

Übung zu Kryptographische Verfahren Übung 1

Christian Viergutz

Fachgruppe Kombinatorische Algorithmen
Fachbereich Mathematik / Informatik
Universität Osnabrück

WS 2006/07



In dieser Übung

- 1 Organisatorisches
- 2 Mathematische Grundlagen für kryptographische Verfahren:
 - 1 Logarithmen / Potenzen
 - 2 Rechnen mit Restklassen (Modulo)
 - 3 ggT: (Erweiterter) Euklidischer Algorithmus
 - 4 Lineare Kongruenzen



Organisation der Übungen

- Übungsgruppen:

Mo, 12:15 – 13:45 Uhr, Raum 69/117

Fr, 08:30 – 10:00 Uhr, Raum 69/E15

Die Übungen laufen parallel, behandeln (grundsätzlich) die gleichen Themen.

- Inhalt:

- Rückgabe der Hausaufgaben
- Lösungen zu den Übungsblättern
- Vorbereitung auf die nächsten Abgaben

- Abgabe der Übungsaufgaben freitags, 12 Uhr, Kasten 42.
(bitte in Gruppen bis max. 4 Personen abgeben)



Logarithmen / Potenzen

Rechenregeln für Logarithmen:

Seien $a, b, x, y \in \mathbb{R}_{>0}$ und $r \in \mathbb{R}$ beliebig. Dann gilt:

$$\log_b(x \cdot y) = \log_b(x) + \log_b(y) \quad (1)$$

$$\log_b(x/y) = \log_b(x) - \log_b(y) \quad (2)$$

$$\log_b(x^r) = r \cdot \log_b(x) \quad (3)$$

$$\log_b(x) = \frac{\log_a(x)}{\log_a(b)} \quad (4)$$

Aufgabe

Stelle die Zahl 10^{24} als Potenz zur Basis 2 dar.



Rechnen in Restklassen, der Ring \mathbb{Z}_n

- Wir betrachten Ganzzahldivision einer Zahl $a \in \mathbb{Z}$ durch $b \in \mathbb{N}$:

$$a = q \cdot b + r$$

Dabei tritt i.A. ein Rest $r \in \{0, \dots, b-1\}$ auf. q und r sind dann eindeutig bestimmt, man schreibt dafür $q = a \operatorname{div} b$ und $r = a \operatorname{mod} b$.

- Zwei Zahlen a, b heißen *kongruent modulo* $n \in \mathbb{N}$, falls gilt $n \mid (a - b)$, geschrieben $a \equiv b \pmod{n}$.
- Der Restklassenring modulo n ist definiert als $(\mathbb{Z}_n, +, \cdot)$, wobei $\mathbb{Z}_n := \{0, \dots, n-1\}$ und Addition und Multiplikation zweier Elemente $a, b \in \mathbb{Z}_n$ definiert sind durch

$$a + b := (a + b) \operatorname{mod} n \quad \text{und} \quad a \cdot b := (a \cdot b) \operatorname{mod} n$$

- \mathbb{Z}_n ist genau dann ein Körper (es gibt zu jedem Element $\neq 0$ ein multiplikatives Inverses), wenn n eine Primzahl ist.



Größter gemeinsamer Teiler

Definition 3.1 (größter gemeinsamer Teiler (ggT))

Seien $a, b \in \mathbb{Z}$. Die Zahl $d \in \mathbb{N}$ heißt **größter gemeinsamer Teiler** von a und b , geschrieben $d = \text{ggT}(a, b)$, falls für jedes $k \in \mathbb{Z}$ mit $k \mid a$ und $k \mid b$ gilt, dass auch $k \mid d$.

Falls $\text{ggT}(a, b) = 1$ ist, dann heißen a und b zueinander **teilerfremd**.

Beobachtung

Für $a, b \in \mathbb{N}$ gilt:

$$\text{ggT}(a, b) = \begin{cases} \text{ggT}(b, a \bmod b), & \text{falls } a \bmod b > 0 \\ b, & \text{falls } a \bmod b = 0 \end{cases}$$

Diese rekursive Berechnungsvorschrift nutzt der Euklidische Algorithmus (EA) aus.



Euklidischer Algorithmus (EA)

EUKLID(a, b)

- 1 **if** $a = 0$ **return** b ;
- 2 **if** $b = 0$ **return** a ;
- 3 **return** EUKLID($b, a \bmod b$);

Mit einer Erweiterung (EEA) lassen sich auch Werte x, y berechnen mit

$$\text{ggT}(a, b) = x \cdot a + y \cdot b$$

ERWEUKLID(a, b)

- 1 **if** $a = 0$ **return** $(b, 0, 1)$;
- 2 **if** $b = 0$ **return** $(a, 1, 0)$;
- 3 $(d, x, y) \leftarrow$ ERWEUKLID($b, a \bmod b$);
- 4 **return** $(d, y, x - (a \text{ div } b) \cdot y)$;



Beispiel zum EEA

Beispiel 3.2 (Berechne $\text{EEA}(90,43)$ in Schemaform)

r	90	43	4	3	1	0
q	/	2	10	1	3	/
x	1	0	1	-10	11	/
y	0	1	-2	21	-23	/

Daraus folgt: $\text{ggT}(90, 43) = 1 = 11 \cdot 90 - 23 \cdot 43$.

Aufgabe

Berechne mittels des obigen Schemas den ggT von 1400 und 308 und gib Zahlen x, y an mit $\text{ggT}(1400, 308) = x \cdot 1400 + y \cdot 308$.



EEA und Berechnung des Inversen

Satz 3.3

Sei $n \in \mathbb{N}_{>1}$. Zu einem $a \in \mathbb{Z}_n$ gibt es genau dann ein multiplikatives Inverses (a^{-1}), wenn a und n teilerfremd sind.

Beispiel 3.4

In \mathbb{Z}_7 ist 4 invers zu 2 (und umgekehrt), da $4 \cdot 2 = 8 \equiv 1 \pmod{7}$.

Beobachtung

Falls ein Inverses zu a in \mathbb{Z}_n existiert, dann ist die Berechnung mit dem EEA möglich:

- Wegen $\text{ggT}(a, n) = 1$ gibt es Zahlen x, y mit $1 = x \cdot a + y \cdot n$.
 - Betrachtung der Gleichung modulo n ergibt: $1 \equiv x \cdot a \pmod{n}$.
- $\Rightarrow x \equiv a^{-1} \pmod{n}$.



Lineare Kongruenzen

Wir betrachten Kongruenzgleichungen der Form $ax \equiv b \pmod{n}$.

Satz 3.5

Die Kongruenz $ax \equiv b \pmod{n}$ ist genau dann lösbar, wenn $\text{ggT}(a, n) \mid b$. Dann gibt es $\text{ggT}(a, n)$ viele Lösungen $x \in \mathbb{Z}_n$.

Beispiel 3.6

Folgende Berechnungen werden in \mathbb{Z}_8 durchgeführt:

- $2x \equiv 5$: $\text{ggT}(2, 8) = 2 \nmid 5$, daher gibt es keine Lösung.
- $3x \equiv 7$: $\text{ggT}(3, 8) = 1 \Rightarrow$ genau eine Lösung: $x \equiv 3^{-1} \cdot 7 \equiv 5 \pmod{8}$
- $4x \equiv 0$: Wegen $\text{ggT}(4, 8) = 4 \mid 0$ gibt es 4 Lösungen: 0, 2, 4, 6.

Aufgabe

Gib, falls möglich, Lösungen der folgenden Gleichungen an:

- 1 $4(x + 25) \equiv 16 \pmod{29}$
- 2 $13(5 - x) \equiv 17x \pmod{31}$

