Mathematik I

Anwendungen in der Kryptographie

Prof. Dr. Doris Bohnet

Sommersemester 2020

Lernziele

- **Begriffe bzw. Aussagen kennen:**
  - ✓ Ring, Körper
  - ✓ RSA-Verschlüsselung
  - ✓ Diffie-Hellmann-Verschlüsselung

- Beispiele für Ringe und endliche Körper kennen
- Wichtige Eigenschaften von Körpern kennen
- Prinzip der RSA-Verschlüsselung und der Diffie-Hellmann-Verschlüsselung kennen

Wiederholungsfragen - Kahoot

1.) inverses Element von $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$

$(1,1) + (a,b) = (0,0)$ ← neutrales Element

also $(1,2)$: $(1,1) + (1,2) = (2,3) = (0,0)$

2.) $\mathbb{Z}_7^*$ 2, $2^2 \bmod 7 = 4 \bmod 7$

$2^3 \bmod 7 = 1 \bmod 7$ $\Rightarrow$ ord(2) = 3, also kein Erzeuger!

denn $|\mathbb{Z}_7^*| = 6$

3.) $f: \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_4$, $f(a) = (a \bmod 3, a \bmod 4)$

$f(4) = (4 \bmod 3, 4 \bmod 4) = (1,0)$

4.) f aus 3.) ist Isomorphismus.

Wiederholung

Chinesischer Restsatz

Für $n_1, \dots, n_k \in \mathbb{N}$ teilerfremd und $x_1, \dots, x_k \in \mathbb{Z}$ gibt es genau eine Lösung $x \in \mathbb{Z}_n$, $n = n_1 \cdot \dots \cdot n_k$ so dass

$$x \bmod n_i = x_i \bmod n_i \qquad i = 1, 2, \dots, k$$

Beispiel: $x \bmod 2 = 1 \bmod 2$, $x \bmod 3 = 1 \bmod 3$, $x \bmod 5 = 3 \bmod 5$

$n_1 = 2$, $x_1 = 1$; $n_2 = 3$, $x_2 = 1$; $n_3 = 5$, $x_3 = 3$

$\Rightarrow n = n_1 \cdot n_2 \cdot n_3 = 2 \cdot 3 \cdot 5 = 30$

n_1: $ggT\left(n_1, \frac{n}{n_1}\right) = 1 = ggT(2, 15)$:

$1 = \overset{8}{r_1} \cdot 2 + \overset{(-1)}{s_1} \cdot 15$

$a_1 = s_1 \cdot 15 = -15$

n_2: $ggT\left(n_2, \frac{n}{n_2}\right) = ggT(3, 10) = 1$:

$1 = \overset{-3}{r_2} \cdot 3 + \overset{1}{s_2} \cdot 10$

$a_2 = s_2 \cdot 10 = 10$

n_3: $ggT\left(n_3, \frac{n}{n_3}\right) = ggT(5, 6) = 1$:

$1 = \overset{-1}{r_3} \cdot 5 + \overset{1}{s_3} \cdot 6$

$a_3 = s_3 \cdot 6 = 6$

$$\begin{cases} x = a_1 \cdot x_1 + \\ \quad a_2 x_2 + \\ \quad a_3 x_3 \bmod 30 \\ x = 13 \bmod 30 \end{cases}$$

Anwendung des Chinesischen Restsatzes

„CRT"

Seien $n_1, n_2, \ldots, n_k \in \mathbb{N}$ zueinander teilerfremde Zahlen. Dann gilt:

$$\mathbb{Z}_{n_1 \cdot \ldots \cdot n_k} \cong \mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_k}$$

z. B. 3,4 teilerfremd: $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$

3,4,5 teilerfremd: $\mathbb{Z}_{60} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$

Beispiel - Ring

$(\mathbb{Z}_4, +)$

neutrales Element →	+	0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

symmetrisch

abelsch Gruppe

$(\mathbb{Z}_4, \cdot)$

neutral	·	0	1	2	3
	0	0	0	0	0
(1)	1	0	1	2	3
	2	0	2	0	2
	3	0	3	2	1

← hier gibt es keine 1

keine Gruppe!

Distributivgesetz: $a \cdot (b+c) = ab + ac$

$(b+c)a = ba + ca$

$\rightsquigarrow (\mathbb{Z}_4, +, \cdot)$ ist ein RING.

Definition - Ring

Eine Menge R mit zwei Verknüpfungen $+,\cdot$ heißt (~~kommutativer~~) Ring, falls
(R1) $(R,+)$ ist eine abelsche Gruppe.
(R2) Die Verknüpfung $\cdot$ ist assoziativ. $a(bc) = (ab)c \quad \forall a,b,c \in R$
(R3) Das Distributivgesetz gilt. $a(b+c) = ab + ac$

Beispiel: $\rightsquigarrow (\mathbb{Z}_n, +, \cdot) \quad n \in \mathbb{N} \quad$ z.B. $(\mathbb{Z}_4, +, \cdot)$

$(\mathbb{Z}, +, \cdot)$ ganze Zahlen

$(2\mathbb{Z}, +, \cdot)$ gerade Zahlen

Beispiel - Körper

$(\mathbb{Z}_5, +)$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

abelsche Gruppe

↑ Addition ist kommutativ

$(\mathbb{Z}_5, \cdot)$

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

neutral ↓

$\mathbb{Z}_5 \setminus \{0\}$ Gruppe

Distributivgesetz

$\Rightarrow (\mathbb{Z}_5, +, \cdot)$ Körper

Definition - Körper

Eine Menge K mit zwei Verknüpfungen $+, \cdot$, so dass
(K1) $(K, +)$ eine abelsche Gruppe mit neutralem Element 0 ist,
(K2) $(K \setminus \{0\}, \cdot)$ eine Gruppe mit neutralem Element 1 ist und
(K3) das Distributivgesetz gilt,
heißt **Körper.**

inverse Elemente der Multiplikation!

Beispiele:

$(\mathbb{R}, +, \cdot)$ Körper
$(\mathbb{Q}, +, \cdot)$ Körper
$(\mathbb{Z}_p, +, \cdot)$ p Primzahl

$ax = b$ ist eindeutig lösbar, denn es gibt a^{-1}: $x = a^{-1}b$

Endliche Körper

Die Ringe $(\mathbb{Z}_p, +, \cdot)$ sind genau dann Körper, wenn p eine Primzahl ist.

Folgerung: Gleichungen wie $ax = b$ sind eindeutig lösbar.

z. B. in $\mathbb{Z}_{12}$: $2x \bmod 12 = 1 \bmod 12$

ist nicht lösbar

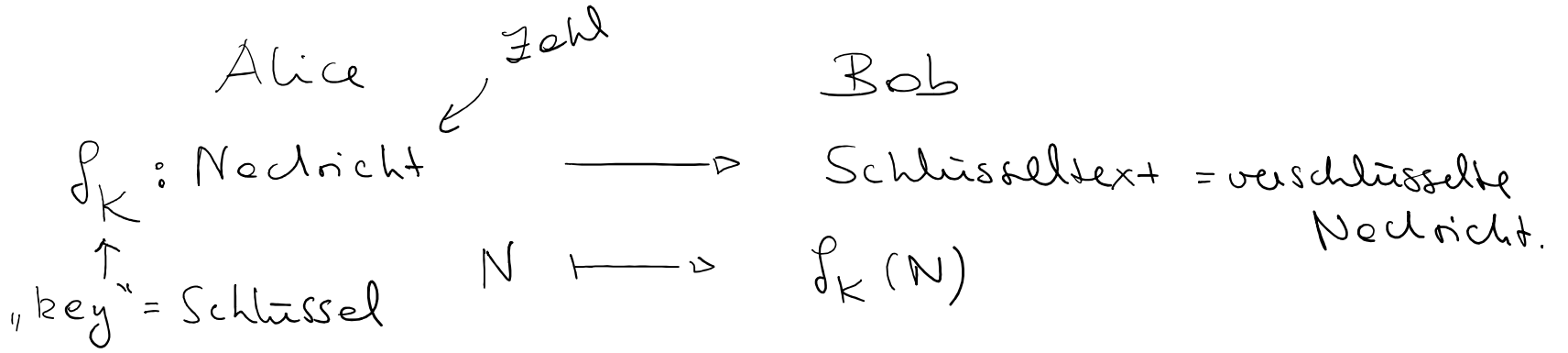
$3x \bmod 12 = 0 \bmod 12$

hat mehrere Lösungen:

$x = 4$, $x = 0$, $x = 8$

in $\mathbb{Z}_{11}$: alles eindeutig lösbar ....

RSA-Verschlüsselung



1. Wähle zwei Primzahlen p, q, so daß $N \in \mathbb{Z}_{p \cdot q}$ (≈ 1024 Bit)
   d.h. $N < p \cdot q$
2. Wähle $e \in \mathbb{Z}^*_{\varphi(n)}$ mit $n = p \cdot q$
   $\varphi(n) = \varphi(p \cdot q)$
   $\varphi(n) = (p-1)(q-1)$
   $ggT(e, (p-1)(q-1)) = 1$
3. Berechne $d \in \mathbb{Z}^*_{\varphi(n)}$ das Inverse von e: $e \cdot d = 1 \bmod \varphi(n)$

n, e öffentlicher Schlüssel von Bob

n, d privater Schlüssel

Anwendung: RSA-Verfahren

1. Es werden Primzahlen p, q gewählt.
2. Es wird der öffentliche Schlüssel berechnet: $n = p \cdot q, e \in \mathbb{Z}^*_{\phi(n)}$
3. Es wird der private Schlüssel berechnet: d $\in \mathbb{Z}^*_{(p-1)(q-1)}$: $d \cdot e = 1 \; mod \; \phi(n)$
4. Eine Nachricht $N \in \mathbb{Z}_n$ für X wird mit dem öffentlichen Schlüssel von X verschlüsselt als: $S = N^e \; mod \; n$
5. Von X wird sie mit Hilfe des privaten Schlüssels entschlüsselt: $N = S^d \; mod \; n$

Warum funktioniert das?

$S = N^e \bmod n$ verschlüsselte Nachricht N

Bob entschlüsselt: $S^d \bmod n = N \bmod n$

Warum funktioniert das?

Satz von Euler: $N^{\varphi(n)} = 1 \bmod n$, $e \cdot d = 1 \bmod \varphi(n)$

$e \cdot d = 1 + k \cdot \varphi(n)$

$S^d \bmod n = N^{ed} \bmod n = N^{1+k\varphi(n)} \bmod n = (N \bmod n)(N^{k\varphi(n)} \bmod n)$

$= N \bmod n$

Einfaches Beispiel

$p = 3,\ q = 5$

öffentlicher Schlüssel: $n = p \cdot q = 15$

$e \in \mathbb{Z}^*_{\varphi(n)} = \mathbb{Z}^*_8$

z. B. $e = 7$

$(n, e) = (15, 7)$

privater Schlüssel: $d \in \mathbb{Z}^*_{\varphi(n)} = \mathbb{Z}^*_8$

so dass $e \cdot d = 1 \mod 8$

$7 \cdot d = 1 \mod 8$

$\rightsquigarrow d = 7$

$S = N^e \mod n$

Nachricht: $N = 12 < 15$: $S = 12^7 \mod 15 = 3 \mod 15$

↳ Schlüsseltext

Entschlüsselung: $N = 3^7 \mod 15 = 12 \mod 15$

$S^d \mod 15$

NR:

$\varphi(n) = \varphi(15) = \varphi(3)\varphi(5)$

$= (3-1)(5-1)$

$\varphi(15) = 8$

$\mathbb{Z}^*_8 = \{1, 3, 5, 7\}$

$12^2 \mod 15 =$

$12^4 \mod 15$

$12^7 \mod 15 = (12^2 \cdot 12^4 \cdot 12) \mod 15$

Anwendung: Diffie-Hellmann

Es soll eine Nachricht zwischen Alice und Bob ausgetauscht werden.

1. Es wird eine Primzahl p gewählt und ein Erzeuger a von $\mathbb{Z}_p^*$ bestimmt.
2. Alice und Bob wählen 2 Zufallszahlen: $q_A, q_B < p - 1$
3. Alice schickt an Bob: $r_A = a^{q_A} mod\ p$
4. Bob schickt an Alice: $r_B = a^{q_B} mod\ p$
5. Alice rechnet: $r_B^{q_A} = a^{q_A q_B} mod\ p = K$
6. Bob rechnet: $r_A^{q_B} = a^{q_A q_B} mod\ p = K$
7. Alice verschlüsselt $N \in \mathbb{Z}_p$: $S = K \cdot N \bmod p$.
8. Bob entschlüsselt: $\mathrm{N} = K^{-1} \cdot S \bmod p$.