Mathematik Vorlesung 30.10.2013

Euklidischer Algorithmus

Ich will den GGT (a, b) finden

Der GGT(a, b) = 1 weil a und b teilerfremd (relativ prim) sein müssen, damit eine Modulare existiert.

Prüfen, ob relativ prim

$a = 3 \quad b = 7$

Rest

$3 = 0 \cdot 7 + 3$

$7 = 2 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0 \Rightarrow GGT(3, 7) = 1$

$a = 7 \quad b = 3$

$7 = 2 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0 \Rightarrow GGT(7, 3) = 1$

$a = 75 \quad b = 38$

Prüfen ob relativ prim

$75 = 1 \cdot 38 + 37$

$38 = 1 \cdot 37 + 1$

$37 = 37 \cdot 1 + 0 \Rightarrow ggT(75, 38) = 1$

$* \Rightarrow 37 = 75 - 1 \cdot 38$

$\Rightarrow 1 = 38 - 1 \cdot 37 = 38 - 1(75 - 1 \cdot 38)$

$= 38 - 1 \cdot 75 + 1 \cdot 38$

$= -1 \cdot 75 + 2 \cdot 38$

$\Rightarrow \underbrace{-1 \cdot 75 \bmod 38}_{=1} + \underbrace{2 \cdot 38 \bmod 38}_{=0}$

~~$\Rightarrow -1 \cdot 75 \bmod 38 + 2 \cdot 38$~~

modulare Inverse $a \cdot b \bmod m = 1$

a = ? b = 75 m = 38

*

$\underbrace{-1}_{a} \cdot 75 \bmod 38 = 1$

$= -1 + 38 = 37$

$\mathbb{Z}_1 \{ \dots, -1, 37, \dots \}$ $\mathbb{Z}_{38} \{ 0, \dots, 37 \}$

$a = 37$ $b = 75$: $37 \cdot 75 \bmod 38 = 1$

$b = 17$ $m = 64$ $a \cdot b \bmod m = 1$

a ↑ gesucht

1. ggT (17, 64) 2.

$64 = 3 \cdot 17 + 13$

$17 = 1 \cdot 13 + 4$

$13 = 3 \cdot 4 + 1$

$4 = 4 \cdot 1 + 0 \Rightarrow$ ggT (17, 64) = 1 ✓

$13 = 64 - 3 \cdot 17$

$4 = 17 - 1 \cdot 13$

$\Rightarrow 1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 1 \cdot 13)$

$= 13 - 3 \cdot 17 + 3 \cdot 13 = 4 \cdot 13 - 3 \cdot 17$

$= -3 \cdot 17 + 4 (64 - 3 \cdot 17)$

$= -3 \cdot 17 + 4 \cdot 64 - 12 \cdot 17$

$1 = -15 \cdot 17 + 4 \cdot 64$

$1 = \underbrace{-15}_{\text{mod } a} \cdot 17 \bmod 64 + 4 \cdot 64 \bmod 64$

b

mod. Inv.: $-15 \rightarrow -15 + 64 = 49$

$49 \cdot 17 \bmod 64 = 1$

Beispiel

Errechnung modularer Inverse ungleich 1

$b = 3 \qquad m = 9$

$3 = 0 \cdot 9 + 3$ ← 1 = ... ← Geht nicht

$9 = 3 \cdot 3 + 0 \Rightarrow ggT(3, 9) = 3$

Weiter mit ~~funktioniert~~ Krem

$a = 63 \qquad m = 217$

1. ggT finden

$217 = 3 \cdot 63 + 28$

$63 = 2 \cdot 28 + 7$

$28 = 4 \cdot \underset{ggT}{\underline{\underline{7}}} + \underline{\underline{0}}$ geht nicht

---

$a = 64 \qquad m = 217$

① ggT finden

$217 = 3 \cdot 64 + 25$

$64 = 2 \cdot 25 + 14$

$25 = 1 \cdot 14 + 11$

$14 = 1 \cdot 11 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot \underline{\underline{1}} + 0$

Erweiterung

② $25 = 217 - 3 \cdot 64$

$14 = 64 - 2 \cdot 25$

$11 = 25 - 1 \cdot 14$

$3 = 14 - 1 \cdot 11$

$2 = 11 - 3 \cdot 3$

$1 = 3 - 1 \cdot 2 = *$

$ggT(64, 217) = 1$

(2.)

$$
\begin{aligned}
* &= 3 - 1 \cdot (11 - 3 \cdot 3) \\
&= -1 \cdot 11 + 4 \cdot (14 - 1 \cdot 11) \\
&= 4 \cdot 14 - 5 \cdot 11 \\
&= 4 \cdot 14 - 5 \cdot (25 - 1 \cdot 14) \\
&= -5 \cdot 25 + 9 \cdot 14 \\
&= -5 \cdot 25 + 9 \cdot (64 - 2 \cdot 25) \\
&= 9 \cdot 64 - 23 \cdot 25 \\
&= 9 \cdot 64 - 23 \cdot (217 - 3 \cdot 64) \\
1 &= -23 \cdot 217 + 78 \cdot 64
\end{aligned}
$$

$m = 217 \quad a = 64$

$$1 = \underbrace{-23 \cdot 217}_{=0} \bmod 217 + 78 \cdot 64 \bmod 217$$

(78 ist Mod. Inv.)

$78 \cdot 64 \bmod 217 = 1$

78 ist die modulare Inverse zu 64 zum Modul 217.

Cäsar Chiffre

a ... z $\mathbb{Z}_{26}$: $m = 26$

0 25

abc $\longrightarrow$ 0 1 2 $\longrightarrow$ Verschlüsseln

$\{0\,1\,2\} \cdot b \bmod 26 = \{0\,1\,2\} \cdot 3 \bmod 26$

$= \{0\,3\,6\} \bmod 26 = \{0\,3\,6\}$

$= \{a\ d\ g\}$

$a \cdot b \bmod 26 = 1$

~~x~~

~~x~~

3

$3 = 0 \cdot 26 + 3$

$26 = 8 \cdot 3 + 2 \quad 2 = 26 - 8 \cdot 3$

$3 = 1 \cdot 2 + 1 \quad 1 = 3 - 1 \cdot 2$

$2 = 2 \cdot 1 + 0 \Rightarrow ggT(3, 26) = 1$

$3 - 1(26 - 8 \cdot 3) = 9 \cdot 3 - 1 \cdot 26$

$1 = \underset{\uparrow}{9} \cdot 3 \bmod 26 + \underbrace{(-1) \cdot 26 \bmod 26}_{0}$

a

Entschlüsseln

$\{a\ d\ g\} = \{0\ 3\ 6\}$

$\{0\ 3\ 6\} \cdot a = \{0\,3\,6\} \cdot 9 \bmod 26 = \{0\ 27\ 54\} \bmod 26$

$\{0\ 1\ 2\} = \{a\ b\ c\}$ //

Kodieren

1. Additiv $x + t \bmod m \longrightarrow x - t \bmod m$
2. Multiplikativ $x \cdot a \bmod m \longrightarrow x \cdot b \bmod m$

1. + 2. Kodieren $x + t \bmod m = y \quad y \cdot a \bmod m = z$
2. + 1. Dekodieren $z \cdot b \bmod m = y - t \bmod m = x$

{Udo} = {20, 3, 14} $\quad a \cdot b \bmod 26 = 3 \cdot 9 \bmod 26 = 1$

1. $t = 16$: $\{20, 3, 14\} + 16 \bmod 26 = \{36, 19, 30\} \bmod 26$
   $\{10, 19, 4\} =$
   {K T E}

2. $a = 3$: $\{10, 19, 4\} \cdot 3 \bmod 26 = \{30, 57, 12\} \bmod 26$
   $\{4, 5, 12\} =$
   Empfänger erhält {E, F, M}

Dekodieren ⇓

~~{E F M}~~

Schritt 2: $\{4, 5, 12\} \cdot 9 \bmod 26 = \{36, 45, 108\} \bmod 26 =$
$\{10, 19, 4\}$

Schritt 1: $\{10, 19, 4\} - 16 \bmod 26 = \{-6, 3, -12\} \bmod 26$
$\{20, 3, 14\} \bmod 26$
{U D O}

RSA - Verschlüsselung

Asymmetrisch weil es öffentliche und private Schlüssel gibt.

Große Zahlen sicherer:

$$x \cdot a \longrightarrow x^e = y \qquad y \cdot b \rightarrow y^d$$

$x^{p-1} \bmod p = 1$, wenn p eine Primzahl ist und $x \in \mathbb{Z}$ und p teilerfremd (relativ prim) sind

kleiner Satz von Fermat

$$x^p \cdot b \bmod p = x^{p-1} \bmod p = 1$$

↑ modulare Inverse

auch Entdeckung der Null und Fermat/Singh

Wie finde ich "e" und "d"

1. p, q Primzahlen (mgl. groß)
2. $n = p \cdot q \qquad m = (p-1) \cdot (q-1)$
3. Wähle e so, dass es teilerfremd zu m ist
   $ggT(e, m) = 1$
4. d ist die modulare Inverse von e zum Modul m
   $e \cdot d \bmod m = 1$
5. (n, e) öffentl. Schlüssel, (n, d) privater Schlüssel
   p, q, m werden nicht benötigt, bleiben jedoch geheim

Kodierung: $x^e \bmod n = y$

Dekodierung: $y^d \bmod n = x$

Beispiel:

1. $p = 11 \qquad q = 7$
2. $n = 11 \cdot 7 = 77 \qquad m = (11-1)\cdot(7-1) = 60$
3. $ggT(e, 60) = 1$

   Suche nach "e" → z.B. $e = 7$

$60 = 8 \cdot 7 + 4 \qquad 4 = 60 - 8 \cdot 7$

$7 = 1 \cdot 4 + 3 \qquad 3 = 7 - 1 \cdot 4$

$4 = 1 \cdot 3 + 1 \qquad 1 = 4 - 1 \cdot 3$

$3 = 3 \cdot 1 + 0 \Rightarrow ggT(7, 60) = 1$

4. $7 \cdot d \bmod 60 = 1$

   $d = 43$

$= 4 - 1 \cdot (7 - 1 \cdot 4) = 2 \cdot 4 - 1 \cdot 7$

$= 2 \cdot (60 - 8 \cdot 7) - 1 \cdot 7$

$1 = -17 \cdot 7 + 2 \cdot 60$

$1 = -17 \cdot 7 \bmod 60$

$1 = 43 \cdot 7 \bmod 60$

5. $(77, 7)$ öffentl. Schlüssel $(77, 43)$ priv. Schlüssel

Verschlüsseln von "2" und "4":

$\{2, 4\}^7 \bmod 77 = \{51, 60\}$

Kode zur Kodierung

$2^7 = 128 \qquad 4^7 = 16384$

$\{51, 60\}^{43} \bmod 77 = \{2, 4\}$

Problem der berechnenden Maschine

Wie berechne ich $51^{43} \bmod 77$?

$$a^2 \bmod m = a \cdot a \bmod m$$

$$= (a(\underbrace{a \cdot \bmod m) \bmod m}_{2\text{-mal}})$$

Weil sonst Speicher voll, Nutzung von Schleifen

$$51(51(\underbrace{51 \bmod 77}_{43\text{ mal}}) \bmod 77) \bmod 77$$

$\Downarrow$

würde 2 ergeben