



## Einführung in Trusted Systems - WS07/08

### 2. Übung

#### Aufgabe 1 (Der erweiterte euklidische Algorithmus)

Betrachten Sie das folgende Beispiel zur Erinnerung an den erweiterten euklidischen Algorithmus.

$i$	0	1	2	3	4	5	6	7
$r$	456	123	87	36	15	6	3	0
$q$	-	3	1	2	2	2	2	
$x$	1	0	1	1	3	7	17	
$y$	0	1	3	4	11	26	63	

$\Rightarrow \text{gcd}(456, 123) = 3 = 456 \cdot 17 + 123 \cdot (-63).$

- (a) Berechnen Sie ganze Zahlen  $x, y$  mit  $77x + 30y = \text{gcd}(77, 30)$  mit dem erweiterten euklidischen Algorithmus.
- (b) Existiert  $30^{-1} \pmod{77}$ ? Falls ja, warum und wie lautet es?

#### Aufgabe 2 (Rechnen mit Kongruenzen)

Zur Erinnerung:  $a \equiv b \pmod{n}$ , falls  $n \mid (b - a)$ . In der Vorlesung wurden die folgenden Rechenregeln für Kongruenzen vorgestellt. Aus  $a \equiv b \pmod{n}$  und  $c \equiv d \pmod{n}$  folgt

- i)  $-a \equiv -b \pmod{n}$
- ii)  $a + c \equiv b + d \pmod{n}$
- iii)  $a \cdot c \equiv b \cdot d \pmod{n}$

Berechnen Sie per Hand  $x \in \mathbb{Z}_{13}$ , so dass

$$x \equiv -12 \pmod{13}, \quad x \equiv 15 + 29 \pmod{13}, \quad x \equiv 131 \cdot (-12) \pmod{13}$$

#### Aufgabe 3 (Rechnen mit Matrizen modulo $m$ )

Betrachten Sie die Matrizen  $A, B$  und den Vektor  $c$  gegeben als

$$A = \begin{pmatrix} 0 & 4 \\ 3 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 3 \\ 2 & 4 \end{pmatrix}, \quad c = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

- (a) Berechnen Sie  $A + B \pmod{5}$ ,  $A \cdot B \pmod{5}$ ,  $A \cdot c \pmod{5}$  und  $A^{-1} \pmod{5}$ .
- (b) Versuchen Sie  $B^{-1} \pmod{5}$  zu berechnen. Was fällt Ihnen auf?

#### Aufgabe 4 (Die affin lineare Blockchiffre)

Betrachten Sie die affin lineare Blockchiffre mit Alphabet  $\Sigma = \mathbb{Z}_{27}$  und Blocklänge 2. Ein Schlüssel ist ein Paar  $(A, b)$  mit  $A \in \mathbb{Z}_{27}^{(2,2)}$  invertierbar und  $b \in \mathbb{Z}_{27}^2$ . Die Verschlüsselungsfunktion ist

$$E : \mathbb{Z}_{27}^2 \rightarrow \mathbb{Z}_{27}^2, v \mapsto Av + b \text{ mod } 27$$

Die Entschlüsselungsfunktion ist

$$D : \mathbb{Z}_{27}^2 \rightarrow \mathbb{Z}_{27}^2, c \mapsto A^{-1}(c - b) \text{ mod } 27$$

Der Schlüssel sei gegeben durch

$$A = \begin{pmatrix} 15 & 4 \\ 7 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 6 \\ 8 \end{pmatrix}.$$

- (a) Verschlüsseln Sie die Nachricht  $v^T = (12, 17)$ .
- (b) Entschlüsseln Sie den Schlüsseltext  $c^T = (13, 4)$ .

#### Aufgabe 5 (Die Permutationschiffre)

Betrachten Sie die Permutationschiffre über dem Alphabet  $\Sigma = \{A, B, \dots, Z\}$  mit Verschlüsselungsfunktion  $E_\sigma(m_1, m_2, m_3) = (m_{\sigma(1)}, m_{\sigma(2)}, m_{\sigma(3)})$ . Es sei

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

- (a) Verschlüsseln Sie den Klartext  $m = \text{ABC}$ .
- (b) Betrachten Sie nun die Permutationschiffre als lineare Blockchiffre mit Verschlüsselungsfunktion  $c = Am$ . Wie sieht  $A$  für obiges  $\sigma$  aus?

#### Hausaufgabe 1 (Invertierbare Matrizen)

Zur Erinnerung: Die Schlüssel linearer Blockchiffren sind modulo  $m$  invertierbare  $n \times n$  Matrizen mit Einträgen aus  $\mathbb{Z}_m$ .

- (a) Wieviele modulo 2 invertierbare Matrizen  $A \in \mathbb{Z}_2^{(2,2)}$  gibt es?
- (b) Wieviele modulo 2 invertierbare Matrizen  $A \in \mathbb{Z}_2^{(n,n)}$  gibt es?
- (c) Wieviele modulo  $m$  invertierbare Matrizen  $A \in \mathbb{Z}_m^{(n,n)}$  gibt es?

*Hinweis:* Eine Matrix  $A \in \mathbb{Z}_m^{(n,n)}$  ist modulo  $m$  invertierbar, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:

- i) Die Determinante von  $A$  ist invertierbar modulo  $m$ .
- ii) Die Zeilenvektoren sind linear unabhängig.
- iii) Die Spaltenvektoren sind linear unabhängig.

**Plagiarismus** *Der Fachbereich Informatik misst der Einhaltung der Grundregeln der wissenschaftlichen Ethik großen Wert bei. Zu diesen gehört auch die strikte Verfolgung von Plagiarismus. Mit der Abgabe einer Lösung (Hausaufgabe, Programmierprojekt, Diplomarbeit, etc.) bestätigen Sie, dass (Sie/Ihre Gruppe) (der alleinige Autor/die alleinigen Autoren) des gesamten Materials sind. Falls Ihnen die Verwendung von Fremdmaterial gestattet war, so müssen Sie dessen Quellen deutlich zitiert haben. Bei Unklarheiten zu diesem Thema finden Sie weiterführende Informationen unter <http://www.informatik.tu-darmstadt.de/Plagiarism>.*