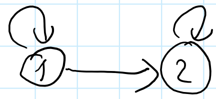


$M = \{1, 2\}$
$R_{100} := \{(1,1),(1,2),(2,2)\}$

- **reflexiv**, wenn für alle x aus M gilt : xRx bzw. $(x,x) \in R$

ja, denn $(1,1) \in R \wedge (2,2) \in R$

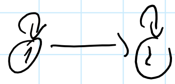
- **symmetrisch**, wenn für alle x, y aus M mit xRy gilt: yRx bzw. falls $(x,y) \in R$, so auch $(y,x) \in R$

nein, denn $(1,2) \in R$ aber $(2,1) \notin R$

- **antisymmetrisch**, wenn für alle x, y aus M mit xRy und yRx gilt: $x = y$ bzw. falls $(x,y) \in R$ und $(y,x) \in R$, so folgt $x = y$

ja, denn $(1,1) \in R \wedge (1,1) \in R \Rightarrow 1 = 1$ ✓
$(2,2) \in R \wedge (2,2) \in R \Rightarrow 2 = 2$ ✓

- **transitiv**, wenn $\forall x, y, z$ aus M mit xRy und yRz gilt: xRz bzw. falls $(x,y) \in R$ und $(y,z) \in R$, so folgt $(x,z) \in R$



$(1,1) \in R \wedge (1,2) \in R \Rightarrow (1,2) \in R$ ✓
$(1,2) \in R \wedge (2,2) \in R \Rightarrow (1,2) \in R$ ✓

Addition von Elementen zweier Restklassen

Seien $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ $(\mathbb{Z}/\equiv_n)$

Seien $a' \in [a]$ u. $b' \in [b]$ beliebig

Dann gilt: $a' + b' \in [a+b]$

Beweis: Für $a' \in [a]$, $b' \in [b]$ existieren $p, q \in \mathbb{Z}$ mit:

$$a' - a = p \cdot n$$
$$b' - b = q \cdot n$$

$$\Rightarrow a' + b' = p \cdot n + a + q \cdot n + b = (p+q) \cdot n + a + b$$
$$a' + b' = (p+q) \cdot n + (a+b)$$
$$\Rightarrow a' + b' \in [a+b]$$

Das motiviert die modulare Addition

$[a], [b] \in \mathbb{Z}/n\mathbb{Z}$

$$[a] + [b] := [a+b]$$

Beispiel $\mathbb{Z}/6\mathbb{Z}$ $\quad n = 6$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

$[1] + [5] = [6] = [0]$
$[2] + [5] = [7] = [1]$

Wiederholung Relationen / Modulare Arithmetik

1. Welche Eigenschaften haben wir für Relationen kennengelernt?
2. Was bedeutet $a \underset{n}{\equiv} b$? Was bedeutet $x \bmod y$
3. Wie kann man $a \underset{n}{\equiv} b$ als Gleichung schreiben?

wobei $b \in \{0, 1, \ldots, n-1\}$

$$a = \underset{\uparrow \text{Quotient}}{q} \cdot n + b$$

ansonsten wenn $a \underset{n}{\equiv} b$

$$\Rightarrow \begin{cases} a = q_1 \cdot n + r \\ b = q_2 \cdot n + r \end{cases}$$

$$a - b = (q_1 - q_2) n$$

d.h. $(a-b)$ ist durch n teilbar
$n \mid (a-b)$ sprich n teilt $a-b$

Bsp $n = 5$ $\quad 17 \underset{5}{\equiv} 12$

$$17 = 3 \cdot 5 + 2$$
$$12 = 2 \cdot 5 + 2$$

Multiplikation von Elementen 2-er Restklassen

$[a], [b] \in \mathbb{Z}/n\mathbb{Z}$

$a' \in [a]$, $b' \in [b]$ beliebig. Dann ist

$a' \cdot b' \in [a \cdot b]$

Beweis: für $a' \in [a]$ u. $b' \in [b]$ existieren p, q mit

$$a' - a = p \cdot n$$
$$b' - b = q \cdot n$$

$$a' \cdot b' = (a + p \cdot n)(b + q \cdot n) = ab + aq n + bp \cdot n + p \cdot q n^2$$
$$= (aq + bp + pq \cdot n) n + ab$$

$\Rightarrow a'b' \in [ab]$

Das motiviert die Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$

$$[a] \cdot [b] = [a \cdot b]$$

Bsp $n = 6$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

$[2] \cdot [3] = [6] = [0]$

Nicht jede Restklasse besitzt ein mult. Inverses

$\rightsquigarrow$ nur die, die teilerfremd ~~zum~~ Modul sind

Rechnen in $\mathbb{Z}/n\mathbb{Z}$

Wenn $a_1 \equiv b_1 \mod n$ $\quad (a_1 \underset{n}{\equiv} b_1)$

$a_2 \equiv b_2 \mod n$

Dann gilt i) $a_1 + a_2 \equiv b_1 + b_2 \mod n$

ii) $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \mod n$

Bsp $5 \underset{4}{\equiv} 9 \qquad 7 \underset{4}{\equiv} 11$

i) $5 + 7 \underset{4}{\equiv} 9 + 11 \qquad$ ii) $5 \cdot 7 \underset{4}{\equiv} 9 \cdot 11$

Beweis zu i) nach Voraussetzung $a_1 \equiv b_1 \mod n$

$$\Leftrightarrow \quad a_1 - b_1 = p \cdot n$$

analog $\quad a_2 - b_2 = q \cdot n$

$$(a_1 + a_2) = (p+q)n + b_1 + b_2$$

$$\Leftrightarrow \quad (a_1 + a_2) - (b_1 + b_2) = (p+q) \cdot n$$

$(a_1 + a_2) - (b_1 + b_2)$ durch n Teilbar

d.h. $\quad a_1 + a_2 \underset{n}{\equiv} b_1 + b_2$

iii) $\quad (a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

Bsp $\quad (11 + 10) \bmod 4 = (11 \bmod 4 + 10 \bmod 4) \bmod 4$

$$= (3 + 2) \bmod 4 = 1$$

iv $\quad (a \cdot b) \bmod n = (a \bmod n)(b \bmod n) \bmod n$

Bsp $\quad (11 \cdot 4) \bmod 4 = (11 \bmod 4)(4 \bmod 4) \bmod 4$

$$= (3 \cdot 0) \bmod 4 = 0$$

$$(11 \cdot 10) \bmod 4 = (3 \cdot 2) \bmod 4$$
$$= 2$$

Anwendung: Caesar Verschlüsselung (additive Inverse)

1. Kodieren wir die Buchstaben
   $A = 0,\ B = 1,\ \_\ \_\_\ \ Z = 25$

Nachricht KLEOPATRA nach der Vorschrift

$y = (x + e) \bmod 26$ mit dem Schlüssel $e = 3$

	K	L	E	O	P	A	T	R	A
x	10	11	4	14	15	0	19	17	0
$y = (x+3) \bmod 26$	13	14	7	17	18	3	22	20	3

Zum Entschlüsseln müssen wir $y = (x+3) \bmod 26$ nach x auflösen indem wir mit -3 auf beiden Seiten addier.

d.h. mit 23 addier

$$x = (y + 23) \bmod 26$$

y	13	14	7	–	–
$x = (y+23)$	10				

y	13	14	7	-	-
$x = (y+23) \bmod 26$	10				

Eulersche φ-Funktion

Einheiten in $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Ein Element $x \in \mathbb{Z}_n$ heißt Einheit, wenn es eine multiplikative Inverse besitzt.

Lemma: ein Element $x \neq 0$, $x \in \mathbb{Z}_n$ ist genau dann eine Einheit wenn x und n teilerfremd.

$$ggT(x, n) = 1$$

Intuition: Wir suchen nach d, so daß $x \cdot d \equiv_n 1$

d.h. $x \cdot d = q \cdot n + 1$

$$x \cdot d - q \cdot n = 1 \qquad (a)$$

Wenn x und n nicht teilerfremd sind

$x = t \cdot \tilde{x}$
$n = t \, \tilde{n}$

Einsetzen in (a) $\quad t \cdot \tilde{x} \cdot d - t \, \tilde{n} \cdot q = 1$

$$t \, (\tilde{x} \cdot d - \tilde{n} \cdot q) = 1$$

$t \in \mathbb{Z}$ $\leadsto$ es gibt kein ganzzahliges d, so daß

ganze Zahl $\cdot$ ganze Zahl $= 1$

Sind x u. n teilerfremd, d.h. $ggT(x, n) = 1$, dann kann man die multiplikative Inverse mit dem erweiterten euklidischen Algorithmus finden. (e.e. A.)

Eulersche φ-Funktion zählt die Menge der Einheiten in $\mathbb{Z}_n$

$$\varphi(n) = |\{x \in \mathbb{Z}_n \mid ggT(x, n) = 1\}| \qquad n \geq 2$$

$$\varphi(p) = p - 1 \qquad , \text{ falls } p \text{ - Primzahl}$$

Sei $n = p \cdot q$ $\quad p, q$ Primzahlen

Dann gilt $\varphi(n) = (p-1)(q-1)$

Euklidischer Algorithmus

Input: $x, n \in \mathbb{Z}$

Output: $ggT(x,n)$

Erweiterter euklidischer A.

Input: $x, n \in \mathbb{Z}$

Output: $d, q \in \mathbb{Z}$

so daß:

$$\underbrace{d \cdot x + q \cdot n = ggT(x,n)}$$

Als Kongruenz rel.

Wenn $ggT(x,n) = 1$

$$d \cdot x = (-q) \cdot n + 1$$
$$d \cdot x = q' \cdot n + 1$$
$$d \cdot x \underset{n}{\equiv} 1$$

$\rightsquigarrow$ d ist mult. Inverse zu x

<u>Bsp</u>: Gesucht d

$$d \cdot 7 \underset{40}{\equiv} 1 \qquad n = 40, \quad x = 7$$

Als Gleichung $\quad d \cdot 7 = q' \cdot 40 + 1$

$$d \cdot 7 + q \cdot 40 = 1 \qquad q = -q'$$

euklidischer Algo

Input: $40, 7$

$$40 = 5 \cdot 7 + 5$$
$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + \boxed{1} \; ggT$$
$$2 = 2 \cdot 1 + 0$$

e. e. A

$$5 = 1 \cdot 40 - 5 \cdot 7$$

$$2 = 1 \cdot 7 - 1 \cdot 5$$
$$= 1 \cdot 7 - 1(1 \cdot 40 - 5 \cdot 7)$$
$$= 6 \cdot 7 - 1 \cdot 40$$

$$1 = 1 \cdot 5 - 2 \cdot 2$$
$$= 1(40 - 5 \cdot 7) - 2(6 \cdot 7 - 1 \cdot 40)$$
$$= 1 \cdot 40 - 5 \cdot 7 - 12 \cdot 7 + 2 \cdot 40$$
$$= -17 \cdot 7 + 3 \cdot 40$$

$$ggT(40,7) = 1 = -17 \cdot 7 + 3 \cdot 40$$

$= -17 \cdot 7 + 3 \cdot 40$

$$ggT(40,7) = 1 = -17 \cdot 7 + 3 \cdot 40$$

$$d = -17 \underset{40}{\equiv} 23$$

Funktionsweise RSA - Verfahren.
(Rivest, Shamir, Adelmann)

(1.) Wähle 2 verschiedene Primzahlen p, q

Berechne $n = p \cdot q$

n: RSA - Modul

(2.) Wähle ein beliebiges $e \in \{2, 3, 4, \ldots, n-1\}$
so daß $ggT(e, \varphi(n)) = 1$, wobei $\varphi(n) = (p-1)(q-1)$

(3) Wähle $d \in \{1, 2, \ldots, n-1\}$ mit $e \cdot d \underset{\varphi(n)}{\equiv} 1$

d.h. d: mult. Inverse zu e mod $\varphi(n)$)

$p, q, \varphi(n)$) braucht man nicht mehr
bleiben aber geheim

(n, e) : öffentlicher Schlüssel

(n, d) : geheimer Schlüssel (nur d geheim)

(4) Zum Verschlüsseln wird die als Binärzahl dargestellte Nachricht in Teile aufgebrochen, so daß jede Teilzahl $< n$ ist.

(5) Verschlüsselung der Teilstücke $m \in \{1, \ldots, n-1\}$

$$c = E((n,e), m) := m^e \bmod n$$

↑ Chiffrat ↑ Encryption

⑥ Entschlüsselung des Chiffrats $c \in \{1, \ldots, n-1\}$

$$m = D((n,d), c) := c^d \bmod n$$

Decryption

RSA mit Zahlen

1. $p = 5, \; q = 7$

$$n = p \cdot q = 5 \cdot 7 = 35$$

2. $\varphi(n) = (5-1) \cdot (7-1) = 4 \cdot 6 = 24$

$e \in \{1, 2, \ldots, 34\}, \quad ggT(e, 24) = 1$

$e = 5$

3. d - bestimmen $\quad e \cdot d \underset{\varphi(n)}{\equiv} 1 \qquad 5 \cdot d \underset{24}{\equiv} 1$

e. A. | e. e. A.

$24 = 4 \cdot 5 + 4$

$5 = 1 \cdot 4 + \boxed{1}$

$4 = 1 \cdot 24 - 4 \cdot 5$

$$\begin{aligned} 1 &= 1 \cdot 5 - 1 \cdot 4 \\ &= 1 \cdot 5 - (1 \cdot 24 - 4 \cdot 5) \\ &= 1 \cdot 5 - 1 \cdot 24 + 4 \cdot 5 \\ &= 5 \cdot 5 - 1 \cdot 24 \end{aligned}$$

$$d = 5$$

öff. Schlüssel $(35, 5)$

geh. Schlüssel $(35, 5)$

(4) $m = 9$

$c = m^e \bmod n = 9^5 \bmod 35 = 4$

(5) $m = c^d \bmod n = 4^5 \bmod 35 = 9$

Beweis der Umkehrbarkeit.

Für Schlüsselpaare (n, e) und (n, d) muß gelten:

$m = c^d \bmod n = (m^e)^d \bmod n$

Message $= m^{e \cdot d} \bmod n$

Zz. $m = m^{e \cdot d} \bmod n$

Wir benutzen den Satz von Euler-Fermat:

$m^{\varphi(n)} \equiv_n 1$ m, n teilerfremd

$e \cdot d \equiv_{\varphi(n)} 1$

$$m^{ed} \equiv_n m^{k \cdot \varphi(n) + 1} \equiv_n m^{k \varphi(n)} \cdot m$$

$$\equiv_n \left(m^{\varphi(n)}\right)^k \cdot m$$

$$\equiv_n 1^k \cdot m$$

$$\equiv_n m$$