19. Vorlesung 24.11.2020

Notiztitel 24.11.2020

Allgemein gilt:

Satz (chinesischer Restsatz für zwei simultane Kongruenzen):
Die simultanen Kongruenzen

$$\overline{x} = \overline{n} \text{ in } \mathbb{Z}_{m_1} \text{ und } \overline{x} = \overline{k} \text{ in } \mathbb{Z}_{m_2}$$

sind lösbar, wenn gilt: $\operatorname{ggT}(m_1, m_2) = 1$.

Es gilt dann: $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$ ist **eine** Lösung, falls gilt $\overline{a} \cdot \overline{m_2} = \overline{1}$ in $\mathbb{Z}_{m_1}$ und $\overline{b} \cdot \overline{m_1} = \overline{1}$ in $\mathbb{Z}_{m_2}$.

Weitere (positive) Lösungen sind $x = x_0 + i \cdot m_1 \cdot m_2$ für $i \in \mathbb{Z}$ (solange $x \geq 0$ gilt).

Beweis: ① $\operatorname{ggT}(m_1, m_2) = 1 \Rightarrow$ (euklid. Algor. & Lemma von Bézout)

a) es existiert $\overline{a}$ in $\mathbb{Z}_{m_1}$ mit $\overline{a} \cdot \overline{m_2} = \overline{1}$ in $\mathbb{Z}_{m_1}$;

b) es existiert $\overline{b}$ in $\mathbb{Z}_{m_2}$ mit $\overline{b} \cdot \overline{m_1} = \overline{1}$ in $\mathbb{Z}_{m_2}$

② Bilde $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$ mit a, b aus ①, dann gilt

2.1 in $\mathbb{Z}_{m_1}$:

$$\overline{x_0} = \overline{n \cdot a \cdot m_2 + k \cdot b \cdot m_1} = \overline{n} \cdot \underbrace{\overline{a} \cdot \overline{m_2}}_{\overset{a)}{=} \overline{1}} + \overline{k} \cdot \overline{b} \cdot \underbrace{\overline{m_1}}_{= \overline{0}} = \overline{n}$$

2.2 in $\mathbb{Z}_{m_2}$:

$$\overline{x_0} = \overline{n \cdot a \cdot m_2 + k \cdot b \cdot m_1} = \overline{n} \cdot \overline{a} \cdot \underbrace{\overline{m_2}}_{= \overline{0}} + \overline{k} \cdot \underbrace{\overline{b} \cdot \overline{m_1}}_{\overset{b)}{=} \overline{1}} = \overline{k}$$

Beispiel: Lösen Sie folgende simultane Kongruenzen

$\overline{x} = \overline{10}$ in $\mathbb{Z}_{101}$ $\rightarrow$ $x \equiv 10 \bmod 101$

$\overline{x} = \overline{11}$ in $\mathbb{Z}_{47}$ $\rightarrow$ $x \equiv 11 \bmod 47$

} alternative Schreibweise

Geben Sie auch die kleinste pos. Zahl x an, die die gegebenen simultanen Kongruenzen löst.

① $\operatorname{ggT}(101, 47)$ bestimmen

$101 = 2 \cdot 47 + 7$

$47 = 6 \cdot 7 + 5$

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$ ← $\operatorname{ggT}(101, 47) = 1$

$2 = 2 \cdot 1 + 0$

$\Rightarrow$ Problem lösbar

② Lemma von Bézout anwenden und Inverse (bzgl. Mult.) bestimmen

$$\begin{aligned}
1 &= 5 - 2\cdot 2 \\
&= 5 - 2\cdot(7 - 1\cdot 5) \\
&= (-2)\cdot 7 + 3\cdot 5 \\
&= (-2)\cdot 7 + 3\cdot(47 - 6\cdot 7) \\
&= 3\cdot 47 - 20\cdot 7 \\
&= 3\cdot 47 - 20\cdot(101 - 2\cdot 47) \\
&= (-20)\cdot 101 + 43\cdot 47
\end{aligned}$$

(2.1) In $\mathbb{Z}_{47}$ gilt

$$\overline{1} = \overline{(-20)\cdot 101 + 43\cdot 47} = \overline{(-20)}\cdot\overline{101} + \underbrace{\overline{43}\cdot\overline{47}}_{=\overline{0}} = \overline{(-20)}\cdot\overline{101}$$

Inverse zu $\overline{101}$ in $\mathbb{Z}_{47}$ ist $\overline{(-20)} = \overline{(-20+47)} = \overline{27}$ ← b

(2.2) In $\mathbb{Z}_{101}$ gilt

$$\overline{1} = \overline{(-20)\cdot 101 + 43\cdot 47} = \overline{(-20)}\cdot\underbrace{\overline{101}}_{=\overline{0}} + \overline{43}\cdot\overline{47} = \overline{43}\cdot\overline{47}$$

Inverse zu $\overline{47}$ in $\mathbb{Z}_{101}$ ist $\overline{43}$ ← a

③ Insgesamt: $x_0 = a\cdot 47\cdot 10 + b\cdot 101\cdot 11$

$$= 43\cdot 47\cdot 10 + 27\cdot 101\cdot 11 = 50207$$

$x_0 = 50207$ ist <u>eine</u> Lösung der geg. simultanen Kongruenzen.
Weitere Lösungen sind $x = x_0 + k\cdot 47\cdot 101$ mit $k\in\mathbb{Z}$, mit $k=-10$ erhält man $x = 50207 - 47470 = 2737$ als kleinste positive Lösung!

<u>Bemerkung:</u>

$\overline{x} = \overline{n_1}$ in $\mathbb{Z}_{m_1}$ → a_1 mit $\overline{a_1}\cdot\overline{m_2} = \overline{1}$ in $\mathbb{Z}_{m_1}$

$\overline{x} = \overline{n_2}$ in $\mathbb{Z}_{m_2}$ → a_2 mit $\overline{a_2}\cdot\overline{m_1} = \overline{1}$ in $\mathbb{Z}_{m_2}$

⇒ $x = n_1\cdot a_1\cdot m_2 + n_2\cdot a_2\cdot m_1$ löst die simultanen Kongruenzen

$$= n_1\cdot a_1\cdot\frac{m_2\cdot m_1}{m_1} + n_2\cdot a_2\cdot\frac{m_2\cdot m_1}{m_2}$$

$$= n_1\cdot a_1\cdot\frac{M}{m_1} + n_2\cdot a_2\cdot\frac{M}{m_2} \quad \leftarrow M = m_1\cdot m_2$$

$\overline{a_1}\cdot\overline{\left(\frac{M}{m_1}\right)} = \overline{1}$ in $\mathbb{Z}_{m_1}$

$\overline{a_2}\cdot\overline{\left(\frac{M}{m_2}\right)} = \overline{1}$ in $\mathbb{Z}_{m_2}$

$$= \sum_{i=1}^{2} n_i\cdot a_i\cdot\frac{M}{m_i} \quad \text{mit } \overline{a_i}\cdot\overline{\left(\frac{M}{m_i}\right)} = \overline{1} \text{ in } \mathbb{Z}_{m_i}$$

andere Darstellung des chin. Restsatzes für 2 Kongruenzen

Diese Darstellung liefert sofort folgende Verallgemeinerung

Satz (Chin. Restsatz für mehrere simultane Kongruenzen)

Die k simultanen Kongruenzen

$$\bar{x} = \bar{n}_i \text{ in } \mathbb{Z}_{m_i} \quad 1 \leq i \leq k$$

sind lösbar, falls gilt $ggT(m_i, m_j) = 1$ für $i \neq j$, $1 \leq i, j \leq k$.
Es gilt dann

$$x_0 = \sum_{i=1}^{k} n_i \cdot a_i \cdot \frac{M}{m_i} \quad \text{ist eine Lösung}$$

mit $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ und $\bar{a}_i \cdot \overline{\left(\frac{M}{m_i}\right)} = \bar{1}$ in $\mathbb{Z}_{m_i}$, $1 \leq i \leq k$.

Weitere Lösungen sind $x = x_0 + l \cdot M$ für $l \in \mathbb{Z}$.

(Beispiel: siehe Skript S. 66/67)

Anwendung modularer Arithmetik (= Rechnen mit Restklassen):

Algorithmen zur Verschlüsselung von Daten!

hier: Grundidee des RSA - Algorithmus (asymmetrische Verschlüsselung)

Rivest, Shamir, Adelman

Sender und Empfänger der Daten haben verschiedene Schlüssel

Empfänger (E) hat einen „privaten" Schlüssel und einen „öffentlichen" Schlüssel

Sender (S) kennt (erhält) den öffentlichen Schlüssel des Empfänger E

S verschlüsselt seine Daten mit dem öffentl. Schlüssel von E und sendet diese (verschlüsselten) Daten an E.
Nur E kann mit seinem (geheim gehaltenen) privaten Schlüssel die verschlüsselten Daten von S entschlüsseln.

Damit ist der Ablauf des Verfahrens klar aber wie/warum funktioniert das?

Konkretes Beispiel (Skript S. 68-72)

Sender (S) ist Student und möchte Empfänger E (Prof. K) verschlüsselt mitteilen das MATHE sein Lieblingsfach ist!

① Kodierung des Wortes MATHE in Zahlen

Text	A	B	C	...	Z
Zahl	1	2	3		26

$\Rightarrow$ MATHE $\rightarrow$ 13|1|20|8|5

Sender (S) will die Zahlenfolge 13|1|20|8|5 verschlüsselt senden

② Schlüsselgenerierung (Ist vor ① gelaufen)

Der Empfänger E nimmt eine sehr große natürliche Zahl N, die das Produkt zweier sehr großer Primzahlen ist: $N = p \cdot q$

p, q Primzahlen (mit mehreren hundert Dezimalstellen)

N ist dann (momentan) auch mit den leistungsfähigsten Computern nicht in (endlicher) angemessener Zeit in das Produkt $p \cdot q$ faktorisierbar!

Empfänger E hat $N = p \cdot q$; er nimmt $\tilde{N} = (p-1) \cdot (q-1)$ und rechnet in $\mathbb{Z}_{\tilde{N}}$: Er bestimmt zunächst e mit $0 < e < \tilde{N}$ und $ggT(e, \tilde{N}) = 1$

$\Rightarrow$ e hat in $\mathbb{Z}_{\tilde{N}}$ ein inverses Element bezgl. der Multiplikation d;

der Empfänger berechnet d mit $\overline{d} \cdot \overline{e} = \overline{1}$ in $\mathbb{Z}_{\tilde{N}}$.

Der „öffentliche" Schlüssel des Empfängers ist (N, e).

Der „private" Schlüssel des Empfängers ist (N, d).

Bei hinreichend großem N kann niemand (kein Supercomputer) in (endlicher) angemessener Zeit aus (N, e) den Schlüssel (N, d) berechnen!

Konkretes Beispiel

Empfänger E wählt $N = 33 = 3 \cdot 11$ also $p = 3$, $q = 11$

Empfänger E berechnet $\tilde{N} = (p-1) \cdot (q-1) = 2 \cdot 10 = 20$

E rechnet also in $\mathbb{Z}_{20}$, er wählt $e = 7$ mit $ggT(7, 20) = 1$

und bestimmt d mit $\overline{d} \cdot \overline{e} = \overline{1}$ in $\mathbb{Z}_{20}$: Es ist $\overline{1} = \overline{7} \cdot \overline{3}$ in $\mathbb{Z}_{20}$

$\Rightarrow d = 3$, $\overline{d} = \overline{3}$ in $\mathbb{Z}_{20}$

„öffentlicher" Schlüssel ist $(33, 7)$, „privater" Schlüssel ist $(33, 3)$

③ Sender will 13|1|20|8|5 mit dem „öffentlichen" Schlüssel verschlüsseln.

Für die zu verschlüsselnde Ziffernfolge $a_n a_{n-1} \ldots a_2 a_1 a_0$ muss gelten: $ggT(a_i, N) = 1$

hier im Beispiel: $ggT(33,13)=1$, $ggT(33,1)=1$, $ggT(20,33)=1$, $ggT(8,33)=1$, $ggT(5,33)=1$

Der Sender S rechnet mit dem „öffentlichen" Schlüssel $(N,e)=(33,7)$ in $\mathbb{Z}_{33}$ und zwar

$$\overline{13^7} = \overline{62748517} = \overline{7} \quad \text{denn } 62748517 = 1901470 \cdot 33 + 7$$

$$\overline{1^7} = \overline{1} \quad \text{denn } 1^7 = 1 = 0 \cdot 33 + 1$$

$$\overline{20^7} = \overline{1280000000} = \overline{26} \quad \text{denn } 1280000000 = 38787878 \cdot 33 + 26$$

$$\overline{8^7} = \overline{2097152} = \overline{2} \quad \text{denn } 2097152 = 63550 \cdot 33 + 2$$

$$\overline{5^7} = \overline{78125} = \overline{14} \quad \text{denn } 78125 = 2367 \cdot 33 + 14$$

$\Rightarrow$ Sender verschlüsselt 13|1|20|8|5 in 7|1|26|2|14

(4) Empfänger E bekommt die Ziffernfolge 7|1|26|2|14 und entschlüsselt mit seinem „privaten" Schlüssel $(N,d)=(33,3)$ und zwar durch Rechnung in $\mathbb{Z}_{33}$:

$$\overline{7^3} = \overline{343} = \overline{13} \quad \text{denn } 343 = 10 \cdot 33 + 13$$

$$\overline{1}^3 = \overline{1} \quad \text{denn } 1 = 0 \cdot 33 + 1$$

$$\overline{26^3} = \overline{17567} = \overline{20} \quad \text{denn } 17567 = 532 \cdot 33 + 20$$

$$\overline{2}^3 = \overline{8} \quad \text{denn } 8 = 0 \cdot 33 + 8$$

$$\overline{14^3} = \overline{2744} = \overline{5} = 2744 = 83 \cdot 33 + 5$$

$\Rightarrow$ Empfänger nimmt 13|1|20|8|5 als entschlüsselte Nachricht, dekodieren mit Buchstabentabelle liefert: MATHE

Theorie dazu (warum funktioniert dieses Verfahren): Vorlesung morgen!