Prof. Dr. M. Helbig
Mathematik – Übung

Hochschule Rosenheim
University of Applied Sciences

Chinesischer Restsatz, Kryptographie

Chinesischer Restsatz. Für welche Zahlen $x \in \mathbb{Z}$ gilt

1. $x \equiv 3 \pmod 2$,
   $x \equiv 3 \pmod 5$,
   $x \equiv 3 \pmod 7$.

2. $x \equiv 1 \pmod 2$,
   $x \equiv 3 \pmod 4$.

3. Was sind die jeweils kleinsten positiven x in ~~a)~~ 1. und ~~b)~~ 2.?

Lösung. ⚠ Voraussetzung von CRS prüfen: Module paarw. teilerfremd!

1. 2, 5, 7 sind verschiedene Primzahlen und somit paarw. teilerfremd!

$x \equiv 3 \pmod 2$	$k_1 = 5 \cdot 7 = 35$	$\underbrace{35}_{1} \cdot 1 \equiv 1 \pmod 2$	$x_1 = 1$
$x \equiv 3 \pmod 5$	$k_2 = 2 \cdot 7 = 14$	$14 \cdot 4 \equiv 1 \pmod 5$	$x_2 = 4$
$x \equiv 3 \pmod 7$	$k_3 = 2 \cdot 5 = 10$	$\underbrace{10}_{3} \cdot 5 \equiv 1 \pmod 7$	$x_3 = 5$

Allg.lsg: $x = 3 \cdot 35 \cdot 1 + 3 \cdot 14 \cdot 4 + 3 \cdot 10 \cdot 5 + k(2 \cdot 5 \cdot 7)$
$= 105 + 168 + 150 + k \cdot 70$
$= 423 + k \cdot 70$

2. Module 2, 4 nicht teilerfremd, d.h. CRS nicht anwendbar!
Streiche zuerst die zweite Kongruenz und löse:
$x \equiv 1 \bmod 2 \iff \boxed{x \overset{(*)}{=} 1 + k \cdot 2}$ (alle ungeraden Zahlen $\ldots, -1, 1, 3, 5, 7, \ldots$)
Setze dies in die zweite Kongruenz ein:
$1 + k \cdot 2 \equiv 3 \bmod 4 \iff 1 + k \cdot 2 = 3 + \ell \cdot 4 \overset{-1}{\iff} k \cdot 2 = 2 + \ell \cdot 4$
$\overset{:2}{\iff} k = 1 + \ell \cdot 2$, setze dies in (*)
$\Rightarrow x \overset{(*)}{=} 1 + (1 + \ell \cdot 2)\, 2 = 1 + 2 + \ell \cdot 4 = 3 + \ell \cdot 4$ $(\ldots, -5, -1, 3, 7, 11, \ldots)$

3. 1.: $x = 423 + k \cdot 70 \Rightarrow x = 423 - 6 \cdot 70 = 3.$

2.: $x = 3 + l \cdot 4 \Rightarrow x = 3 + 0 \cdot 4 = 3.$

Eigener Lösungsversuch.

Rechnen mit großen Zahlen mit CRS. In C kann man mittels des Datentyps `unsigned long long` (nur) 64-bit Zahlen darstellen, also Zahlen x mit

$$0 \leq x \leq 2^{64} - 1 = 18.446.744.073.709.551.615.$$

In der Kryptographie braucht man aber viel größere Zahlen (z.B. in RSA hat der Modul mindestens 1024 Bit, also 309 Dezimalstellen!). Eine Möglichkeit zur Darstellung und dem Rechnen mit großen Zahlen bietet der Chinesische Restsatz:

Wenn $m_1, m_2, \ldots, m_n$ paarweise teilerfremd (und groß, aber noch im Datentyp darstellbar!) sind und $m = m_1 m_2 \cdots m_n$ (riesengroß!), so kann jede Zahl x mit $0 \leq x \leq m$ eindeutig durch ihre Reste $a_k = x \bmod m_k$ $(1 \leq k \leq n)$ repräsentiert werden:

$$x \leftrightarrow (a_1, \ldots, a_n).$$

Beispiel: $m_1 = 9$, $m_2 = 8$. Dann ist etwa $39 \overleftrightarrow{=} (3, 7)$, denn $39 \equiv 3 \pmod 9$ und $39 \equiv 7 \pmod 8$. Umgekehrt kann zu jedem Tupel mithilfe des chinesischen Restsatzes die Zahl rekonstruiert werden: man erhält $x = 39$ als eindeutige Lösung von

$$x \equiv 3 \,(\text{mod } 9),$$
$$x \equiv 7 \,(\text{mod } 8).$$

Wir addieren und multiplizieren jetzt x, y nicht direkt, sondern rechnen mit den Resten: Sind $x \leftrightarrow (a_1, \ldots, a_n)$, $y \leftrightarrow (b_1, \ldots, b_n)$ zwei Zahlen, so entspricht

$$x + y \leftrightarrow ((a_1 + b_1) \bmod m_1, \ldots, (a_n + b_n) \bmod m_n),$$
$$x \cdot y \leftrightarrow ((a_1 \cdot b_1) \bmod m_1, \ldots, (a_n \cdot b_n) \bmod m_n).$$

Fazit: Anstatt mit den großen Zahlen x, y zu rechnen, wird mit den kleineren Resten gerechnet und am Ende das Ergebnis mit dem chinesischen Restsatz zurückgerechnet. (Die einzelnen Reste können parallel berechnet werden, Stichworte: Nebenläufigkeit und Multicore-Rechner! In der Praxis verwendet man für die Module m_k Zahlen der Form $2^l - 1$, da sich die Modulo-Rechnung für diese Zahlen binär gut implementieren lässt.)

Jetzt zur eigentlichen **Aufgabe** - wir rechnen leider nur exemplarisch mit kleinen Zahlen :'-(. Angenommen, Ihre Lieblingsprogrammiersprache kann nur 4-bit Zahlen x mit

$$0 \leq x \leq 2^4 - 1 = 15$$

darstellen. Sie möchten aber auch 9-bit Zahlen x mit

$$0 \leq x \leq 2^9 - 1 = 511$$

addieren und multiplizieren.

1. Wählen Sie passende Module, um nach obigem Verfahren
2. $459 + 510$ und
3. $459 \cdot 510$ zu berechnen.

Lösung.

1. Für die Module habe ich $0, \dots, 15$ zur Verfügung: Wähle maximale Primzahlpotenzen (sind teilerfremd!):

$$0 \le m_1 = 2^3 = 8,\ m_2 = 3^2 = 9,\ m_3 = 5,\ m_4 = 7,\ m_5 = 11,\ m_6 = 13 \le 15$$

$$\Rightarrow m = m_1 \cdots m_6 = 360.360$$

2.
$$459 \leftrightarrow (459 \bmod 8, 459 \bmod 9, 459 \bmod 5, 459 \bmod 7, 459 \bmod 11, 459 \bmod 13)$$
$$= (3, 0, 4, 4, 8, 4)$$
$$+\ 510 \leftrightarrow (6, 6, 0, 6, 4, 3)$$
$$(9, 6, 4, 10, 12, 7)$$
$$\|\|\|\|\|\|\|\|\|$$
$$131$$

6 Threads parallel

Mit CRS entspricht dies x mit

$x \equiv 1 \pmod 8$	$k_1 = 9 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 45.045$
$x \equiv 6 \pmod 9$	$k_2 = 8 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 40.040$
$x \equiv 4 \pmod 5$	$k_3 = 8 \cdot 9 \cdot 7 \cdot 11 \cdot 13 = 72.072$
$x \equiv 3 \pmod 7$	$k_4 = 8 \cdot 9 \cdot 5 \cdot 11 \cdot 13 = 51.480$
$x \equiv 1 \pmod{11}$	$k_5 = 8 \cdot 9 \cdot 5 \cdot 7 \cdot 13 = 32.760$
$x \equiv 7 \pmod{13}$	$k_6 = 8 \cdot 9 \cdot 5 \cdot 7 \cdot 11 = 27.720$

$$\overbrace{45.045}^{5} \cdot \square \equiv 1 \pmod 8 \Rightarrow x_1 = 5$$
$$\overbrace{40.040}^{8} \cdot \square \equiv 1 \pmod 9 \Rightarrow x_2 = 8$$
$$\vdots$$

$$x = 1 \cdot 45045 \cdot 5 + 6 \cdot 40.040 \cdot 8 + \dots + k \cdot 360.360 \equiv 969 \pmod{360.360}$$

3. analog multiplizieren!

Eigener Lösungsversuch.

Lineare Kryptographie. Es wird mit $E(x) = (a \cdot x + b) \bmod 26$ verschlüsselt. Dabei ist $0 \leq x < 26$ die Nummer des zu verschlüsselnden Buchstabens (0-25 entspricht a-z).

1. Sei $a = 3, b = 2$. Verschlüsseln Sie „informatik“ und entschlüsseln Sie „ismvkhob“.
2. Geben Sie die Entschlüsselung als Funktion $D(x)$ an. Welche Zahlen $0 \leq a, b < 26$ sind für eine eindeutige Ver-/Entschlüsselung geeignet?
3. Gibt es Zahlen $0 \leq a, b < 26$, so dass $E(x) = D(x)$ für alle $0 \leq x < 26$?

Lösung. 1. $E(x) = (3x + 2) \bmod 26$

a-z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
x = 0-25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
y=E(x)	2		8			17			0		6		12	15	18	21		1		7	10					
a-z	c		i			r			a		g		m	p	s	v		b		h	k					

Verschlüsselung: "informatik" $\xmapsto{E}$ "aprsbmchag"

Entschlüsselung über Umkehrfkt von E: $y = 3x+2 \iff y-2 = 3x \iff x = 9\cdot(y-2)$ ($9 = 3^{-1}$ in $\mathbb{Z}_{26}$)

"ismvkhob" $\xmapsto{E^{-1}=D}$ "computer"

$y = 8$

$x = 9\cdot(8-2) = 54 \equiv 2$

2. $E(x) = (ax+b) \bmod 26 \iff x = a^{-1}(y-b) \bmod 26$, also $D(y) = a^{-1}(y-b)$

(y = y; a^{-1} in $\mathbb{Z}_{26}$)

d.h. b beliebig, aber a muss invertierbar in $\mathbb{Z}_{26}$ sein $\iff ggT(a, 26) = 1$ (2·13)

$\iff a \in \{1,3,5,7,9,11,15,17,19,21,23,25\}$

($\varphi(26) = 1 \cdot 12 = 12$ Stück)

3. $E(x) = D(x)\ (\forall x \in \mathbb{Z}_{26}) \iff ax + b = a^{-1}(x-b)\ (\forall x \in \mathbb{Z}_{26})$

$a^{-1}x - a^{-1}b$

Koeffvgl: $a = a^{-1}$, $b = -a^{-1}b$

$\Downarrow$

$a \cdot a = 1$

Probieren: $a = 1, 25$

1. Fall: $a = 1$: $b = -b \Rightarrow 2b = 0 \Rightarrow b = 0, 13$

2. Fall: $a = 25$: $b = -25b \Rightarrow \underbrace{26}_{0}b = 0$ d.h. b beliebig.

Eigener Lösungsversuch.