DS

Tutorial

Norina Grosch, Sebastian Reichmann

17. Dezember 2019

Organisatorisches

Feedback, Kritik, Wünsche per Unimail an:

- norina.marie.grosch [at] uni-weimar.de
- sebastian.reichmann [at] uni-weimar.de

Bitte an beide Mails, dann bekommt ihr schneller eine Antwort.

`www.uni-weimar.de/~zixi2567/tutoriate/ds/ws1819`

Organisatorisches

Feedback, Kritik, Wünsche per Unimail an:

- norina.marie.grosch [at] uni-weimar.de
- sebastian.reichmann [at] uni-weimar.de

Bitte an beide Mails, dann bekommt ihr schneller eine Antwort.
`www.uni-weimar.de/~zixi2567/tutoriate/ds/ws1819`

Am Besten bis Freitag Abend, damit wir es noch einarbeiten können ;)

Organisatorisches

Feedback, Kritik, Wünsche per Unimail an:

- norina.marie.grosch [at] uni-weimar.de
- sebastian.reichmann [at] uni-weimar.de

Bitte an beide Mails, dann bekommt ihr schneller eine Antwort.
`www.uni-weimar.de/~zixi2567/tutoriate/ds/ws1819`

Am Besten bis Freitag Abend, damit wir es noch einarbeiten können ;)

Das Tutoriat ist nicht für das Lösen der Übungsaufgaben bestimmt!

Ablauf

1. Anmerkungen zu Belegabgaben
2. Stoffwiederholung

Section 1

Anmerkungen zu Belegabgaben

Abgaben

Gruppeneigenschaften:

- Nichtleere Menge G
- Verknüpfung $\circ : G \times G \to G$ (Abgeschlossenheit)
  - $\to$ Gruppoid
- Assoziativität $a \circ (b \circ c) = (a \circ b) \circ c$
  - $\to$ Halbgruppe
- Neutrales Element $a \circ e = e \circ a = a$
  - $\to$ Monoid
- Inverses Element $a \circ a^{-1} = e$
  - $\to$ Gruppe

Section 2

Stoffwiederholung

Isomorphismus

- Gegeben: 2 Gruppen $(G, \circ)$ and $(H, \diamond)$
- Gibt es eine bijektive Funktion $\pi : G \to H$ für die gilt:

$$\pi(a \circ b) = \pi(a) \diamond \pi(b)$$

so nennt man π den Isomorphismus von $(G, \circ)$ and $(H, \diamond)$ und die beiden Gruppen sind isomorph zu einander.

Isomorphismus

- Gegeben: 2 Gruppen $(G, \circ)$ and $(H, \diamond)$
- Gibt es eine bijektive Funktion $\pi : G \to H$ für die gilt:

$$\pi(a \circ b) = \pi(a) \diamond \pi(b)$$

so nennt man π den Isomorphismus von $(G, \circ)$ and $(H, \diamond)$ und die beiden Gruppen sind isomorph zu einander.

- Beispiel:
  - $(\mathbb{Z}_{13}^*, a \cdot b \mod 13)$ and $(\mathbb{Z}_{13}^*, 2 \cdot a \cdot b \mod 13)$

Isomorphismus

- Gegeben: 2 Gruppen $(G, \circ)$ and $(H, \diamond)$
- Gibt es eine bijektive Funktion $\pi : G \to H$ für die gilt:

$$\pi(a \circ b) = \pi(a) \diamond \pi(b)$$

so nennt man π den Isomorphismus von $(G, \circ)$ and $(H, \diamond)$ und die beiden Gruppen sind isomorph zu einander.

- Beispiel:
  - $(\mathbb{Z}_{13}^*, a \cdot b \mod 13)$ and $(\mathbb{Z}_{13}^*, 2 \cdot a \cdot b \mod 13)$
  - $\pi(x) = 2^{-1} \cdot x \mod 13 = 7 \cdot x \mod 13$

Isomorphismus

- Gegeben: 2 Gruppen $(G, \circ)$ and $(H, \diamond)$
- Gibt es eine bijektive Funktion $\pi : G \to H$ für die gilt:

$$\pi(a \circ b) = \pi(a) \diamond \pi(b)$$

so nennt man π den Isomorphismus von $(G, \circ)$ and $(H, \diamond)$ und die beiden Gruppen sind isomorph zu einander.

- Beispiel:
  - $(\mathbb{Z}_{13}^*, a \cdot b \mod 13)$ and $(\mathbb{Z}_{13}^*, 2 \cdot a \cdot b \mod 13)$
  - $\pi(x) = 2^{-1} \cdot x \mod 13 = 7 \cdot x \mod 13$

$$\pi(a \cdot b \mod 13) = 2 \cdot \pi(a) \cdot \pi(b) \mod 13$$
$$7 \cdot a \cdot b \mod 13 = 2 \cdot 7 \cdot a \cdot 7 \cdot b \mod 13$$
$$7 \cdot a \cdot b \mod 13 = a \cdot 7 \cdot b \mod 13$$

Diffie-Helman Schlüsselaustausch

- Alice und Bob wählen Primzahl p und Primzahl q, welche p-1 teilt
- Alice und Bob einigen sich auf einen Generator $g \in (\mathbb{Z}_p^*, *)$

Diffie-Helman Schlüsselaustausch

- Alice und Bob wählen Primzahl p und Primzahl q, welche p-1 teilt
- Alice und Bob einigen sich auf einen Generator $g \in (\mathbb{Z}_p^*, *)$
- Alice wählt geheimes $a \in \mathbb{Z}_q$ und schickt $A = g^a$ mod p an Bob
- Bob wählt geheimes $b \in \mathbb{Z}_q$ und schickt $B = g^b$ mod p an Alice

Diffie-Helman Schlüsselaustausch

- Alice und Bob wählen Primzahl p und Primzahl q, welche p-1 teilt
- Alice und Bob einigen sich auf einen Generator $g \in (\mathbb{Z}_p^*, *)$
- Alice wählt geheimes $a \in \mathbb{Z}_q$ und schickt $A = g^a$ mod p an Bob
- Bob wählt geheimes $b \in \mathbb{Z}_q$ und schickt $B = g^b$ mod p an Alice
- öffentlich bekannt sind nun also: p, q, g, A und B

Diffie-Helman Schlüsselaustausch

- Alice und Bob wählen Primzahl p und Primzahl q, welche p-1 teilt
- Alice und Bob einigen sich auf einen Generator $g \in (\mathbb{Z}_p^*, *)$
- Alice wählt geheimes $a \in \mathbb{Z}_q$ und schickt $A = g^a$ mod p an Bob
- Bob wählt geheimes $b \in \mathbb{Z}_q$ und schickt $B = g^b$ mod p an Alice
- öffentlich bekannt sind nun also: p, q, g, A und B
- Alice und Bob berechnen mit geheimen a, b $g^{ab} = A^b = B^a = K$
- Dieses K wird als Schlüssel verwendet

Shamir Secret Sharing

- Wir wollen ein Geheimnis S auf n Personen aufteilen, aber man soll mindestens k dieser Personen brauchen um das Geheimnis zu berechnen.
- Idee: Funktionen vom Grad k-1 werden durch k Punkte eindeutig definiert

Shamir Secret Sharing

- Wir wollen ein Geheimnis S auf n Personen aufteilen, aber man soll mindestens k dieser Personen brauchen um das Geheimnis zu berechnen.
- Idee: Funktionen vom Grad k-1 werden durch k Punkte eindeutig definiert
- Wir setzen $a_0 = S$ und wählen k-1 zufällige Zahlen $a_1 ... a_{k-1}$ und bauen daraus ein Polynom:
- $f(x) = a_{k-1}x^{k-1} + ... + a_1x^1 + a_0$

Shamir Secret Sharing

- Wir wollen ein Geheimnis S auf n Personen aufteilen, aber man soll mindestens k dieser Personen brauchen um das Geheimnis zu berechnen.
- Idee: Funktionen vom Grad k-1 werden durch k Punkte eindeutig definiert
- Wir setzen $a_0 = S$ und wählen k-1 zufällige Zahlen $a_1 ... a_{k-1}$ und bauen daraus ein Polynom:
- $f(x) = a_{k-1}x^{k-1} + ... + a_1x^1 + a_0$
- Nun generieren wir n Wertepaare (i, f(i)), zB. mit i = 1, 2, ..., n
- Mit k dieser Paare können wir nun eindeutig das Polynom berechnen und somit f(0) = S berechnen
- Doch wie bestimmen wir das Polynom?

Shamir Secret Sharing

- Wir wollen ein Geheimnis S auf n Personen aufteilen, aber man soll mindestens k dieser Personen brauchen um das Geheimnis zu berechnen.
- Idee: Funktionen vom Grad k-1 werden durch k Punkte eindeutig definiert
- Wir setzen $a_0 = S$ und wählen k-1 zufällige Zahlen $a_1 ... a_{k-1}$ und bauen daraus ein Polynom:
- $f(x) = a_{k-1}x^{k-1} + ... + a_1x^1 + a_0$
- Nun generieren wir n Wertepaare (i, f(i)), zB. mit i = 1, 2, ..., n
- Mit k dieser Paare können wir nun eindeutig das Polynom berechnen und somit f(0) = S berechnen
- Doch wie bestimmen wir das Polynom?
- Interpolation (zB Lagrange)

Lagrange

Gegeben:

i	a	b
1	a_1	b_1
2	a_2	b_2
...	...	...
n	a_n	b_n

$$L(x) = \sum_{i=1}^{n} (b_i \cdot \frac{x - a_1}{a_i - a_1} \cdot \ldots \cdot \frac{x - a_{i-1}}{a_i - a_{i-1}} \cdot \frac{x - a_{i+1}}{a_i - a_{i+1}} \cdot \ldots \cdot \frac{x - a_n}{a_i - a_n})$$

WICHTIG: Wir können nicht teilen, sondern multiplizieren stattdessen mit dem mutiplikativen Inversen des Nenners!

Lagrange

Beispiel: $x^2 \mod 101$

i	a	b
1	1	1
2	4	16
3	7	49
4	10	100

Polynome

Polynome

Ein Polynom p über einen Körper K ist $p(x) = \sum_{i \leq 0} a_i x^i$ wobei nur endlich viele $a_i \neq 0$, $a_i \in K$.

Polynomdivision - Beispiel

$$p(1) = (3x^3 + 8x^2 + 10x + 3) : (3x - 1)$$

Polynome

Polynome

Ein Polynom p über einen Körper K ist $p(x) = \sum_{i \leq 0} a_i x^i$ wobei nur endlich viele $a_i \neq 0$, $a_i \in K$.

Polynomdivision - Beispiel

$$p(1) = (3x^3 + 8x^2 + 10x + 3) : (3x - 1)$$

$$p(1) = (x^2 + 3x + 4) + \frac{x+7}{3x-1}$$

Polynome

Polynome

Ein Polynom p über einen Körper K ist $p(x) = \sum_{i \leq 0} a_i x^i$ wobei nur endlich viele $a_i \neq 0$, $a_i \in K$.

Polynomdivision - Beispiel

$$p(1) = (3x^3 + 8x^2 + 10x + 3) : (3x - 1)$$

$p(1) = (x^2 + 3x + 4) + \frac{x+7}{3x-1}$

Generatorpolynom P = $x^4 + x^2 + x + 1$ = 10111
Nachricht N = 101010
Polynomdivision: 10101000000 : 10111

Polynome

Polynome

Ein Polynom p über einen Körper K ist $p(x) = \sum_{i \leq 0} a_i x^i$ wobei nur endlich viele $a_i \neq 0$, $a_i \in K$.

Polynomdivision - Beispiel

$$p(1) = (3x^3 + 8x^2 + 10x + 3) : (3x - 1)$$

$p(1) = (x^2 + 3x + 4) + \frac{x+7}{3x-1}$

Generatorpolynom P = $x^4 + x^2 + x + 1$ = 10111
Nachricht N = 101010
Polynomdivision: 10101000000 : 10111
Rest = 1
Codewort: 10101000001

Polynome - (Ir)reduzibilität

Irreduzible Polynome

Ein Polynom $p(x) \in K[X]$ ist irreduzibel über K, wenn $p = r \cdot q$ und $\forall r, q \in K[x]$:

$$deg(r) = 0 \vee deg(q) = 0$$

Polynome - (Ir)reduzibilität

Irreduzible Polynome

Ein Polynom $p(x) \in K[X]$ ist irreduzibel über K, wenn $p = r \cdot q$ und $\forall r, q \in K[x]$:

$$deg(r) = 0 \vee deg(q) = 0$$

- Irreduzibilität ist auf den Körper K begrenzt
  - $p(x) = x^2 + 1$ reduzibel in $\mathbb{Z}_2$, irreduzibel in $\mathbb{Z}_3$

Polynome - (Ir)reduzibilität

Irreduzible Polynome

Ein Polynom $p(x) \in K[X]$ ist irreduzibel über K, wenn $p = r \cdot q$ und $\forall r, q \in K[x]$:

$$deg(r) = 0 \vee deg(q) = 0$$

- Irreduzibilität ist auf den Körper K begrenzt
  - $p(x) = x^2 + 1$ reduzibel in $\mathbb{Z}_2$, irreduzibel in $\mathbb{Z}_3$
- Polynome von $deg(p) = 1$ sind immer irreduzibel

Polynome - (Ir)reduzibilität

Irreduzible Polynome

Ein Polynom $p(x) \in K[X]$ ist irreduzibel über K, wenn $p = r \cdot q$ und $\forall r, q \in K[x]$:

$$deg(r) = 0 \vee deg(q) = 0$$

- Irreduzibilität ist auf den Körper K begrenzt
  - $p(x) = x^2 + 1$ reduzibel in $\mathbb{Z}_2$, irreduzibel in $\mathbb{Z}_3$
- Polynome von $deg(p) = 1$ sind immer irreduzibel
- Bedeutung von irreduziblen Polynomen ist vergleichbar mit Primzahlen für natürliche Zahlen

Polynome - (Ir)reduzibilität

Irreduzible Polynome

Ein Polynom $p(x) \in K[X]$ ist irreduzibel über K, wenn $p = r \cdot q$ und $\forall r, q \in K[x]$:

$$deg(r) = 0 \vee deg(q) = 0$$

- Irreduzibilität ist auf den Körper K begrenzt
  - $p(x) = x^2 + 1$ reduzibel in $\mathbb{Z}_2$, irreduzibel in $\mathbb{Z}_3$
- Polynome von $deg(p) = 1$ sind immer irreduzibel
- Bedeutung von irreduziblen Polynomen ist vergleichbar mit Primzahlen für natürliche Zahlen
- Keine Nullstellen $\rightarrow$ keine linearen Faktoren (Hinweis auf Irreduzibilität)

Polynome - (Ir)reduzibilität

Irreduzible Polynome

Ein Polynom $p(x) \in K[X]$ ist irreduzibel über K, wenn $p = r \cdot q$ und $\forall r, q \in K[x]$:

$$deg(r) = 0 \vee deg(q) = 0$$

- Irreduzibilität ist auf den Körper K begrenzt
  - $p(x) = x^2 + 1$ reduzibel in $\mathbb{Z}_2$, irreduzibel in $\mathbb{Z}_3$
- Polynome von $deg(p) = 1$ sind immer irreduzibel
- Bedeutung von irreduziblen Polynomen ist vergleichbar mit Primzahlen für natürliche Zahlen
- Keine Nullstellen $\rightarrow$ keine linearen Faktoren (Hinweis auf Irreduzibilität)
- Aber quadratische Teilpolynome sind evtl. ein Produkt zweier Polynome

Fragen?

https://pbs.twimg.com/profile_images/472920133414158336/8MqCNSsC.jpeg