
Fortgeschrittene Techniken der Kryptographie

Jürgen Fuß

Episode 13: Polynombasierende Verfahren

HAGENBERG | LINZ | STEYR | WELS



UNIVERSITY
OF APPLIED SCIENCES
UPPER AUSTRIA

Polynome und Restklassen

Irreduzible Polynome

Für das Folgende soll K ein beliebiger Körper sein, wie immer also wieder \mathbb{R} oder \mathbb{Z}_p . Wie in \mathbb{Z} gibt es auch in $K[x]$ Elemente, die sich in Produkte zerlegen lassen und andere, die dies nicht erlauben.

Definition

Ein Polynom $f \in K[x]$ heißt **reduzibel**, wenn es Polynome g und h gibt, so dass $p = g \cdot h$ und die Grade der Polynome g und h kleiner sind als der Grad von f .

Andernfalls heißt f **irreduzibel**.

Die irreduziblen Polynome sind sozusagen die Primzahlen in $K[x]$. Wie in \mathbb{Z} ist auch in $K[x]$ eine eindeutige Primfaktorzerlegung möglich.

Restklassen von Polynomen

Wir definieren (für $f, g, h \in K[x]$):

$$\underbrace{g = h} \pmod{f} \text{ genau dann, wenn } f \mid \underbrace{g - h} \quad (1)$$

Für die Menge der Restklassen modulo f schreiben wir $K[x]/(f)$.

Satz

Ist K ein Körper und f ein irreduzibles Polynom in $K[x]$, dann ist $K[x]/(f)$ ein Körper.

Beispiel: Addition in $\mathbb{R}[x]/(x^2 + 1)$

Polynome mit reellen Koeff.

Wir rechnen in $\mathbb{R}[x]/(x^2 + 1)$.

Restklassen modulo $x^2 + 1$

$$[x^3 + 2]_{x^2+1} = [-x + 2]_{x^2+1}$$
$$\begin{array}{r} x^3 + 2 \text{ mod } x^2 + 1 \\ - x^3 - x \\ \hline -x + 2 \end{array}$$

Rest

$$x^3 + 2 \text{ mod } x^2 + 1 = -x + 2$$

Addition $[(4 + 3x)]_f + [(3 - x)]_f = [4 + 3x + 3 - x]_f = [7 + 2x]_f.$

$(4 + 3x) \text{ mod } (x^2 + 1)$

Subtraktion $[(4 + 3x)]_f - [(3 - x)]_f = [(4 + 3x) - (3 - x)]_f = [1 + 4x]_f.$

Beispiel: Multiplikation in $\mathbb{R}[x]/(x^2 + 1)$

Multiplikation $[(4 + 3x)]_f \cdot [(3 - x)]_f = [(\underline{4 + 3x})(\underline{3 - x})]_f = [12 + 5x - 3x^2]_f.$
 $= [5x + 15]_f$

Hier passiert etwas: wir können den Rest bei Division durch f berechnen.
Also

$$\begin{array}{r} \parallel \\ -3x^2 + 5x + 12 : x^2 + 1 = -3 \\ -3x^2 \quad \quad \quad -3 \\ \quad \quad \quad 5x + 15 \quad \text{Rest} \end{array}$$

Also ist $[(4 + 3x)]_f \cdot [(3 - x)]_f = [5x + 15]_f$.

Beispiel: Division in $\mathbb{R}[x]/(x^2 + 1)$

Division $\frac{[4+3x]_f}{[3-x]_f} = ?$. $[4+3x]_f \cdot [3-x]_f^{-1}$

Auch keine Überraschung: erweiterter Euklidscher Algorithmus wie in \mathbb{Z}_p .

$$\begin{aligned} -x+3 : 10 &= -\frac{x}{10} + \frac{3}{10} \\ \underline{-x} & \\ \underline{\underline{3}} & \\ 0 & \text{rest} \end{aligned}$$

	$x^2 + 1$	$3 - x$	
f	$x^2 + 1$	<u>1</u>	<u>0</u>
$2-x$	$-x + 3$	<u>0</u>	<u>1</u>
	<u>10</u>	<u>$1/10$</u>	<u>$-x - 3$</u>
	<u>0</u>	<u>$3+x/10$</u>	<u>$-\frac{1}{10}x + \frac{3}{10}$</u>

$$\begin{aligned} x^2 + 1 : -x + 3 &= -x - 3 \\ -x^2 - x & \\ \hline 3x + 1 & \\ +3x - 9 & \\ \hline 10 & \text{rest} \end{aligned}$$

Gut, der ggT ist 1 und $[3 - x]_f^{-1} = [\frac{1}{10}(3 + x)]_f$. Also ist

$$\frac{[4+3x]_f}{[3-x]_f} = \underbrace{[(4+3x)]_p}_{=} \cdot \underbrace{[\frac{1}{10}(3+x)]_f}_{=} = \dots = [\underbrace{\frac{9}{10} + \frac{13}{10}x}]_f.$$

Beispiel: Bequemer rechnen in $\mathbb{R}[x]/(x^2 + 1)$

Das Berechnen der Reste ist etwas mühsam, es geht auch bequemer, wie, das wissen wir schon längst. Schaut man genauer hin, so bemerkt man, dass wir hier \mathbb{C} , den Körper der komplexen Zahlen, konstruiert haben. Wir brauchen statt x lediglich i zu schreiben.

Rechnet man modulo f , so ist $x^2 + 1 = 0 \pmod{f}$, oder mit i : $i^2 + 1 = 0 \pmod{f}$, bzw. $i^2 = -1 \pmod{f}$. Jetzt ist alles klar, die komplexe Zahl i ist die Resklasse $[x]_f$.

$$\begin{aligned}(4+3i)(3-i) &= 12 + 9i - 4i - 9i^2 \\ &\leq 12 + 5i - \underbrace{9i^2}_{=-1} = 12 + 5i + 9 = 21 + 5i\end{aligned}$$

Beispiel: Bequemer rechnen in $\mathbb{R}[x]/(x^2 + 1)$

Man kann es auch so sehen: wir haben einen neuen Körper konstruiert, indem wir zu \mathbb{R} einfach ein neues Element i hinzugefügt haben. Man schreibt daher auch oft $\mathbb{R}(i)$ für diesen Körper und nennt $\mathbb{R}(i)$ **Erweiterungskörper** von \mathbb{R} .

In $\mathbb{R}(i)$ ist f nicht mehr irreduzibel, denn nun ist $x^2 + 1 = \underline{(x + i)} \underline{(x - i)}$. Also „zerfällt“ f jetzt in die Linearfaktoren $(x + i)$ und $(x - i)$, weswegen der Körper $\mathbb{R}(i)$ auch **Zerfällungskörper** von f genannt wird.

In aller Kürze zusammengefasst haben wir

$$\mathbb{C} \approx \mathbb{R}(i) \approx \mathbb{R}[x]/(x^2 + 1).$$

Beispiel: Der Körper $\mathbb{Z}_2[x]/(x^2 + x + 1)$

Das Polynom $f = x^2 + x + 1$ ist irreduzibel in $\mathbb{Z}_2[x]$. Wie vorher rechnen wir am bequemsten, indem wir eine fiktive Lösung α der Gleichung $x^2 + x + 1 = 0$ zu \mathbb{Z}_2 hinzufügen, wir erhalten den Körper $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2[x]/(x^2 + x + 1)$. Sehen wir uns diesen Körper an.

Wir verzichten gleich auf die Schreibweise als Restklassen und verwenden α . Die Elemente von $\mathbb{Z}_2(\alpha)$ sind:

$$0, 1, \alpha, \alpha + 1$$

$\mathbb{Z}_2(\alpha)$ ist ein Körper mit 4 Elementen. Das neue α ist eine Lösung von $x^2 + x + 1 = 0$, und daher ist $\alpha^2 = \alpha + 1$ (man beachte die Ähnlichkeit zu \mathbb{C}).

$$f = \underline{x^2 + x + 1}$$

$$\underbrace{(x^3 + x + 1) + (x^4 + x^3 + 1)}_{[x^3 + x + 1]_F} = x^4 + \cancel{x^3} + x + \cancel{1} = \underline{\underline{x^4 + x}}$$

$$[x^3 + x + 1]_F + [x^4 + x^3 + 1]_F = [x^4 + x]_F = [0]_F$$

$x^4 + x$ $\underline{x^2 + x + 1}$ $x^4 + x^3 + x^2$ $\underline{x^3 + x^2 + x}$ $x^2 + x^2 + x$ $\underline{\underline{0}} \quad \text{Rest}$
--

$$x^2 + x + 1 = 0$$

$$x^2 = x + 1$$

$$x^3 = x^2 + x$$

$$x^4 = x^3 + x^2$$

↓

$$x^2 + x$$

↓

$$x + 1$$

$$x^3 + x + 1 = \left[\begin{array}{cccc} 1 & 0 & 1 & 1 \end{array} \right]$$

$$x^4 + x^3 + 1 = \left[\begin{array}{cccc} 1 & 1 & 0 & 0 & 1 \end{array} \right]$$

$$x^4 + x \leftarrow \underline{1 \ 0 \ 0 \ 1 \ 0}$$

Beispiel: Rechnen in $\mathbb{Z}_2[x]/(x^2 + x + 1)$

In $\mathbb{Z}_2(\alpha)$ addiert und multipliziert man wie folgt:

<u>+</u>	0	1	<u>x</u>	<u>$\{x+1\}$</u>	<u>\cdot</u>	0	1	<u>α</u>	$\alpha + 1$
0	0	1	α	$\alpha + 1$	0	0	0	0	0
1	1	0	$\alpha + 1$	α	1	0	1	α	$\alpha + 1$
α	α	$\alpha + 1$	0	1	α	0	α	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	α	1	0	$\alpha + 1$	0	$\alpha + 1$	1	α

Die Kehrwerte der vier Elemente von $\mathbb{Z}_2(\alpha)$ sind:

$$\alpha \cdot (\alpha + 1) = \alpha^2 + \alpha$$

$$= \underline{\alpha} + 1 + \underline{\alpha}$$

$$= 1$$

$\frac{g}{g^{-1}}$	0	1	α	$\alpha + 1$
	-	<u>1</u>	<u>$\alpha + 1$</u>	α

Satz

Für jedes $p \in \mathbb{P}$ und jedes $n \in \mathbb{N}$ gibt es ein irreduzibles Polynom $f \in \mathbb{Z}_p[x]$ vom Grad n und somit einen endlichen Körper mit p^n Elementen. Wir nennen diesen Körper $\text{GF}(p^n) := \mathbb{Z}_p[x]/(f)$, **Galoisfeld mit p^n Elementen**. Das sind alle endlichen Körper.

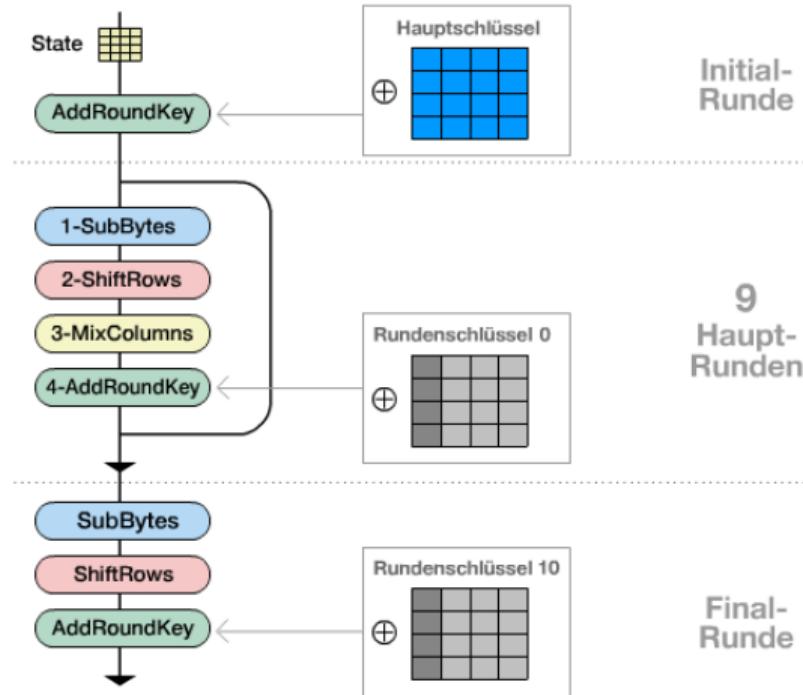
si.py (eigtl. galois)

Rechnen im Körper $\mathbb{Z}_5(\alpha) = \mathbb{Z}_5[x]/(x^3 + 3x + 2)$.

```
> import galois
> k = galois.GF( 5**3, irreducible_poly="x^3+3x+2", repr="poly" )
> k
<class 'galois.GF(5^3)'>
> g = k("x^2+3x+1")
> g
GF(\alpha^2 + 3\alpha + 1, order=5^3)
> g**2 * ( g**2 + 2*g )
GF(\alpha + 2, order=5^3)
> g**(-1)
GF(\alpha^2 + 2, order=5^3)
```

Advanced Encryption Standard (AES) und der Galois Counter Mode (GCM)

AES – Überblick



GF(2⁸) in AES

Operationen im endlichen Körper

$$GF(2^8) = \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1) = \mathbb{Z}_2(\alpha),$$

wobei $\alpha^8 = \alpha^4 + \alpha^3 + \alpha + 1$ ist.

Bytes werden als Elemente in diesem Körper interpretiert.

$$\begin{aligned} \{0,1\}^8 &\mapsto GF(2^8) \\ b_7 b_6 \dots b_0 &\rightarrow b_7 \alpha^7 + b_6 \alpha^6 + \dots + b_0 \in \mathbb{Z}_2(\alpha) \end{aligned}$$

Die Summe zweier Bytes (in GF(2⁸)) ist das bitweise XOR der Bytes.¹

¹Die Multiplikation lässt sich allerdings auf Bitebene nicht mehr einfach erklären. Dies ist ein wichtiger Punkt, der die Analyse des Verfahrens schwierig und AES gegen viele Arten von Angriffen resistent macht.

AES – MixColumns

Im MixColumns-Schritt wird das State Array als eine 4×4 -Matrix S mit Elementen aus $\text{GF}(2^8)$ als Einträgen interpretiert und gemäß

$$S \leftarrow \begin{pmatrix} \alpha & \alpha + 1 & 1 & 1 \\ 1 & \alpha & \alpha + 1 & 1 \\ 1 & 1 & \alpha & \alpha + 1 \\ \alpha + 1 & 1 & 1 & \alpha \end{pmatrix} \cdot S$$

upgedatet. Die Multiplikation und Addition sind hier wieder im Körper $\text{GF}(2^8)$ gemeint.²

²Durch diese Konstruktion als Matrixmultiplikation lässt sich mathematisch einfach beweisen, dass Änderungen in wenigen Einträgen der State-Matrix S durch den MixColumns-Schritt stets zu vielen Änderungen in der State-Matrix führen. Diese Eigenschaft wird üblicherweise als Diffusion bezeichnet, sie sorgt dafür, dass schwerer vom Chiffraut auf den Klartext geschlossen werden kann.

AES – SubBytes

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES – SubBytes

Die Werte in der Tabelle sind nicht willkürlich gewählt. Aus einem Byte $b_7 b_6 \dots b_0$ wird in zwei Schritten ein Byte $s_7 s_6 \dots s_0$. Dabei wird zunächst das Byte $b_7 b_6 \dots b_0$ als Element von $\text{GF}(2^8)$ interpretiert und dort sein Kehrwert berechnet, also

$$(b_7\alpha^7 + \dots + b_0)^{-1} = y_7\alpha^7 + \dots + y_0 \text{ in } \text{GF}(2^8).$$

Das Ergebnis $s_7 s_6 \dots s_0$ ergibt sich dann (gerechnet wird jetzt modulo 2) mit

$$\begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

GCM Revisited

- ▶ Verschlüsselung im Randomized CTR Mode
- ▶ Ein Wert $H := E_K(0 \dots 0)$ wird berechnet.
- ▶ Für Chiffrautblock c wird der Tag t upgedatet gemäß $t = (t + c) \cdot H$.
- ▶ Gerechnet wird im Körper $\text{GF}(2^{128}) = \mathbb{Z}_2[x]/(x^{128} + x^7 + x^2 + x + 1)$.
- ▶ ... und noch ein paar (technische) Details.

