

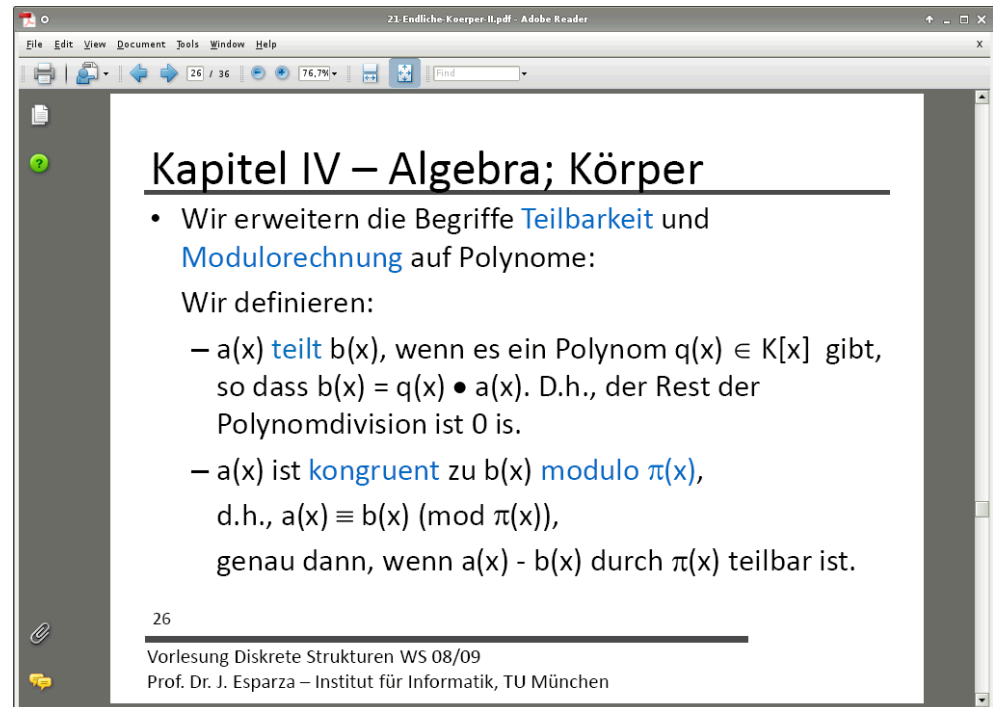
Script generated by TTT

Title: Esparza: Diskrete Strukturen (03.02.2009)

Date: Tue Feb 03 14:05:32 CET 2009

Duration: 73:50 min

Pages: 27



21-Endliche-Koerper-II.pdf - Adobe Reader

Kapitel IV – Algebra; Körper

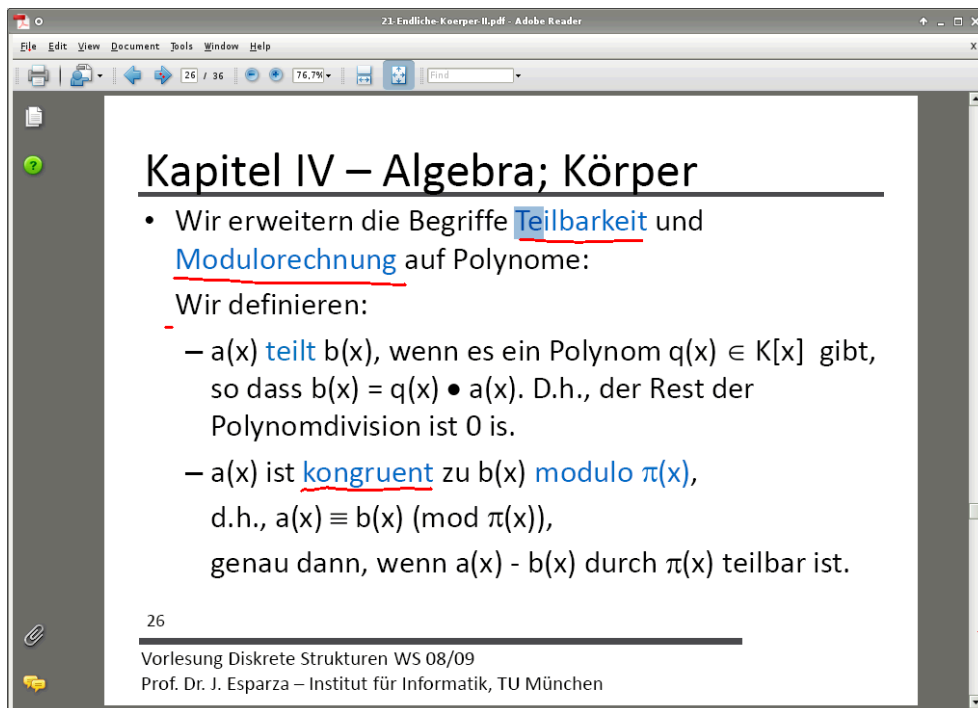
- Wir erweitern die Begriffe **Teilbarkeit** und **Modulorechnung** auf Polynome:

Wir definieren:

- $a(x)$ **teilt** $b(x)$, wenn es ein Polynom $q(x) \in K[x]$ gibt, so dass $b(x) = q(x) \cdot a(x)$. D.h., der Rest der Polynomdivision ist 0 ist.
- $a(x)$ ist **kongruent** zu $b(x)$ **modulo** $\pi(x)$, d.h., $a(x) \equiv b(x) \pmod{\pi(x)}$, genau dann, wenn $a(x) - b(x)$ durch $\pi(x)$ teilbar ist.

26

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München



21-Endliche-Koerper-II.pdf - Adobe Reader

Kapitel IV – Algebra; Körper

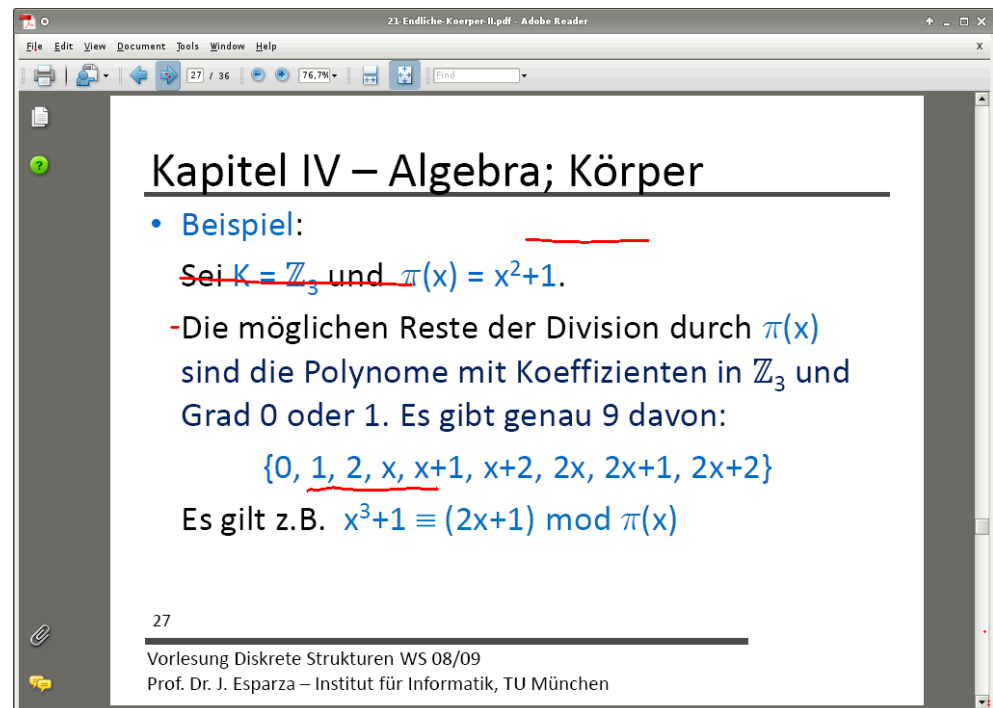
- Wir erweitern die Begriffe **Teilbarkeit** und **Modulorechnung** auf Polynome:

Wir definieren:

- $a(x)$ **teilt** $b(x)$, wenn es ein Polynom $q(x) \in K[x]$ gibt, so dass $b(x) = q(x) \cdot a(x)$. D.h., der Rest der Polynomdivision ist 0 ist.
- $a(x)$ ist **kongruent** zu $b(x)$ **modulo** $\pi(x)$, d.h., $a(x) \equiv b(x) \pmod{\pi(x)}$, genau dann, wenn $a(x) - b(x)$ durch $\pi(x)$ teilbar ist.

26

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München



21-Endliche-Koerper-II.pdf - Adobe Reader

Kapitel IV – Algebra; Körper

- Beispiel:**
~~Sei $K = \mathbb{Z}_3$ und $\pi(x) = x^2 + 1$.~~
- Die möglichen Reste der Division durch $\pi(x)$ sind die Polynome mit Koeffizienten in \mathbb{Z}_3 und Grad 0 oder 1. Es gibt genau 9 davon:
 $\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$

Es gilt z.B. $x^3 + 1 \equiv (2x + 1) \pmod{\pi(x)}$

27

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

21-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

28 / 36 76.7%

Click to go to the next page in the document

Kapitel IV – Algebra; Körper $\pi(x)$ \odot

- Die Kongruenzrelation teilt die Menge $K[x]$ in Äquivalenzklassen:

$$K[x]_{\pi(x)} := \{f(x) \mid f(x) \in K[x], \text{grad}(f) < \text{grad}(\pi)\}.$$

- Wenn K endlich ist, dann ist $K[x]_{\pi(x)}$ auch endlich.
- Es gilt dann $\langle K[x]_{\pi(x)}, +_{\pi(x)}, \cdot_{\pi(x)} \rangle$

$$f(x) +_{\pi(x)} g(x) := (f(x) + g(x)) \bmod \pi(x)$$

$$f(x) \cdot_{\pi(x)} g(x) := (f(x) \cdot g(x)) \bmod \pi(x)$$

28

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

21-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

28 / 36 76.7%

Click to go to the next page in the document

Kapitel IV – Algebra; Körper

- Die Kongruenzrelation teilt die Menge $K[x]$ in Äquivalenzklassen:

$$K[x]_{\pi(x)} := \{f(x) \mid f(x) \in K[x], \text{grad}(f) < \text{grad}(\pi)\}.$$

- Wenn K endlich ist, dann ist $K[x]_{\pi(x)}$ auch endlich.
- Es gilt dann

$$f(x) +_{\pi(x)} g(x) := (f(x) + g(x)) \bmod \pi(x)$$

$$f(x) \cdot_{\pi(x)} g(x) := (f(x) \cdot g(x)) \bmod \pi(x)$$

28

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

21-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

29 / 36 76.7%

Click to go to the next page in the document

Kapitel IV – Algebra; Körper

- Wir haben bewiesen $\langle \mathbb{Z}_n[x], +_n, \cdot_n \rangle$ ist Körper $\Leftrightarrow n$ ist Primzahl
- Frage: Wann ist $\langle K[x]_{\pi(x)}, +_{\pi(x)}, \cdot_{\pi(x)} \rangle$ ein Körper?
- Antwort (ohne Beweis): $\langle \mathbb{Z}_n[x], +_n, \cdot_n \rangle$ ist Körper $\Leftrightarrow \pi(x)$ ist irreduzibel
- Definition:

Ein Polynom $\pi(x) \in K[x]$ mit $\pi(x) \neq 0$ heißt irreduzibel (über K), falls für alle $f(x), g(x) \in K[x]$ gilt:

$$\pi(x) = f(x) \cdot g(x) \Rightarrow \text{grad}(f) = 0 \text{ oder } \text{grad}(g) = 0.$$

29

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

21-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

30 / 36 76.7%

Click to go to the next page in the document

Kapitel IV – Algebra; Körper

- Beispiel:

Betrachten wir $K = \mathbb{Z}_2$ und $\pi(x) = x^2 + x + 1$.

$\mathbb{Z}_2[x]_{\pi(x)}$ besteht aus allen Polynomen in $\mathbb{Z}_2[x]$ mit Grad 0 oder 1: $\mathbb{Z}_2[x]_{\pi(x)} = \{0, 1, x, x+1\}$

Die Multiplikationstabellen sehen wie folgt aus:

$+_{\pi(x)}$	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$\cdot_{\pi(x)}$	0	1	x	x+1
0	0	0	0	0
1	1	1	x	x+1
x	x	x	x+1	1
x+1	x+1	x+1	1	x

30

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

21-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

31 / 36 76.7%

Kapitel IV – Algebra; Körper

- **Beispiel:**
Betrachten wir $K = \mathbb{Z}_2$ und $\pi(x) = x^2+1$.

→ $\mathbb{Z}_2[x]_{\pi(x)}$ besteht aus allen Polynomen in $\mathbb{Z}_2[x]$ mit Grad 0 oder 1: $\mathbb{Z}_2[x]_{\pi(x)} = \{0, 1, x, x+1\}$

Die Multiplikationstabellen sehen wie folgt aus:

$+\pi(x)$	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$\cdot_{\pi(x)}$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	1	x+1
x+1	0	x+1	x+1	0

31 Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

$$\begin{array}{r} x + 1 \\ + x + 1 \\ \hline 0 \end{array}$$

21-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

30 / 36 76.7%

Kapitel IV – Algebra; Körper

- **Beispiel:**
Betrachten wir $K = \mathbb{Z}_2$ und $\pi(x) = x^2+x+1$.

→ $\mathbb{Z}_2[x]_{\pi(x)}$ besteht aus allen Polynomen in $\mathbb{Z}_2[x]$ mit Grad 0 oder 1: $\mathbb{Z}_2[x]_{\pi(x)} = \{0, 1, x, x+1\}$

Die Multiplikationstabellen sehen wie folgt aus:

*x^2+x div x^2+x+1
 $-(x^2+x+1)$
 $\quad \quad \quad 1$*

$+\pi(x)$	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$\cdot_{\pi(x)}$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

30 Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

21-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

31 / 36 76.7%

Kapitel IV – Algebra; Körper

- **Beispiel:**
Betrachten wir $K = \mathbb{Z}_2$ und $\pi(x) = x^2+1$.

$\mathbb{Z}_2[x]_{\pi(x)}$ besteht aus allen Polynomen in $\mathbb{Z}_2[x]$ mit Grad 0 oder 1: $\mathbb{Z}_2[x]_{\pi(x)} = \{0, 1, x, x+1\}$

Die Multiplikationstabellen sehen wie folgt aus:

$0 \cdot (x^2+1) \equiv (x+1) \cdot (x+1)$ $\text{mod } x^2+1$

$+\pi(x)$	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$\cdot_{\pi(x)}$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	1	x+1
x+1	0	x+1	x+1	0

31 Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

$$\begin{array}{r} x + 1 \\ + x + 1 \\ \hline 0 \end{array}$$

$x \cdot x + 1$ mod $x^2 + 1$

||

$$\begin{array}{r} x^2 + x \\ - (x^2 + 1) \\ \hline x + 1 \end{array}$$

$0 \cdot (x^2 + 1) = (x + 1) \cdot (x + 1)$

Kapitel IV – Algebra; Körper

- Beispiel:** $x^2 + \cancel{x} + 1$

Betrachten wir $K = \mathbb{Z}_2$ und $\pi(x) = x^2 + 1$.

$\mathbb{Z}_2[x]_{\pi(x)}$ besteht aus allen Polynomen in $\mathbb{Z}_2[x]$ mit Grad 0 oder 1: $\mathbb{Z}_2[x]_{\pi(x)} = \{0, 1, x, x+1\}$

Die Multiplikationstabellen sehen wie folgt aus:

$+\pi(x)$	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$\cdot\pi(x)$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	1	x+1
x+1	0	x+1	x+1	0

31 Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

$0 \cdot (x^2 + 1) = (x + 1) \cdot (x + 1)$

Kapitel IV – Algebra; Körper

- Der Grund, warum $K = \mathbb{Z}_2$ für $\pi_1(x) = x^2 + 1$ die Gruppeneigenschaften nicht erfüllt, ist dass $\pi_1(x)$ **reduzibel** über K ist.

D.h., dass $\pi_1(x)$ als Produkt zweier Polynome vom Grad größer gleich 1 schreiben lässt:

$$\pi_1(x) = x^2 + 1 = (x + 1) \cdot (x + 1) \text{ (in } \mathbb{Z}_2)$$

Dies ist für $x^2 + x + 1$ nicht der Fall.

32

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel IV – Algebra; Körper

- Der Grund, warum $K = \mathbb{Z}_2$ für $\pi_1(x) = x^2 + 1$ die Gruppeneigenschaften nicht erfüllt, ist dass $\pi_1(x)$ **reduzibel** über K ist.

D.h., dass $\pi_1(x)$ als Produkt zweier Polynome vom Grad größer gleich 1 schreiben lässt:

$$\pi_1(x) = x^2 + 1 = (x + 1) \cdot (x + 1) \text{ (in } \mathbb{Z}_2)$$

Dies ist für $x^2 + x + 1$ nicht der Fall.

32

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

23-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

33 / 36 76.7%

Kapitel IV – Algebra; Körper

Satz:
Ist K ein endlicher Körper und $\pi(x)$ ein Polynom in $K[x]$. Dann gilt:

$\langle K[x]_{\pi(x)}, +_{\pi(x)}, \cdot_{\pi(x)} \rangle$ ist ein Körper

$\Leftrightarrow \Rightarrow$

$\pi(x)$ ist irreduzibel über $K[x]$.

33

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

23-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

34 / 36 76.7%

Kapitel IV – Algebra; Körper

- Eigenschaften von Restklassenringen
- Satz:**
Sei K ein Körper mit n Elementen, und sei $g \in K[x]$, $d = \text{grad}(g) \geq 1$.
Dann besitzt $K[x]_g$ genau n^d Elemente.

0 1 2 ... d-1
n n n ... n

34

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

23-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

35 / 36 76.7%

Kapitel IV – Algebra; Körper

- Satz:**
Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es einen **endlichen Körper** mit **p^n Elementen**; dieser wird mit **$GF(p^n)$** bezeichnet (GF = Galois Field, nach Evariste Galois (1811–1832))).

0 1 2 ... d-1
n n n ... n

35

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

23-Endliche-Koerper-II.pdf - Adobe Reader

File Edit View Document Tools Window Help

35 / 36 76.7%

Kapitel IV – Algebra; Körper

- Satz:**
Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es einen **endlichen Körper** mit **p^n Elementen**; dieser wird mit **$GF(p^n)$** bezeichnet (GF = Galois Field, nach Evariste Galois (1811–1832))).

$p(x) = 0$ $x+1 = 0$
 $x^2 - 2x + 4 = 0$
 $\rightarrow x^3 - 2x^2 + 5x - 3 = 0$
 $x^4 -$

35

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

$$\begin{array}{r} x + 1 \\ + x + 1 \\ \hline 0 \end{array}$$

$$\begin{array}{r} x \cdot x + 1 \text{ mod } x^2 + 1 \\ \parallel \\ x^2 + x \text{ div } x^2 + 1 \\ - (x^2 + 1) \quad 1 \\ \hline x + 1 \end{array}$$

23-Endliche-Koerper-II.pdf - Adobe Reader

$ax^2 + bx + c = 0$

Kapitel IV – Algebra; Körper

- Satz: $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es einen **endlichen Körper** mit p^n **Elementen**; dieser wird mit $GF(p^n)$ bezeichnet (GF = Galois Field, nach Evariste Galois (1811–1832)).

35

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

23-Endliche-Koerper-II.pdf - Adobe Reader

Kapitel IV – Algebra; Körper

- Beweis:

$n = 1$: $\mathbb{Z}_p = GF(p)$ ist ein Körper mit p Elementen.

$n > 1$: Sei $K = \mathbb{Z}_p$. Sei $g \in K[x]$ ein irreduzibles Polynom vom Grad n .

Dann ist $K[x]_g$ ein Körper, und hat genau p^n Elemente (siehe Satz auf Seite 33).

$p(x) = 0$

$x^2 - 2x + 4 = 0$

$\rightarrow x^3 - 2x^2 + 5x - 3 = 0$

$x^4 -$

36

Vorlesung Diskrete Strukturen WS 08/09
Prof. Dr. J. Esparza – Institut für Informatik, TU München

$$ax^2 + bx + c = 0$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

RSA public key cryptography

public private

$$n = p \cdot q$$

$$\varphi(n) = (p-1) \cdot (q-1)$$

$$e: 1 < e < \varphi(n)$$

$$\text{ggT}(e, \varphi(n)) = 1 \rightarrow \text{Euklid}$$

$$d: d \cdot e \equiv 1 \pmod{\varphi(n)}$$

$$1 \dots n$$

$$\frac{n}{\text{Wahl}}$$

$$10^{12}$$

$$\frac{a \cdot e + b \cdot \varphi(n)}{1} \equiv 1 \pmod{10^2 \text{ (open)}}$$

Wenn funktioniert es?

n, e, d

$$c^d \equiv (m^e)^d \pmod{n}$$

$$\equiv m^{ed} \pmod{n}$$

$$ed = 1 + k \cdot \varphi(n) \text{ für ein } k$$

$$\equiv m^{1+k \cdot \varphi(n)} \pmod{n}$$

$$\equiv m \cdot \frac{(m^k)^{\varphi(n)}}{1} \pmod{n}$$

$$\equiv m$$

Öffentlicher Schlüssel

n, e

Privater Schlüssel

d

Chiffrieren einer Nachricht M

$$1) \underline{M} \rightsquigarrow \underline{m} < n$$

$$2) \underline{c} \equiv \underline{m}^e \pmod{n}$$

Dechiffrieren

$$3) \underline{c}^d \equiv \underline{m} \pmod{n}$$

$$4) \underline{m} \rightsquigarrow M$$

$p = 61$ $q = 53$ $n = 61 \cdot 53 = 3233$ $m_1 = m^2 \pmod{3233}$
 $\varphi(n) = 3120$ $m_2 = m_1 \cdot m_1 \pmod{3233}$
Kapitel IV – Algebra; Körper
 • Beweis: $d \cdot e \equiv 1 \pmod{\varphi(n)}$
 $n = 1: \mathbb{Z}_p = \text{GF}(p)$ ist ein Körper mit p Elementen
 $n > 1:$ Sei $K = \mathbb{Z}_p$. Sei $g \in K[x]$ ein irreduzibles Polynom von Grad $n = 17$
 Dann ist $K[x]_g$ ein Körper, und hat genau p^n Elemente (siehe Satz auf Seite 33).
 Sei $m = 123$ $m_1 = 123 \cdot 123 \pmod{3233}$
 $c = 123^{17} \pmod{3233} = 855$
 $855^{2753} \pmod{3233} = 123$
 Vorlesung Diskrete Strukturen, WS 08/09
 Prof. Dr. J. Espartero – Institut für Informatik, TU München