom $P(x)$ vom Grad n haben, aber nur Werte an den Punkten $x_1, ..., x_n$ kennen?

Polynominterpolation

Frage: Was passiert, wenn wir ein Polynom $P(x)$ vom Grad n haben, aber nur Werte an den Punkten $x_1, ..., x_n$ kennen?

Dann gibt es unendlich viele Möglichkeiten! Alle Polynome

$$P(x) + a \cdot (x - x_1)(x - x_2) \cdots (x - x_n)$$

vom Grad n sind dann mögliche Lösungen!

Shamir's Secret Sharing

Zurück zu unserem ursprünglichen Problem. Wir wollen ein Passwort D (irgendeine Zahl, z.B. $D = 1234$) unter 11 Leuten aufteilen, so dass mindestens 6 Leute das Passwort rekonstruieren können.

Shamir's Secret Sharing

Zurück zu unserem ursprünglichen Problem. Wir wollen ein Passwort D (irgendeine Zahl, z.B. $D = 1234$) unter 11 Leuten aufteilen, so dass mindestens 6 Leute das Passwort rekonstruieren können.

Idee von Shamir's Secret Sharing: Sei D das numerische Passwort, das verschlüsselt werden soll. Wir können das Passwort nun als Koeffizient eines Polynoms verschlüsseln!

Shamir's Secret Sharing

Zurück zu unserem ursprünglichen Problem. Wir wollen ein Passwort D (irgendeine Zahl, z.B. $D = 1234$) unter 11 Leuten aufteilen, so dass mindestens 6 Leute das Passwort rekonstruieren können.

Idee von Shamir's Secret Sharing: Sei D das numerische Passwort, das verschlüsselt werden soll. Wir können das Passwort nun als Koeffizient eines Polynoms verschlüsseln!

1. Wähle $a_1, ..., a_5 \in \mathbb{Z}$ zufällig.
2. Definiere das Polynom $P(x) = D + a_1 x + a_2 x^2 + ... + a_5 x^5$.
3. Generiere die Datenpunkte $(1, P(1)), (2, P(2)), ..., (11, P(11))$ und verteile die 11 Datenpunkte an die 11 Personen.
4. Aus 6 dieser Datenpunkte können wir das Polynom $P(x)$ (und das Passwort $D = P(0)$) rekonstruieren!

Shamir's Secret Sharing

Zurück zu unserem ursprünglichen Problem. Wir wollen ein Passwort D (irgendeine Zahl, z.B. $D = 1234$) unter 11 Leuten aufteilen, so dass mindestens 6 Leute das Passwort rekonstruieren können.

Idee von Shamir's Secret Sharing: Sei D das numerische Passwort, das verschlüsselt werden soll. Wir können das Passwort nun als Koeffizient eines Polynoms verschlüsseln!

1. Wähle $a_1, ..., a_5 \in \mathbb{Z}$ zufällig.
2. Definiere das Polynom $P(x) = D + a_1 x + a_2 x^2 + ... + a_5 x^5$.
3. Generiere die Datenpunkte $(1, P(1)), (2, P(2)), ..., (11, P(11))$ und verteile die 11 Datenpunkte an die 11 Personen.
4. Aus 6 dieser Datenpunkte können wir das Polynom $P(x)$ (und das Passwort $D = P(0)$) rekonstruieren!

Fünf Personen können keine zusätzliche Information über D gewinnen, da es dann unendlich viele Lösungen für das interpolierte Polynom $P(x)$ gibt!