KRYPTOLOGIE UND SYSTEMSICHERHEIT

Sommersemester 2020

Technische Hochschule Mittelhessen

Andre Rein

– Modulare Arithmetik –

MODULARE ARITHMETIK (EINFÜHRUNG)

Die modulare Arithmetik spielt in der Kryptographie eine bedeutende Rolle

- Viele (fast alle) klassische/historische Verfahren können so mathematisch beschrieben werden
- Viele moderne **asymmetrische** Verfahren und einige **symmetrische** Verfahren basieren auf modularer Arithmetik, z.B.:
  - Asymmetrisch: RSA/DSA
  - Symmetrisch: AES

MODULARE ARITHMETIK

Berechnungen in der modularen Arithmetik basieren auf **endlichen Mengen**. D.h. das die Anzahl der **Elemente** dieser Mengen ist **begrenzt**.

- In anderen Feldern der Mathematik oder im Alltag sind wir eigentlich an Berechnungen von Zahlen aus **unendlichen** Mengen gewöhnt
  - Menge der natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
  - Menge der ganzen Zahlen $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$
  - Menge der rationalen Zahlen $\mathbb{Q} = \{\ldots, -\frac{2}{1}, -\frac{1}{1}, -\frac{1}{2}, 0, \frac{1}{2}, \frac{1}{1}, \frac{2}{1}, \ldots\}$

MODULARE ARITHMETIK

Frage: Kennen Sie eine **endliche** Menge an die wir sehr gewöhnt sind und die wir fast täglich verwenden?

MODULARE ARITHMETIK

Wir möchten in einer Menge mit 9 Zahlen rechnen:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

Ist ein Ergebnis kleiner 9, können wir die normalen Rechenregeln für eine Addition und Multiplikation verwenden.

$5 + 3 = 8$ oder $3 * 2 = 6$

Sobald ein Ergebnis nicht mehr in unsere Menge liegt, verwenden wir die **Modulo**-Operation (mod) und nehmen als Ergebnis den Rest.

$$4 * 3 = 12 \Rightarrow 12 \equiv 3 \bmod 9$$

Nun liegt das Ergebnis der Berechnung wieder in unserer Menge.

MODULARE ARITHMETIK - DEFINITION

Seien $a, r, m \in \mathbb{Z}$ (wobei $\mathbb{Z}$ die Menge aller ganzen Zahlen inklusive 0 ist) und $m > 0$. Dann gilt:

$$a \equiv r \bmod m$$

wenn m ein Teiler von $a - r$ ist.

m ist der **Modulus** (der Modul) und r ist der **Rest**. Man sagt auch, dass a und r **kongruent** bezüglich des **Moduls** sind.

MODULARE ARITHMETIK - BERECHNUNG DES RESTS

Jede Zahl $a \in \mathbb{Z}$ kann für einen gegeben Modul in folgender Form dargestellt werden:

$$a = q * m + r \text{ mit } 0 \leq r < m$$

Es gilt: $a - r = q * m$ (d.h. m teilt $a - r$). Daher kann man schreiben:

$$a \equiv r \bmod m$$

Man beachte, dass $r \in \{0, 1, 2, \ldots, m - 1\}$.

Seien $a = 23$ und $m = 9$ gegeben. Dann gilt:

$$23 = 3 * 9 + 5 \Rightarrow 23 \equiv 5 \bmod 9$$

MODULARE ARITHMETIK - RESTKLASSEN

Laut unser Definition sind alle folgenden Berechnungen korrekt:

$$12 \equiv 3 \mod 9, \text{da } 9|(12-3)$$
$$12 \equiv 21 \mod 9, \text{da } 9|(12-21)$$
$$12 \equiv -6 \mod 9, \text{da } 9|(12-(-6)$$

$x|y$ bedeutet x teilt y

Die Menge $\{\ldots, -24, -15, -6, 3, 12, 21, 30, \ldots\}$ bildet eine sogenannte Restklasse. Alle Elemente einer Restklasse verhalten sich äquivalent.

MODULARE ARITHMETIK - RESTKLASSEN

Für unser Beispiel existieren insgesamt 9 (d.h. 8 weitere) Restklassen.

Eine Restklasse ist: $\{\ldots, -24, -15, -6, 3, 12, 21, 30, \ldots\}$

Aufgabe: Schreiben Sie alle Restklassen auf, die die Elemente **0**, **10**, **29**, **35** und **-10** enthalten!✍

MODULARE ARITHMETIK - RESTKLASSEN

Wir haben gesagt: Alle Elemente einer Restklasse verhalten sich äquivalent. Was bedeutet das eigentlich?

	Alle Elemente einer Berechnung können durch ein beliebiges anderes Element der gleichen Restklasse ersetzt werden.

Wir berechnen: $3^8 = 6561 \equiv 2 \mod 7$, da $6561 = 937 * 7 + 2$
Alternativ können wir auch folgendes rechnen: $3^8 = 3^4 * 3^4 = 81 * 81$

	Das ist noch keine Ersetzung, das geht sowieso immer!

Nun ersetzen wir die 81 mit einem Element aus der gleichen Restklasse, z.B. 4 und rechnen: $3^8 = 81 * 81 \equiv 4 * 4 = 16 \mod 7 \Rightarrow 16 \equiv 2 \mod 7$

Wie wir sehen, ist das Endergebnis das gleiche!

MODULARE ARITHMETIK - RESTKLASSEN

Üblicherweise wählen wir aus allen möglichen Resten einer Berechnung, den Rest mit dem Wert im Bereich:

$$0 \leq m \leq m - 1$$

Wie wir gesehen haben, macht es jedoch mathematisch **keinen Unterschied** welchen konkreten Wert wir aus einer Restklasse auswählen.

Generell lässt sich jedoch, insbesondere per Hand, mit niedrigen Werten leichter rechnen!

MODULARE ARITHMETIK - RESTKLASSENRINGE

Ein **Ring** ist ein fundamentales Konstrukt der Algebra und erlaubt es bestimmte **Rechenoperationen** nach bestimmten **Regeln** mit Elementen einer Menge auszuführen.

Der Restklassenring $\mathbb{Z}_m$ besteht aus:

1. Der Menge $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ sowie
2. den beiden Rechenoperationen $+$ und $*$ für alle $a, b \in \mathbb{Z}_m$, es gilt:
    1. $a + b \equiv c \mod m$, für $c \in \mathbb{Z}_m$
    2. $a * b \equiv d \mod m$, für $d \in \mathbb{Z}_m$

MODULARE ARITHMETIK - RESTKLASSENRINGE

BEISPIEL

Es sei $m = 6$, d.h. wir betrachten $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

- **Addition**: $4 + 4 = 8 \equiv 2 \mod 6$
- **Multiplikation**: $3 * 5 = 15 \equiv 3 \mod 6$
- **Addition** und **Multiplikation**: $(3 * 5) + (2 * 3 * 4) + 2 + 3 = 44 \equiv 2 \mod 6$

MODULARE ARITHMETIK - RESTKLASSENRINGE

EIGENSCHAFTEN

1. **Abgeschlossenheit** → Wenn zwei beliebige Elemente der Menge miteinander *addiert* oder *multipliziert* werden, ist das Ergebnis abermals ein Element des Rings!
2. **Assoziativität** → *Addition* und *Multiplikation* sind assoziativ, d.h. es gilt:
    1. $a + (b + c) = (a + b) + c$ für alle $a, b, c \in \mathbb{Z}_m$
    2. $a * (b * c) = (a * b) * c$ für alle $a, b, c \in \mathbb{Z}_m$
3. **Kommutativität** → *Addition* und *Multiplikation* sind kommutativ, d.h. es gilt:
    1. $a + b = b + a$ für alle $a, b \in \mathbb{Z}_m$
    2. $a * b = b * a$ für alle $a, b \in \mathbb{Z}_m$
4. **Distributivität** → Für die *Addition* und *Multiplikation* gilt das Distributivgesetz:
    1. $a * (b + c) = (a * b) + (a * c)$ für alle $a, b, c \in \mathbb{Z}_m$

MODULARE ARITHMETIK - RESTKLASSENRINGE

ZUSÄTZLICHE EIGENSCHAFTEN DER ADDITION

Die Addition ist **assoziativ** und **kommutativ** und es existiert ein **neutrales Element** 0 bezüglich der Addition. D.h. für jedes Element der Gruppe $\mathbb{Z}_m$ gilt:

$$a + 0 \equiv a \bmod m$$

Das bedeutet außerdem: Für jedes Element a des Rings existiert ein **negatives** Element $-a$, sodass gilt:

- $a + (-a) \equiv 0 \bmod m$ d.h. jedes Element hat eine ***additive Inverse***

MODULARE ARITHMETIK - MULTIPLIKATION

Die Multiplikation ist **assoziativ** und **kommutativ** und es existiert ein **neutrales Element** 1 bezüglich der Multiplikation. D.h. für jedes Element der Gruppe $\mathbb{Z}_m$ gilt:

$$a * 1 \equiv a \bmod m$$

Nicht jedes Element a des Rings hat auch ein **negatives** Element a^{-1} für das gilt:

$$a * (a^{-1}) \equiv 1 \bmod m$$

D.h. die ***multiplikative Inverse*** existiert nur für **bestimmte** Elemente der Menge $\mathbb{Z}_m$. Nur wenn die Inverse a^{-1} zu einem Element a existiert kann eine Division durchgeführt werden, da gilt:

- $\frac{b}{a} \equiv b * a^{-1} \bmod m$

MODULARE ARITHMETIK - MULTIPLIKATIVE INVERSE

Ein Element $a \in \mathbb{Z}_m$ hat genau dann eine Inverse a^{-1}, wenn gilt:

- $ggT(a, m) = 1$

Der ggT ist der *größte gemeinsamer Teiler*, also die größte natürliche Zahl, die sowohl a als auch m teilt. Haben zwei Zahlen a, m einen ggT von 1, also wenn gilt $ggT(a, m) = 1$, sagt man das a und m **teilerfremd** oder **relativ prim** sind!

Wie berechnet man nun die **multiplikativ Inverse**?

Die multiplikative Inverse wird normalerweise mit dem sog. *erweiterten euklid'schen Algorithmus berechnet*. (Wir lernen den Algorithmus später bei asymmetrischer Kryptographie kennen!) Aktuell lösen wir das Problem durch ausprobieren!

MODULARE ARITHMETIK - BERECHNUNG DES GGT (BEISPIEL)

Beispielberechnung von $ggT(83, 405)$

405	=	4	*	83	+	73
83	=	1	*	73	+	10
73	=	7	*	10	+	3
10	=	3	*	3	+	1
3	=	1	*	1	+	0

MODULARE ARITHMETIK - BERECHNUNG DES GGT ✍

Aufgaben - Berechnen Sie per Hand den ggT zu:

- $a_1 = 167, m = 264$ also $ggT(167, 264)$ und
- $a_2 = 165, m = 500$ also $ggT(165, 500)$

Geben Sie an ob eine Inverse für

- a_1^{-1} für $a_1 = 167 \in \mathbb{Z}_{264}$ und a_2^{-1} $a_2 = 165 \in \mathbb{Z}_{500}$ existiert!

MODULARE ARITHMETIK - RESTKLASSENRING

Zusammenfassend kann man sagen, dass der Restklassenring $\mathbb{Z}_m$ aus der Menge der ganzen Zahlen $\{0, 1, 2, \ldots, m-1\}$ besteht und man in dem Ring ***addieren***, ***subtrahieren***, ***multiplizieren*** und, eingeschränkt auf bestimmte Elemente, auch ***dividieren*** kann.