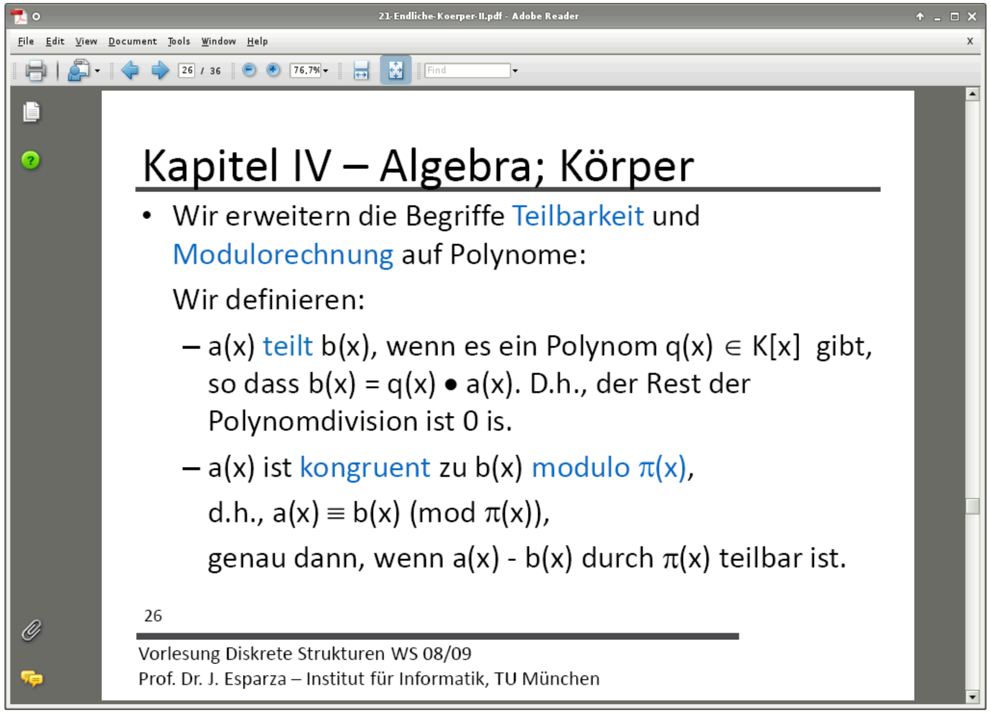
**Script** generated by TTT

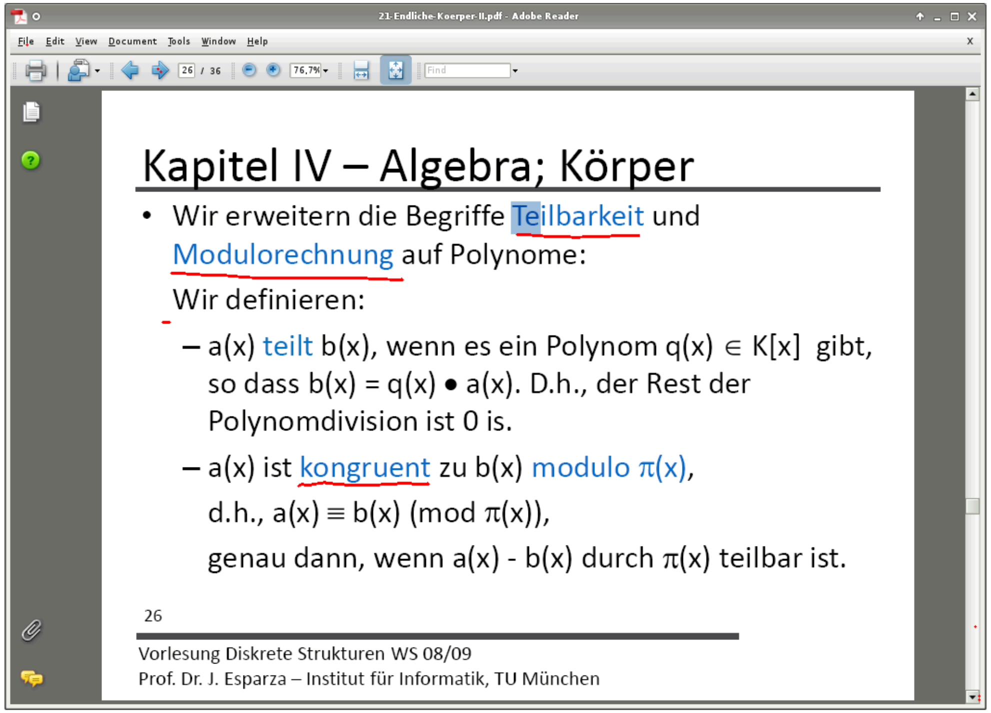
Title: Esparza: Diskrete Strukturen (03.02.2009)

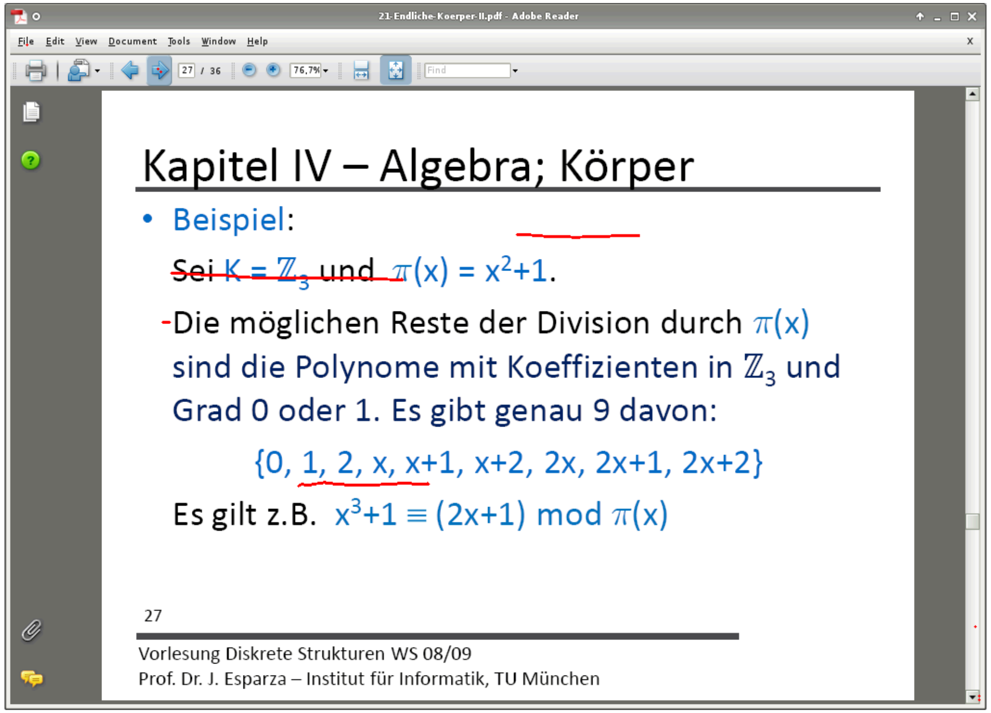
Date: Tue Feb 03 14:05:32 CET 2009

Duration: 73:50 min

Pages: 27



# Kapitel IV – Algebra; Körper

$\pi(x)$

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

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

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

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

  $f(x) \bullet_{\pi(x)} g(x) := (f(x) \bullet g(x)) \bmod \pi(x)$



Click to go to the next page in the document

# Kapitel IV – Algebra; Körper

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

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

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

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

  $f(x) \bullet_{\pi(x)} g(x) := (f(x) \bullet g(x)) \bmod \pi(x)$

28

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

Click to go to the next page in the document

# Kapitel IV – Algebra; Körper

- Wir haben bewiesen

  $\langle \mathbb{Z}_n[x], +_n, \bullet_n \rangle$ ist Körper $\Leftrightarrow$ n ist Primzahl

- Frage: Wann ist $\langle K[x]_{\pi(x)}, +_{\pi(x)}, \bullet_{\pi(x)} \rangle$ ein Körper?
- Antwort (ohne Beweis):

  $\langle \mathbb{Z}_n[x], +_n, \bullet_n \rangle$ 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:

  $(x^2+2x+1) = (x+1)(x+1)$

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



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 |

| $\bullet_{\pi(x)}$ | 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 |

# 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 |

| $\bullet_{\pi(x)}$ | 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 |





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



$x^2+x$ div $x^2+x+1$
$-(x^2+x+1)$
$-1$ 1

# 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 |

| $\bullet_{\pi(x)}$ | 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 |







$0 \; (x^2+1) \equiv (x+1)\cdot(x+1)$ mod

# Kapitel IV – Algebra; Körper

$x^2 + \cancel{2x} + 1$

- 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 |

| $\bullet_{\pi(x)}$ | 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 |

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

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

$=$

$x^2 + x$ div $x^2+1$

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

$x+1$



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

# Kapitel IV – Algebra; Körper

$x^2 + \cancel{2x} + 1$

- **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 |

| $\bullet_{\pi(x)}$ | 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 |





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

# 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:

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

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



21-Endliche-Koerper-II.pdf - Adobe Reader
File Edit View Document Tools Window Help
32 / 36 76,7%

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:

$\pi_1(x) = x^2+1 = (x+1)\bullet(x+1)$ (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

Satz:

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

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

$$\Leftrightarrow \qquad \Rightarrow$$

$$\pi(x) \text{ ist irreduzibel über } K[x].$$





# 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 $\boxed{n^d}$ Elemente.

0 1 2 ... d-1

n n n ... n





# 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





# 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)).

$p(x) = 0$

$x + 1 = 0$

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

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

$x^4 -$

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

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

$=$

$x^2 + \cancel{x} \quad \text{div} \quad x^2 + 1 = 1$

$-(x^2 + 1)$

$x + 1$

$ax^2 + bx + c = 0$

# Kapitel IV – Algebra; Körper

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

  Zu jeder Primzahl p und zu jeder natürlichen Zahl n ≥ 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)).



# 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 ∈ 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).

$x + 1 = 0$

$p(x) = 0$

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

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

$x^4 -$



$ax^2 + bx + c = 0$

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

RSA public key cryptography

public private

$\boxed{n} = \boxed{p \cdot q}$ $1 \, . \, . \, —— \, n$

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

$n$

$\log n$

$10^{12}$

$\boxed{e}$: $1 < e < \varphi(n)$

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

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

$\underbrace{a}_{1} e + \underbrace{b \varphi(n)}_{0} = 1 \mod \varphi(n)$ $10^{12}$

Öffentlicher Schlüssel $n, e$

Privater Schlüssel $d$

Chiffrieren einer Nachricht $M$

1) $M \rightsquigarrow m < n$

2) $c \equiv m^e \pmod n$

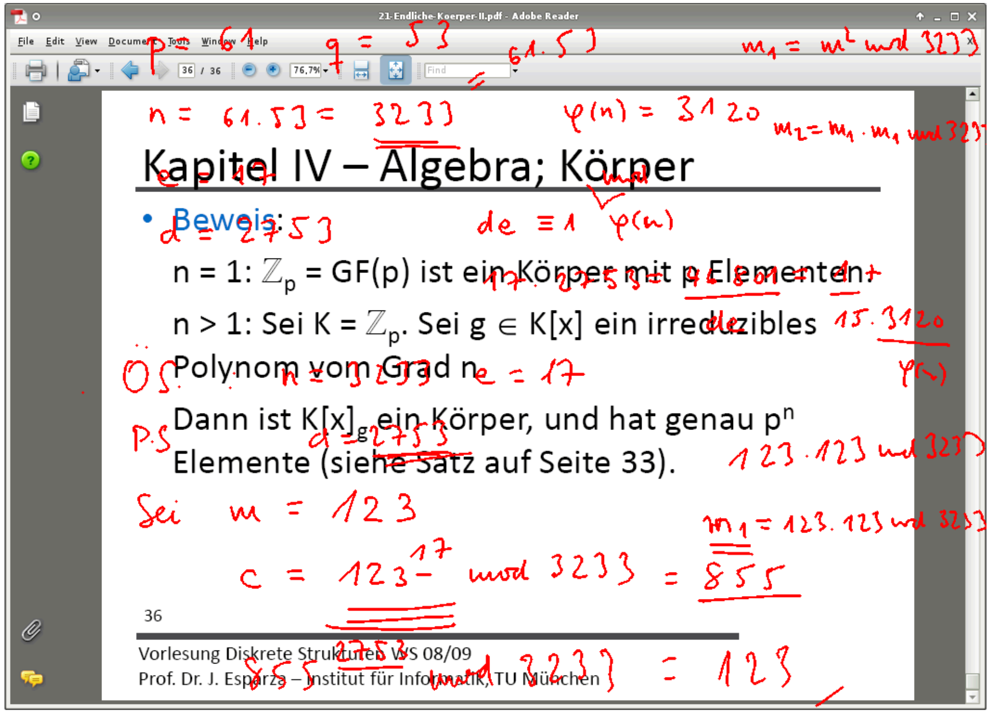
Dechiffrieren

3) $c^d \equiv m \pmod n$

4) $m \rightsquigarrow M$

Wann funktioniert es? $n \; e$ $d$

$$c^d \equiv (m^e)^d \mod n$$
$$\equiv m^{ed} \mod n$$
$$ed = 1 + k\,\varphi(n) \text{ für ein } k$$
$$\equiv m^{1+k\varphi(n)} \mod n$$
$$\equiv m \underbrace{(m^k)^{\varphi(n)}}_{\equiv 1} \mod n$$
$$\overset{?}{\equiv} m$$




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).



$p = 61$ $q = 53$ $61 \cdot 53$

$n = 61 \cdot 53 = 3233$ $\varphi(n) = 3120$

$e = 17$

$d = 2753$ $de \equiv 1 \mod \varphi(n)$

$17 \cdot 2753 = 1 + 15 \cdot 3120$

ÖS $n = 3233$ $e = 17$

P.S $d = 2753$

Sei $m = 123$

$c = 123^{17} \mod 3233 = 855$

$855^{2753} \mod 3233 = 123$

$m_1 = m^2 \mod 3233$

$m_2 = m_1 \cdot m_1 \mod 3233$

$123 \cdot 123 \mod 3233$

$m_1 = 123 \cdot 123 \mod 3233$