Endliche Körper

Dozent: Prof. Dr. Michael Eichberg

Kontakt: michael.eichberg@dhbw-mannheim.de

Basierend auf: *Cryptography and Network Security - Principles and Practice, 8th Edition, William Stallings*

Version: 1.0.1

Folien: [HTML] https://delors.github.io/sec-endliche-koerper/folien.de.rst.html

[PDF] https://delors.github.io/sec-endliche-koerper/folien.de.rst.html.pdf

Fehler melden:

https://github.com/Delors/delors.github.io/issues

Gruppen, Ringe und Körper

```
((((((
    endliche Körper
        in Körper)
            in Integritätsring)
                in kommutative Ringe)
                    in Ringe)
                        in Abel'schen Gruppen)
                            in Gruppen)
```

Integritätsring:
Integral Domains
Körper: *Fields*
neutrales Element:
Identity element

Übersetzungen mathematischer Fachbegriffe ins Deutsche: https://www.henked.de/woerterbuch.htm

Gruppen

Eine Menge von Elementen mit einer binären Operation $\cdot$, die jedem geordneten Paar (a, b) von Elementen in G ein Element $(a \cdot b) \in G$ zuordnet, so dass die folgenden Axiome befolgt werden:

(A1) Abgeschlossenheit:

Wenn a und b zu G gehören, dann ist $a \cdot b$ auch in G.

(A2) Assoziativität:

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in G$.

(A3) Existenz eines neutralen Elements:

Es gibt ein Element $e \in G$, so dass $a \cdot e = e \cdot a = a$ für alle $a \in G$

(A4) Existenz eines inversen Elements:

Für jedes $a \in G$ gibt es ein Element a' in G, so dass $a \cdot a' = a' \cdot a = e$

Abel'sche Gruppen

(A1 bis A4) und:

(A5) Kommutativität:

$a \cdot b = b \cdot a$ für alle $a, b \in G$

Zyklische Gruppen - Exkursion

- Die Potenzierung ist innerhalb einer Gruppe als eine wiederholte Anwendung des Gruppenoperators definiert, so dass $a^3 = a \cdot a \cdot a$.
- Wir definieren:
  - $a^0 = e$ als das neutrale Element
  - $a^{-n} = (a')^n$, wobei a' das inverse Element von a innerhalb der Gruppe ist.
- Eine Gruppe G ist zyklisch, wenn jedes Element von G eine Potenz a^k (k ist eine ganze Zahl) eines festen Elements $a \in G$ ist.
- Das Element a erzeugt somit die Gruppe G. a ist somit der Generator von G.
- Eine zyklische Gruppe ist immer abelsch und kann endlich oder unendlich sein.

Ringe

- Ein Ring R, manchmal auch als $\{R, +, \times\}$ bezeichnet, ist eine Menge von Elementen mit zwei binären Operationen, genannt Addition und Multiplikation, so dass für alle $a, b, c \in R$ die Axiome (A1-A5) erfüllt sind.
- R ist eine abelsche Gruppe in Bezug auf die Addition; das heißt, R erfüllt die Axiome A1 bis A5. Für den Fall einer additiven Gruppe bezeichnen wir das neutrale Element als 0 und den Kehrwert von a als $-a$.

(M1) Abgeschlossenheit der Multiplikation:

Wenn a und b teil von R sind, dann ist ab auch in R

(M2) Assoziativität der Multiplikation:

$a(bc) = (ab)c$ für alle $a, b, c \in R$

(M3) Distributivgesetz:

$a(b + c) = ab + ac$ für alle $a, b, c \in R$

$(a + b)c = ac + bc$ für alle $a, b, c \in R$

Im Wesentlichen ist ein Ring eine Menge, in der wir Addition, Subtraktion

$[a - b = a + (-b)]$ und Multiplikation durchführen können, ohne die Menge zu verlassen.

- Ein Ring wird als kommutativ bezeichnet, wenn er die folgende zusätzliche Bedingung erfüllt:

  (M4) Kommutativität der Multiplikation:

  $ab = ba$ für alle $a, b \in R$

Integritätsring

Ein kommutativer Ring, der den folgenden Axiomen gehorcht:

(M5) Existenz eines neutralen Elements bzgl. der Multiplikation:

Es gibt ein Element 1 in R, so dass $a1 = 1a = a$ für alle $a \in R$

(M6) Keine Nullteiler:

Wenn $a, b \in R$ und $ab = 0$, dann ist entweder $a = 0$ oder $b = 0$

Körper

- Ein Körper F, manchmal auch bezeichnet als $\{F, +, \times\}$, ist eine Menge von Elementen mit zwei binären Operationen, genannt Addition und Multiplikation, so dass für alle $a, b, c \in F$ die Axiome (A1-M6) gelten.

(M7) Existenz der multiplikativen Inversen:

Für jedes a in F, außer 0, gibt es ein Element $a^{-1} \in F$, so dass $aa^{-1} = (a^{-1})a = 1$

- Im Wesentlichen ist ein Körper eine Menge, in der wir Addition, Subtraktion, Multiplikation und Division durchführen können, ohne die Menge zu verlassen. Die Division ist mit der folgenden Regel definiert: $a/b = a(b^{-1})$

Beispiel

Bekannte Beispiele für Körper sind die rationalen Zahlen, die reellen Zahlen und die komplexen Zahlen.

Hinweis

Die Menge aller ganzen Zahlen mit den üblichen Operationen bildet keinen Körper, da nicht jedes Element der Menge ein multiplikatives Inverses hat.

F ist ein Integritätsbereich, d. h. F erfüllt die Axiome A1 bis A5 und M1 bis M6

Körper ≙ 🇺🇸 *Field*

Eigenschaften von Gruppen, Ringen und Körpern

Körper

Integritätsbereich

Kommutativer Ring

Ring

Abelsche Gruppe

Gruppen

(A1) Abgeschlossen bzgl. Addition
(A2) Assoziativität der Addition
(A3) Neutrales Element bzgl. Add.
(A4) Inverse bzgl. der Addition

(A5) Kommutativität der Addition

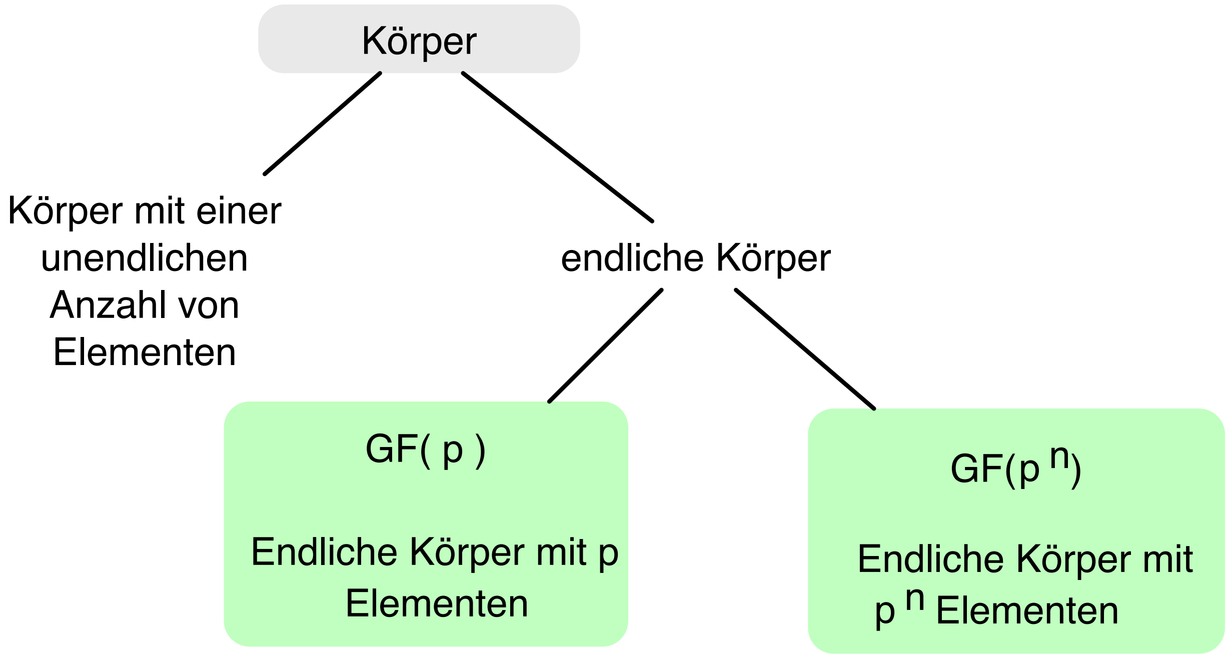
(M1) Abgeschlossen bzgl. Multi.
(M2) Assoziativität der Multiplikation
(M3) Distributiv Gesetz

(M4) Kommutativität der Multi.

(M5) neutrales Element bzgl. Multi.
(M6) Nullteilerfrei

(M7) Inverses Element bzgl. Multi.

Unterteilung von Körpern



Endliche Körper der Form $GF(p)$

- Endliche Körper bilden die Grundlage von Fehlererkennungs- / Fehlerkorrekturcodes und insbesondere von bedeutenden kryptografischen Algorithmen.
- Es kann gezeigt werden, dass die Ordnung eines endlichen Körpers eine Potenz einer Primzahl p^n sein muss, wobei n eine positive ganze Zahl ist.

Die Ordnung eines endlichen Körpers ist die Anzahl der Elemente des Körpers.

- Der endliche Körper der Ordnung p^n wird allgemein als $GF(p^n)$ bezeichnet.
- GF steht für 🇺🇸 *Galois Field* (🇩🇪 *Galoiskörper*), zu Ehren des Mathematikers, der als erster endliche Körper untersucht hat.

klassische Rechnung mit ganzen Zahlen modulo 8[1]

Addition Modulo 8

+	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
0	**0**	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	**0**
2	2	3	4	5	6	7	**0**	1
3	3	4	5	6	7	**0**	1	2
4	4	5	6	7	**0**	1	2	3
5	5	6	7	**0**	1	2	3	4
6	6	7	**0**	1	2	3	4	5
7	7	**0**	1	2	3	4	5	6

Multiplikation Modulo 8

×	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	**1**	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	**1**	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	**1**

[1] Hervorgehoben ist jeweils das inverse Element.

Additive and Muliplikative Inverse Modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

klassische Rechnung mit ganzen Zahlen modulo 7[2]

Addition Modulo 7

+	*0*	*1*	*2*	*3*	*4*	*5*	*6*
0	**0**	1	2	3	4	5	6
1	1	2	3	4	5	6	**0**
2	2	3	4	5	6	**0**	1
3	3	4	5	6	**0**	1	2
4	4	5	6	**0**	1	2	3
5	5	6	**0**	1	2	3	4
6	6	**0**	1	2	3	4	5

Multiplikation Modulo 7

×	*0*	*1*	*2*	*3*	*4*	*5*	*6*
0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6
2	0	2	4	6	**1**	3	5
3	0	3	6	2	5	**1**	4
4	0	4	**1**	5	2	6	3
5	0	5	3	**1**	6	4	2
6	0	6	5	4	3	2	**1**

[2] Hervorgehoben ist jeweils das inverse Element.

Additive und Muliplikative Inverse Modulo 7

w	$-w$	w^{-1}
0	0	–
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Der Körper GF(2)

Addition

$+$	0	1
0	0	1
1	1	0

Multiplikation

$\times$	0	1
0	0	0
1	0	1

Inverse

w	$-w$	w^{-1}
0	0	0
1	0	1

Die Addition ist die XOR-Operation und die Multiplikation ist die AND-Operation.

Endliche Körper - Konstruktion

In diesem Abschnitt haben wir gezeigt, wie man endliche Körper der Ordnung p konstruiert, wobei p prim ist.

$GF(p)$ ist mit den folgenden Eigenschaften definiert:

1. $GF(p)$ besteht aus p Elementen.
2. Die binären Operationen $+$ und $\times$ sind über der Menge definiert. Die Operationen der Addition, Subtraktion, Multiplikation und Division können durchgeführt werden, ohne die Menge zu verlassen. Jedes Element der Menge, das nicht 0 ist, hat eine multiplikative Inverse.

Quintessenz

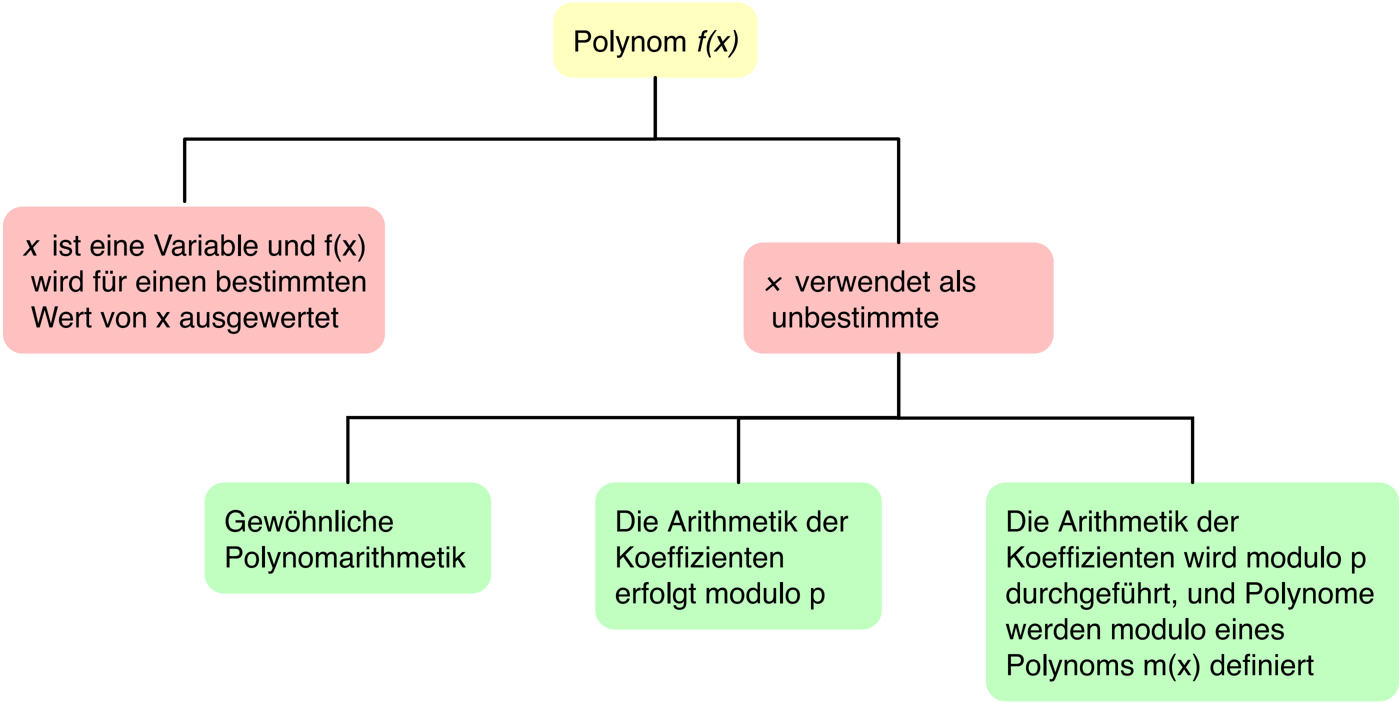
Wir haben gezeigt, dass die Elemente von $GF(p)$ die ganzen Zahlen $\{0, 1, \ldots, p-1\}$ sind und dass die arithmetischen Operationen Addition und Multiplikation modulo p sind.

Hinweis

Die modulare Arithmetik Modulo 8 ist *kein* Körper.

Für eine effiziente Nutzung klassischer Computer benötigen wir einen endlichen Körper der Form $GF(2^n)$.

Die Behandlung von Polynomen



(indeterminate *unbestimmte*)

Beispiel für gewöhnliche Polynomarithmetik

Addition:

$$(x^3 + x^2 + 2) + (x^2 - x + 1)$$

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

Subtraktion:

$$(x^3 + x^2 + 2) - (x^2 - x + 1)$$

$$= x^3 + x + 1$$

Multiplikation:

$$(x^3 + x^2 + 2) \times (x^2 - x + 1) =$$

$$\begin{array}{cccccccccccc}
 & & & & x^3 & + & x^2 & & & + & 2 & \\
 & - & x^4 & - & x^3 & & & - & 2x & & & \\
x^5 & + & x^4 & & & + & 2x^2 & & & & & = \\
\hline
x^5 & & & & & + & 3x^2 & - & 2x & + & 2 &
\end{array}$$

Division:

$$(x^3 + x^2 + 2) : (x^2 - x + 1) = x + 2 + \left(\frac{x}{x^2 - x + 1} \right)$$

Polynomarithmetik mit Koeffizienten in Z_p

- Wenn jedes eindeutige Polynom als Element der Menge betrachtet wird, dann ist diese Menge ein Ring.
- Wenn die Polynomarithmetik auf Polynomen über einem Körper durchgeführt wird, dann ist die Division möglich.
- Wenn wir versuchen, eine Polynomdivision über eine Koeffizientenmenge durchzuführen, die kein Körper ist, dann ist die Division nicht immer definiert.
  - Auch wenn die Koeffizientenmenge ein Körper ist, ist die Polynomdivision nicht unbedingt exakt; d. h. es gibt ggf. einen Rest.
  - Unter der Voraussetzung, dass Reste erlaubt sind, dann ist die Polynomdivision möglich, wenn die Koeffizientenmenge ein Körper bildet.

Das bedeutet nicht, dass eine exakte Teilung möglich ist.

Polynomiale Division

- Wir können jedes Polynom in der Form schreiben: $f(x) = q(x)g(x) + r(x)$
  - $r(x)$ kann als Rest interpretiert werden
  - Es gilt $r(x) = f(x)\ mod\ g(x)$
- Wenn es keinen Rest gibt, dann teilt $g(x)$ das Polynom $f(x)$
  - Notation: $g(x)|f(x)$
  - Wir können sagen, dass $g(x)$ ein Faktor von $f(x)$ ist
  - Oder $g(x)$ ist ein Teiler von $f(x)$
- Ein Polynom $f(x)$ über einem Körper F ist irreduzibel, genau dann wenn $f(x)$ nicht als Produkt zweier Polynome ausgedrückt werden kann, die beide Element von F sind und beide einen niedrigeren Grad als $f(x)$ haben.
  - Ein irreduzibles Polynom wird auch als Primpolynom bezeichnet.
- Die Polynomdivision kann über die Multiplikation definiert werden. Sei $a, b \in F$ dann ist $a/b = a \times b^{-1}$, wobei b^{-1} das einzige Element des Körpers ist, für das $bb^{-1} = 1$ gilt.

Beispiel für Polynomarithmetik über GF(2)

Erinnerung

$$\begin{aligned} 1+1 &= 1-1 &&= 0 \\ 1+0 &= 1-0 &&= 1 \\ 0+1 &= 0-1 &&= 1 \end{aligned}$$

Addition

$$(x^7+x^5+x^4+x^3+x+1)+(x^3+x+1)=x^7+x^5+x^4$$

1

Subtraktion

$$(x^7+x^5+x^4+x^3+x+1)-(x^3+x+1)=x^7+x^5+x^4$$

2

Multiplikation

$$(x^7+x^5+x^4+x^3+x+1)\times(x^3+x+1)=$$

$$\begin{array}{ccccccccccccccccccc}
 & & & & x^7 & + & & & x^5 & + & x^4 & + & x^3 & + & & & x & + & 1 \\
 & & x^8 & + & & & x^6 & + & x^5 & + & x^4 & + & & & x^2 & + & x & & \\
x^{10} & + & x^8 & + & x^7 & + & x^6 & + & & & x^4 & + & x^3 & & & & & & = \\
\hline
x^{10} & & & & & & & & & + & x^4 & & & + & x^2 & & & + & 1
\end{array}$$

3

Division

$$\begin{array}{lllllllllllll}
(x^7 & + & x^5 & + & x^4 & + & x^3 & + & x & + & 1):(x^3+x+1) & = & x^4+1 \\
-(x^7 & + & x^5 & + & x^4) & & & & & & & \hat{=} & -1\times(x^3+x+1)\times x^4 \\
 & & & & & & -(x^3 & + & x & + & 1) & \hat{=} & -1\times(x^3+x+1)\times 1
\end{array}$$

4

Bestimmung des GGTs zweier Polynome

- Das Polynom $c(x)$ ist der größte gemeinsame Teiler von $a(x)$ und $b(x)$, wenn die folgenden Bedingungen erfüllt sind:
  - $c(x)$ teilt sowohl $a(x)$ als auch $b(x)$
  - Jeder Teiler von $a(x)$ und $b(x)$ ist auch ein Teiler von $c(x)$
- Eine äquivalente Definition ist:

  $ggt[a(x), b(x)]$ ist das *Polynom maximalen Grades*, das sowohl $a(x)$ als auch $b(x)$ teilt.
- Der euklidische Algorithmus kann erweitert werden, um den größten gemeinsamen Teiler von zwei Polynomen zu finden, deren Koeffizienten Elemente eines Körpers sind.

Arithmetik in $GF(2^3)$: Addition

		000	001	010	011	100	101	110	111
	$+$	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
000	*0*	**0**	1	2	3	4	5	6	7
001	*1*	1	**0**	3	2	5	4	7	6
010	*2*	2	3	**0**	1	6	7	4	5
011	*3*	3	2	1	**0**	7	6	5	4
100	*4*	4	5	6	7	**0**	1	2	3
101	*5*	5	4	7	6	1	**0**	3	2
110	*6*	6	7	4	5	2	3	**0**	1
111	*7*	7	6	5	4	3	2	1	**0**

Die Definition der Addition des endlichen Körpers $GF(2^3)$ wird in Kürze behandelt.

Wiederholung

Die Subtraktion zweier Elemente des Körpers kann über die Addition definiert werden. Seien $a, b \in F$ dann ist $a - b = a + (-b)$, wobei $-b$ das einzige Element in F ist, für das $b + (-b) = 0$ gilt ($-b$ wird als das Negativ von b bezeichnet).

Arithmetik in $GF(2^3)$: Multiplikation

		000	001	010	011	100	101	110	111
	$\times$	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	**1**	2	3	4	5	6	7
010	2	0	2	4	6	3	**1**	7	5
011	3	0	3	6	5	7	4	**1**	2
100	4	0	4	3	7	6	2	5	**1**
101	5	0	5	**1**	4	2	7	3	6
110	6	0	6	7	**1**	5	3	2	4
111	7	0	7	5	2	**1**	6	4	3

Die Definition der Multiplikation des endlichen Körpers $GF(2^3)$ wird in Kürze behandelt.

Die Anzahl der Vorkommen der ganzen Zahlen ungleich Null ist bei der Multiplikation einheitlich (Vor allem im Vergleich zu Z_8); dies ist für kryptographische Zwecke förderlich.

Arithmetik in $GF(2^3)$

Additive ($-w$) and Multiplicative Inverses (w^{-1})

w	$-w$	w^{-1}
0	0	–
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

(Die Werte wurden aus den vorherigen Tabellen abgelesen.)

Polynomarithmetik über $GF(2^3)$

Um den endlichen Körper $GF(2^3)$ zu konstruieren, müssen wir ein irreduzibles Polynom vom Grad 3 wählen, d.h. entweder $(x^3 + x^2 + 1)$ oder $(x^3 + x + 1)$.

Mit Multiplikationen modulo $x^3 + x + 1$ haben wir nur die folgenden acht Polynome in der Menge der Polynome über $GF(2)$:

$$0, 1, x, x^2, x + 1, x^2 + 1, x^2 + x, x^2 + x + 1$$

Hinweis

Der Verschlüsselungsalgorithmus **AES** führt die Arithmetik im endlichen Körper $GF(2^8)$ mit dem folgenden irreduziblen Polynom aus:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Die 8 Polynome sind die möglichen "Reste" bei der Division von Polynomen über $GF(2^3)$ mit $x^3 + x + 1$.

Polynomarithmetik im $GF(2^3)$ Modulo $(x^3 + x + 1)$

Addition

		000	*001*	*010*	*011*	*100*	*101*	*110*	*111*
	$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	**0**	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	**0**	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	**0**	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	**0**	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	**0**	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	**0**	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	**0**	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	**0**

Polynomarithmetik im $GF(2^3)$ Modulo $(x^3 + x + 1)$

Multiplikation

		000	*001*	*010*	*011*	*100*	*101*	*110*	*111*
	$\times$	*0*	*1*	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	*0*	0	0	0	0	0	0	0	0
001	*1*	0	**1**	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	**1**	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	**1**	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	**1**
101	x^2+1	0	x^2+1	**1**	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	**1**	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	**1**	x^2+x	x^2	$x+1$

Beispiel

$$((x^2) \times (x^2+1) = x^4 + x^2)\ mod\ (x^3 + x + 1) = x$$

Multiplikation in $GF(2^n)$

- Mit keiner einfachen Operation lässt sich die Multiplikation in $GF(2^n)$ erreichen.
- Es gibt jedoch eine vernünftige, unkomplizierte Technik.

"Beispiel: Multiplikation in $GF(2^8)$ wie von AES verwendet"

Beobachtung: $x^8 \; mod \; m(x) = [m(x) - x^8] = x^4 + x^3 + x + 1$

Es folgt, dass die Multiplikation mit x (d.h., $0000\,0010$) als 1-Bit-Linksverschiebung gefolgt von einer bedingten bitweisen XOR-Operation mit $0001\,1011$ implementiert werden kann:

$$x \times f(x) = \begin{cases} (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) & wenn \; b_7 = 0 \\ (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) \oplus 00011011 & wenn \; b_7 = 1 \end{cases}$$

Multiplikation mit einer höheren Potenz von x kann durch wiederholte Anwendung der vorherigen Gleichung erreicht werden. Durch Hinzufügen von Zwischenergebnissen kann die Multiplikation mit einer beliebigen Konstanten in $GF(2^n)$ erreicht werden.

Das von **AES** verwendete Polynom ist:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Bzgl. der Beobachtung: Wenn wir zum Beispiel das Polynom x^7 multiplizieren mit x gilt:

$$(x^7 \times x = x^8) \; mod \; m(x) = x^4 + x^3 + x + 1$$

da

$$\frac{x^8}{x^8 + x^4 + x^3 + x + 1} = 1 \; Rest \; x^4 + x^3 + x + 1.$$

1. Beispiel:

$$(x^7 + x^6 + 1) \times x = (x^8 + x^7 + x) \; mod \; m(x)$$

Hilfsrechnung:

$$\begin{array}{lllllll} x^8+ & x^7+ & & & x & & /(x^8 + x^4 + x^3 + x + 1) = 1 \; Rest \; x^7 + x^4 + x^3 + 1 \\ -(x^8+ & & x^4+ & x^3+ & x+ & 1) & \\ & x^7+ & x^4+ & x^3+ & & 1 & \end{array}$$

2. Beispiel:

$$x^7 \times x^2 = (x^9) \; mod \; m(x)$$

Hilfsrechnung:

$$\begin{array}{llllll} x^9 & & & & & /(x^8 + x^4 + x^3 + x + 1) = x \; Rest \; x^5 + x^4 + x^2 + x \\ -(x^9+ & x^5+ & x^4+ & x^2+ & x) & \end{array}$$

Die Multiplikation mit x^2 kann durch die zweifache Multiplikation mit x unter Anwendung der obigen Gleichung erreicht werden kann. D. h. $x^7 \times x^2 = (x^7 \times x) \times x$

Überlegungen zur Berechnung

- Da die Koeffizienten 0 oder 1 sind, kann ein solches Polynom als Bitfolge dargestellt werden
  - Addition ist ein XOR dieser Bitstrings
  - Multiplikation ist eine Linksverschiebung gefolgt von einem XOR

    (vgl. klassische Multiplikation per Hand.)
- Die Modulo-Reduktion erfolgt durch wiederholtes Ersetzen der höchsten Potenz durch den Rest des irreduziblen Polynoms (auch Shift und XOR)

Übung

Füllen Sie die fehlenden Werte aus ($GF(2^m)$)

Polynomial	**Binary**	**Decimal**
$x^7 + x^6 + x^4 + x + 1$		
	11001001	
		133
$x^4 + x^2 + x$		
	00011001	
		10

Füllen Sie die fehlenden Werte aus ($GF(2^m)$)

Polynomial	Binary	Decimal
$x^7 + x^6 + x^4 + x + 1$		
	11001001	
		133
$x^4 + x^2 + x$		
	00011001	
		10

Übung

Gegeben sei $GF(2^5)$ mit dem irreduziblen Polynom $p(x) = x^5 + x^2 + 1$

1. Berechne: $(x^3 + x^2 + x + 1) - (x + 1)$
2. Berechne: $(x^4 + x) \times (x^3 + x^2)$
3. Berechne: $(x^3) \times (x^2 + x^1 + 1)$
4. Berechne: $(x^4 + x)/(x^3 + x^2)$ geben $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

   Zur Erinnerung: Division kann als Multiplikation definiert werden. Seien $a, b \in F$, dann ist $a/b = a \times (b^{-1})$, wobei b^{-1} die Umkehrung von b ist.

5. Verifiziere: $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

Gegeben sei $GF(2^5)$ mit dem irreduziblen Polynom $p(x) = x^5 + x^2 + 1$

1. Berechne: $(x^3 + x^2 + x + 1) - (x + 1)$
2. Berechne: $(x^4 + x) \times (x^3 + x^2)$
3. Berechne: $(x^3) \times (x^2 + x^1 + 1)$
4. Berechne: $(x^4 + x)/(x^3 + x^2)$ geben $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

   Zur Erinnerung: Division kann als Multiplikation definiert werden. Seien $a, b \in F$, dann ist $a/b = a \times (b^{-1})$, wobei b^{-1} die Umkehrung von b ist.

5. Verifiziere: $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

Übung - $GF(2^8)$

Nehmen wir an, dass 7 und 3 stellvertretend für die Bitmuster der Koeffizienten des Polynoms stehen.

- Berechne: $7d - 3d$
- Berechne: $7d + 3d$
- Berechne: $(0x03 \ \times \ 0x46)$

  (0x3 und 0x46 sind die Hexadezimaldarstellungen der Koeffizienten des Polynoms und diese repräsentieren (auch nur) die Bitmuster der Koeffizienten des Polynoms)

Nehmen wir an, dass 7 und 3 stellvertretend für die Bitmuster der Koeffizienten des Polynoms stehen.

- Berechne: $7d - 3d$
- Berechne: $7d + 3d$

- Berechne: $(0x03 \times 0x46)$

  (0x3 und 0x46 sind die Hexadezimaldarstellungen der Koeffizienten des Polynoms und diese repräsentieren (auch nur) die Bitmuster der Koeffizienten des Polynoms)