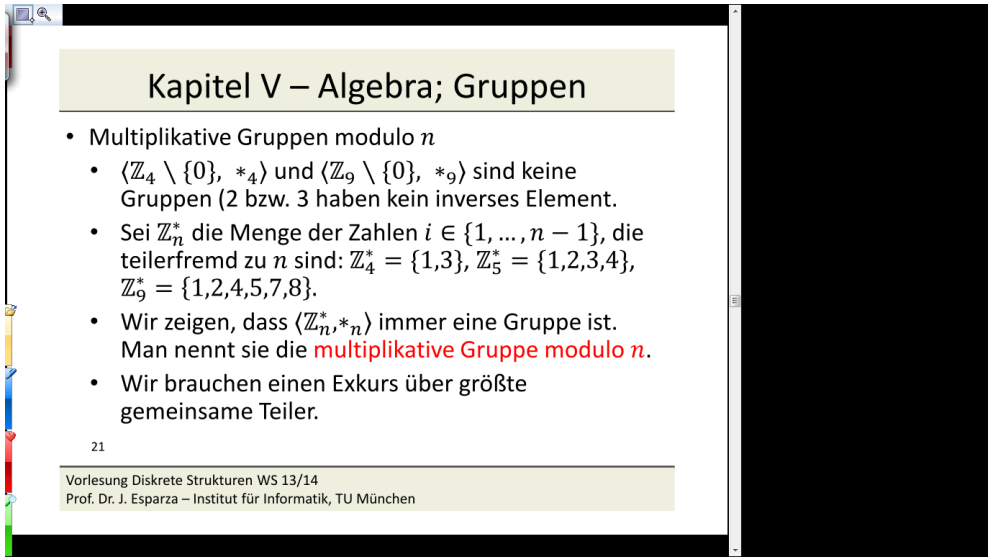
Script generated by TTT

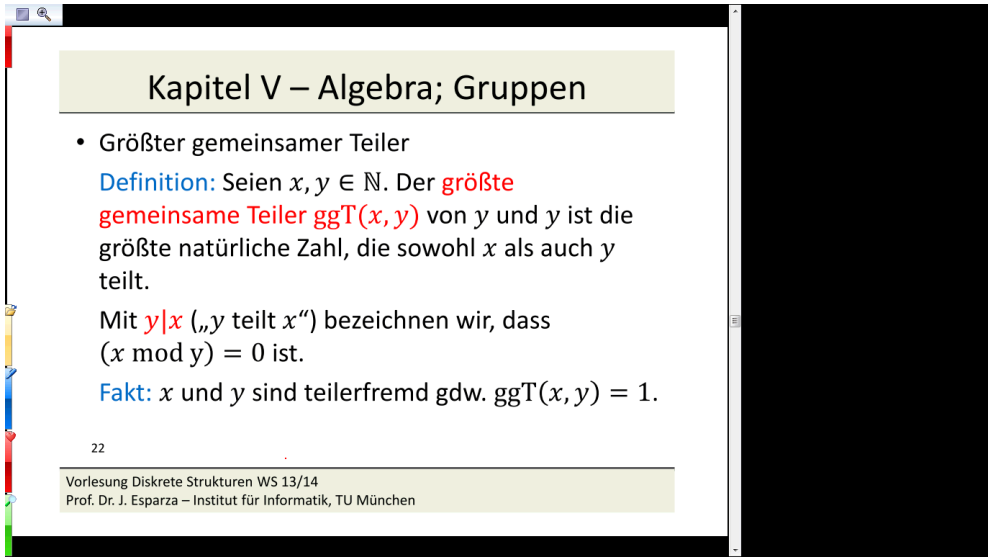
Title: Esparza: Diskrete Strukturen (04.02.2014)

Date: Tue Feb 04 13:47:09 CET 2014

Duration: 89:43 min

Pages: 29





Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

Satz: Seien $x, y \in \mathbb{N}$ mit $x \leq y$.

(1) Wenn $(y \bmod x) = 0$ dann
$\mathrm{ggT}(x, y) = x$

(2) Wenn $(y \bmod x) > 0$ dann
$\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x)$

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

Beweis: (1) Klar.

(2). Es gilt $y = (y \bmod x) + \lfloor y/x \rfloor \cdot x$.

Daraus folgt für alle $z \in \mathbb{N}$:

$(z|x \text{ und } z|y)$ gdw. $(z|x \text{ und } z|(y \bmod x))$.

(Zur Erinnerung: $z|x$ bedeutet „z teilt x“)

Damit haben (x, y) und $(x, y \bmod x)$ dieselben gemeinsamen Teiler, und so insbesondere

$\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x)$. □

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

Beweis: (1) Klar.

(2). Es gilt $y = (y \bmod x) + \lfloor y/x \rfloor \cdot x$.

Daraus folgt für alle $z \in \mathbb{N}$:

$(z|x \text{ und } z|y)$ gdw. $(z|x \text{ und } z|(y \bmod x))$.

(Zur Erinnerung: $z|x$ bedeutet „z teilt x“)

Damit haben (x, y) und $(x, y \bmod x)$ dieselben gemeinsamen Teiler, und so insbesondere

$\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x)$. □

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

Der Satz führt zum Euklidischen Algorithmus zur Berechnung vom ggT zweier Zahlen:

Procedure ggT $(x, y \in \mathbb{N}$ mit $x \leq y)$
if $(y \bmod x) = 0$ **then return** x
else return $\mathrm{ggT}(y \bmod x, x)$

(Euklid von Alexandria, ca. 325–265 v. Chr.)

- Größter gemeinsamer Teiler

Der Satz führt zum Euklidischen Algorithmus zur Berechnung vom ggT zweier Zahlen:

Procedure ggT $(x, y \in \mathbb{N}$ mit $x \leq y)$
if $(y \bmod x) = 0$ **then return** x
else return $\mathrm{ggT}(y \bmod x, x)$

(Euklid von Alexandria, ca. 325–265 v. Chr.)

- Größter gemeinsamer Teiler

Satz: Seien $x, y \in \mathbb{N}$. Es gibt $a, b \in \mathbb{Z}$ mit

$$\mathrm{ggT}(x, y) = ax + by$$

Beweis: Durch Induktion über $\max\{x, y\}$.

Basis: $\max\{x, y\} = 1$.

Dann $x = 1 = y$ und $\mathrm{ggT}(x, y) = 1 = 1 \cdot x + 0 \cdot y$.

Schritt: $\max\{x, y\} > 1$.

O.b.d.A. sei $x \leq y$. Wir betrachten zwei Fälle.

Fall 1. $(y \bmod x) = 0$. Dann $\mathrm{ggT}(x, y) = x = 1 \cdot x + 0 \cdot y$.

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

Satz: Seien $x, y \in \mathbb{N}$. Es gibt $a, b \in \mathbb{Z}$ mit

$$\mathrm{ggT}(x, y) = ax + by$$

Beweis: Durch Induktion über $\max\{x, y\}$.

Basis: $\max\{x, y\} = 1$.

Dann $x = 1 = y$ und $\mathrm{ggT}(x, y) = 1 = 1 \cdot x + 0 \cdot y$.

Schritt: $\max\{x, y\} > 1$.

O.b.d.A. sei $x \leq y$. Wir betrachten zwei Fälle.

Fall 1. $(y \bmod x) = 0$. Dann $\mathrm{ggT}(x, y) = x = 1 \cdot x + 0 \cdot y$.

26

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

- Größter gemeinsamer Teiler

Fall 2. $(y \bmod x) > 0$. In diesem Fall gelten $x < y$ und $\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x)$. Wir haben

$$\max\{x, y \bmod x\} = x < y \leq \max\{x, y\}$$

und so (Induktionsannahme) gibt es $a', b' \in \mathbb{Z}$ mit

$$\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x) = a'(y \bmod x) + b'x$$

Mit $y \bmod x = y - \lfloor y/x \rfloor \cdot x$ erhalten wir

$$\begin{aligned} \mathrm{ggT}(x, y) &= a'(y - \lfloor y/x \rfloor \cdot x) + b'x \\ &= (b' - \lfloor y/x \rfloor a')\, x + a'y \end{aligned}$$ □

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

  Der Beweis des Satzes führt zu einem Algorithmus für die Berechnung der Zahlen a und b, dem Erweiterten Euklidischen Algorithmus:

Procedure ErwggT($x, y \in \mathbb{N}$ mit $x \leq y$)
  if $(y \bmod x) = 0$ **then return** $(1, 0)$
  else $(a', b') :=$ ErwggT($y \bmod x, x$);
    $(a, b) := (b' - \lfloor y/x \rfloor a',\ a')$;
    return (a, b)

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

  Beispiel mit $x = 45, y = 63$.

$$\begin{aligned}
&\text{ggT}(45,63) && 9 = \big(1 - \lfloor 63/45 \rfloor \cdot (-2)\big) \cdot 45 + (-2) \cdot 63 \\
&= && = 3 \cdot 45 + (-2) \cdot 63 \\
&\text{ggT}(18,45) && 9 = \big(0 - \lfloor 45/18 \rfloor \cdot 1\big) \cdot 18 + 1 \cdot 45 \\
&= && = -2 \cdot 18 + 1 \cdot 45 \\
&\text{ggT}(\ 9,18) && 9 = 1 \cdot 9 + 0 \cdot 18 \\
&= \\
&9
\end{aligned}$$

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

  Der Beweis des Satzes führt zu einem Algorithmus für die Berechnung der Zahlen a und b, dem Erweiterten Euklidischen Algorithmus:

Procedure ErwggT($x, y \in \mathbb{N}$ mit $x \leq y$)
  if $(y \bmod x) = 0$ **then return** $(1, 0)$
  else $(a', b') :=$ ErwggT($y \bmod x, x$);
    $(a, b) := (b' - \lfloor y/x \rfloor a',\ a')$;
    return (a, b)

ggT(x,y) = ax + by

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

  Beispiel mit $x = 45, y = 63$.

$$\begin{aligned}
&\text{ggT}(45,63) && 9 = \big(1 - \lfloor 63/45 \rfloor \cdot (-2)\big) \cdot 45 + (-2) \cdot 63 \\
&= && = 3 \cdot 45 + (-2) \cdot 63 \\
&\text{ggT}(18,45) && 9 = \big(0 - \lfloor 45/18 \rfloor \cdot 1\big) \cdot 18 + 1 \cdot 45 \\
&= && = -2 \cdot 18 + 1 \cdot 45 \\
&\text{ggT}(\ 9,18) && 9 = 1 \cdot 9 + 0 \cdot 18 \\
&= \\
&9
\end{aligned}$$

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebra; Gruppen

- Multiplikative Gruppen modulo n

  Satz: $\langle \mathbb{Z}_n^*, *_n \rangle$ ist eine Gruppe für alle $n \geq 1$.

  Beweis: Wir zeigen, dass jedes $x \in \mathbb{Z}_n^*$ ein inverses Element hat.

  Sei $x \in \mathbb{Z}_n^*$ beliebig. Es gilt $\mathrm{ggT}(x, n) = 1$.

  Der ErwggT berechnet $a, b \in \mathbb{Z}$ mit $ax + bn = 1$.

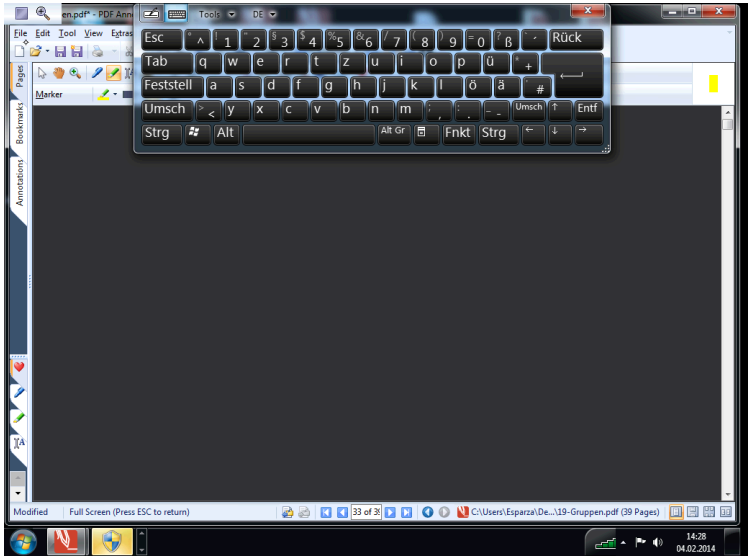
  Es gilt also $a *_n x +_n b *_n n = 1$.

  Aus $(b *_n n) = 0$ folgt $(a *_n x) = 1$.

  Wähle $x^{-1} := a \bmod n$. □

Kapitel V – Algebra; Gruppen

- Multiplikative Gruppen modulo n
- Korollar: Sei $\varphi(n) = |\mathbb{Z}_n^*|$. Ist n Primzahl, dann gilt $\varphi(n) = n - 1$.



Kapitel V – Algebraische Strukturen

- Asymmetrische Kryptosysteme (public key):
  - Jeder Teilnehmer hat zwei Schlüssel: einen geheimen Schlüssel (private key) und einen öffentlichen Schlüssel (public key).
  - Die öffentlichen Schlüssel werden in einem öffentlichen „Schlüsselverzeichnis“ veröffentlicht (vgl. Telefonbuch).
  - Eine Nachricht von A an B wird von A mit Hilfe des öffentlichen Schlüssels von B verschlüsselt.
  - Die Entschlüsselung einer chiffrierten Nachricht erfolgt mit dem privaten Schlüssel von B.

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem
  - Das populärste asymmetrische Kryptosystem.
  - Benannt nach Rivest, Shamir, und Adleman (ähnliche Methode von Cocks wurde geheim gehalten).
  - Die Schlüssel sind (sehr) große Zahlen.
  - Die Verfahren für Ver- und Entschlüsselung basieren auf Zahlentheorie.

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Schlüssel
  - Jeder Teilnehmer erzeugt zwei große Primzahlen p und q und setzt $n = pq$.
  - Sei $\phi := |\mathbb{Z}_n^*| = (p-1)(q-1)$
  - Die Teilnehmer wählen $c \in \mathbb{Z}_\phi^*$ und berechnen $d := c^{-1}$, das inverse Element von c in $\langle \mathbb{Z}_\phi^*, *_\phi \rangle$.

    (d kann mit dem Erweiterten Euklidischen Algorithmus berechnet werden).
  - Öffentlicher Schlüssel: (n, c)
  - Privater Schlüssel: d

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Verschlüsseln (Vereinfacht!)

  Um eine chiffrierte Nachricht an einen Teilnehmer B mit öffentlichem Schlüssel (n, c) zu senden:

  1. Zerlege die Nachricht so in Blöcke, dass jeder Block durch eine Zahl $m < n$ dargestellt werden kann (e.g. ASCII codes).
  2. Berechne für jeden Block das Element $x = m^c$ in der Gruppe $\mathbb{Z}_n^*$. Die Chiffrierung des Blocks ist die Zahl x.
  3. Schicke die Chiffrierungen x_1, x_2, x_3 … der Blöcke an B.

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Entschlüsseln

  Um eine chiffrierte Nachricht, die an einen Teilnehmer B mit öffentlichem Schlüssel (n, c) und privatem Schlüssel d geschickt wurde, zu entschlüsseln:

  1. Berechne die Elemente x^d von $\mathbb{Z}_n^*$ für $x = x_1, x_2, x_3$.
  2. Diese Zahlen sind garantiert die Darstellungen m der Blöcke. Gewinne aus ihnen die Nachricht zurück.

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Verschlüsseln (Vereinfacht!)

  Um eine chiffrierte Nachricht an einen Teilnehmer B mit öffentlichem Schlüssel (n, c) zu senden:

  1. Zerlege die Nachricht so in Blöcke, dass jeder Block durch eine Zahl $m < n$ dargestellt werden kann (e.g. ASCII codes).
  2. Berechne für jeden Block das Element $x = m^c$ in der Gruppe $\mathbb{Z}_n^*$. Die Chiffrierung des Blocks ist die Zahl x.
  3. Schicke die Chiffrierungen x_1, x_2, x_3 … der Blöcke an B.

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Entschlüsseln

  Um eine chiffrierte Nachricht, die an einen Teilnehmer B mit öffentlichem Schlüssel (n, c) und privatem Schlüssel d geschickt wurde, zu entschlüsseln:

  1. Berechne die Elemente x^d von $\mathbb{Z}_n^*$ für $x = x_1, x_2, x_3$.
  2. Diese Zahlen sind garantiert die Darstellungen m der Blöcke. Gewinne aus ihnen die Nachricht zurück.

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Beispiel (aus Wikipedia)
  - $p = 61,\ q = 53$
  - $n = 61 \cdot 53 = 3233$
  - $\phi = 60 \cdot 52 = 3120$
  - Wähle $c = 17,\ d = 2753$
    - Es gilt $cd = 46801 = 1 + 15 \cdot 3120 = 1 + k\,\phi$
  - Öffentlicher Schlüssel: $(3233, 17)$
  - Privater Schlüssel: 2753

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Beispiel (aus Wikipedia)
  - $p = 61,\ q = 53$
  - $n = 61 \cdot 53 = 3233$
  - $\phi = 60 \cdot 52 = 3120$
  - Wähle $c = 17,\ d = 2753$
    - Es gilt $cd = 46801 = 1 + 15 \cdot 3120 = 1 + k\,\phi$
  - Öffentlicher Schlüssel: $(3233, 17)$
  - Privater Schlüssel: 2753

9

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Warum funktioniert es?
  - Wir haben $x^d = (m^c)^d = m^{cd}$
  - Wegen $cd \equiv 1 \bmod \phi$ gibt es k mit
    $$cd = 1 + k\phi$$
  - Es folgt $m^{cd} = m^{1+k\phi} = m(m^\phi)^k$ und mit dem Lemma von Euler
    $$x^d = m^{cd} = m(m^\phi)^k \equiv m \bmod n$$

(Bemerkung: Der Satz von Euler beweist Korrektheit von RSA nur für $m \in \mathbb{Z}_n^*$. Ein anderes, ähnliches Argument zeigt sie auch für $m \equiv 0 \bmod p$ und $m \equiv 0 \bmod q$.)

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Ist es sicher?
  - Keine Garantie!
  - Bisher kein effizientes Verfahren bekannt, welches aus dem öffentlichen Schlüssel (n, c) den privaten Schlüssel d berechnet.
  - Wenn man p und q kennt, dann kann d effizient berechnet werden. Für die Faktorisierung der Zahl n ist jedoch kein effizientes Verfahren bekannt. (Es existiert jedoch ein polynomielles Verfahren für hypotetischen Quantenrechner.)