Aufgabe (Verwendung der Gruppe $(\mathbb{Z}_n, +)$ anstatt $(\mathbb{Z}_n^*, \cdot)$)

Ein Student schlägt das folgende Protokoll als Vereinfachung des Shamirschen No-Key-Protokolls vor. Ziel des Protokolls ist die sichere Übertragung einer Nachricht $m \in \mathbb{Z}_n^*$ von A zu B. Dabei ist n eine öffentlich bekannte Primzahl.

Teilnehmer A		*Teilnehmer* B
Wählt $a \in_{\mathrm{R}} \mathbb{Z}_n^*$ zufällig und berechnet $c := m \cdot a \bmod n$.		
	$\xrightarrow{c}$	
		Wählt $b \in_{\mathrm{R}} \mathbb{Z}_n^*$ zufällig und berechnet $d := c \cdot b \bmod n$.
	$\xleftarrow{d}$	
Berechnet $e := d \cdot a^{-1} \bmod n$.		
	$\xrightarrow{e}$	
		Berechnet $m = e \cdot b^{-1} \bmod n$.

Beschreiben Sie, wie ein Angreifer, der n kennt und außerdem die verschickten Chiffren c, d und e abfangen konnte, die Verschlüsselung brechen kann.

Antwort

Bekannt ist:

- $c = m \cdot a$
- $d = m \cdot a \cdot b$
- $e = m \cdot a \cdot b \cdot a^{-1} = m \cdot b$

Berechne

$$\underbrace{(ma)}_{=c} \cdot \underbrace{(mb)}_{=e} \cdot \underbrace{(mab)^{-1}}_{=d^{-1}} = m$$

Konvention
Wir schreiben: $a \perp b \;\Leftrightarrow\; \operatorname{ggT}(a, b) = 1$

Chinesischer Restsatz
Gibt es eine Lösung x des Systems von linearen Kongruenzen

$$\begin{aligned} c_1 x &\equiv d_1 \pmod{m} \\ c_2 x &\equiv d_2 \pmod{n} \end{aligned}$$

wobei $c_1 \in \mathbb{Z}_m^*, c_2 \in \mathbb{Z}_n^*,\; m \perp n$?

Zunächst:

$$\begin{aligned} x &\equiv c_1^{-1} d_1 \pmod{m} \\ x &\equiv c_2^{-1} d_2 \pmod{n} \end{aligned}$$

Setze $a := c_1^{-1} d_1,\ b := c_2^{-1} d_2$.

Wir suchen also eine Lösung x von

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

Beispiel. Wir haben x Kekse. Wenn wir die Kekse auf 5 Freunde verteilen, bleiben 2 übrig, wenn wir sie auf 7 Freunde verteilen bleiben 4 übrig.

$$x \equiv 2 \pmod{5}$$
$$x \equiv 4 \pmod{7}$$

Wie viele Kekse könnten wir haben?

$$32, 67, 102, ..., 942, ..., 1782, ... \text{ (Es gibt unendlich viele Lösungen.)}$$

Allgemein: Falls $m \perp n$, können wir $m^{-1}_{\text{mod } n}$ und $n^{-1}_{\text{mod } m}$ bestimmen.

Für obiges Problem lautet eine Lösung:

$$x = (an^{-1}_{\text{mod } m} n + bm^{-1}_{\text{mod } n} m) \bmod mn \qquad \in \mathbb{Z}_{mn}$$

denn

$$x = an^{-1}_{\text{mod } m} n + bm^{-1}_{\text{mod } n} m \equiv a \underbrace{n^{-1}_{\text{mod } m} n}_{\equiv 1} \equiv a \pmod{m}$$
$$x = an^{-1}_{\text{mod } m} n + bm^{-1}_{\text{mod } n} m = b \underbrace{m^{-1}_{\text{mod } n} m}_{\equiv 1} \equiv b \pmod{n}$$

Beispiel. Für obiges Beispiel:

$$x \equiv 2 \pmod{5}$$
$$x \equiv 4 \pmod{7}$$

$$3 \equiv 7^{-1} \pmod{5}$$
$$3 \equiv 5^{-1} \pmod{7}$$

d.h.

$$\begin{aligned} & 2 \cdot 7^{-1}_{\text{mod } 5} \cdot 7 + 4 \cdot 5^{-1}_{\text{mod } 7} \cdot 5 \bmod 35 \\ &= 2 \cdot 3 \cdot 7 + 4 \cdot 3 \cdot 5 \bmod 35 \\ &= 42 + 60 \bmod 35 \\ &= 32 \text{ ist eine Lösung} \end{aligned}$$

Satz 1 (Chinesischer Restsatz (Spezialfall))**.** *Zu jedem Paar $(a, b) \in \mathbb{Z}_m \times Z_n, m \perp n$ haben die Kongruenzen*

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

die eindeutige gemeinsame Lösung

$$x = (an^{-1}_{\text{mod } m} n + bm^{-1}_{\text{mod } n} m) \bmod (mn) \in \mathbb{Z}_{mn}.$$

Beweis. Definiere die Funktion

$$\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

mit

$$\psi(x) := (x \bmod m, x \bmod n).$$

Wir zeigen: ψ ist bijektiv, damit folgt sowohl die Existenz als auch die Eindeutigkeit.

- ψ ist surjektiv: Für beliebige $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ ist x mit

  $$x := \psi^{-1}(a, b) = (an^{-1}_{\bmod m} n + bm^{-1}_{\bmod n} m) \bmod (mn) \in \mathbb{Z}_{mn}$$

  ein Wert, der das lineare Kongruenzsystem

  $$\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod n \end{aligned}$$

  erfüllt, d.h. $\psi(x) = (a, b)$

- ψ ist injektiv: Da

  $$|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = m \cdot n = |\mathbb{Z}_{mn}|,$$

  und jedes Paar $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ ein Urbild in Z_{mn} hat, kann es höchstens ein $x \in \mathbb{Z}_{mn}$ geben mit $\psi(x) = (a, b)$.

- d.h. ψ ist bijektiv.

$\square$

Satz 2 (Chinesischer Restsatz)**.** *Seien $n_1, ..., n_k$ paarweise teilerfremd. Zu jedem Tupel $(a_1, ..., a_k) \in \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &... \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Dann ist für $n = \prod_{i=1}^{k} n_i$

$$x = \left(\sum_{i=1}^{k} a_i \cdot \left(\frac{n}{n_i}\right)^{-1}_{\bmod n_i} \cdot \frac{n}{n_i} \right) \bmod n \qquad \in \mathbb{Z}_{n_1 \cdot ... \cdot n_k}$$

eine eindeutige gemeinsame Lösung.

Notation:

$$(a_1, ..., a_k) \circ\!\!-\!\!\bullet\; x$$

Folgerung 3. *Für a, b mit*

$$(a_1, ..., a_k) \circ\!\!-\!\!\!\bullet\ a \quad \textit{und}\ (b_1, ..., b_k) \circ\!\!-\!\!\!\bullet\ b$$

folgt:

$$(a_1 \circ b_1, ..., a_k \circ b_k) \circ\!\!-\!\!\!\bullet\ a \circ b \qquad (\circ \in \{+, \cdot\})$$

Anwendung:
Rechnung von großen Zahlen kann auf Rechnungen kleiner Zahlen reduziert werden.
Seien $p_1, ..., p_k$ die ersten k Primzahlen.

$$\begin{tikzcd}
a, b < 2^n \arrow[r, "\text{direkte Multiplikation}"] \arrow[d, "\substack{\text{modulo} \\ p_1,\dots,p_k}"'] & a \cdot b \\
\substack{(a_1, ..., a_k) \\ (b_1, ..., b_k)} \arrow[r, "\substack{\text{komponentenweise} \\ \text{Multiplikation}}"] & (a_1 b_1 \bmod p_1, ..., a_k b_k \bmod p_k) \arrow[u, "\substack{\text{Rücktrans-} \\ \text{formation} \\ \text{mittels} \\ \text{Chin. Rests.}}"']
\end{tikzcd}$$

Das Produkt $a \cdot b$ ist $< 2^{2n}$. Wähle k so, dass $\prod_{i=1}^{k} p_i \geq 2^{2n}$. Da $p_i \geq 2$ kann man $k \leq 2n$ wählen.
Beispiel. mit $n_1 = 5$ und $n_2 = 7$ und $n = n_1 \cdot n_2 = 35$.

		a_2						
		0	1	2	3	4	5	6
	0	0	15	30	10	25	5	20
	1	21	1	16	31	11	26	6
a_1	2	7	22	2	17	32	12	27
	3	28	8	23	3	18	33	13
	4	14	29	9	24	4	19	34

Besonders markiert sind die 4 Quadratwurzeln der 1, nämlich

$$(1, 1), \quad (1, 6) = (1, -1), \quad (4, 1) = (-1, 1), \quad (4, 6) = (-1, -1)$$

Es gilt (siehe Folgerung 3):

$$\Big((\pm 1, \pm 1)\Big) = \Big((\pm 1)^2, (\pm 1)^2\Big) = \Big(1, 1\Big) \circ\!\!-\!\!\!\bullet\ 1$$

Fazit: Wenn n in k teilerfremde Faktoren zerfällt, n ungerade, $n = n_1 \cdot ... \cdot n_k$, dann gibt es mindestens 2^k Quadratwurzeln der 1. Diese entsprechen den Zahlen $(\pm 1, \pm 1, ..., \pm 1)$.

Ausnahme: Wenn man modulo $n_i = 2$ rechnet, dann ist $-1 \equiv 1$. In diesem Fall gibt es mindestens 2^{k-1} Quadratwurzeln.

Aufgabe: Welche Rechenzeit benötigt die Transformation $(a_1, ..., a_k) \circ\!\!-\!\!\bullet\ x$ von links nach rechts als Funktion von m (=Anzahl der Bits der beteiligten Zahlen) und k.
Antwort:

- Von rechts nach links:

  $$x \mapsto (x \bmod n_1, ..., x \bmod n_k)$$

  Dies erfordert k-mal Division mit Rest: $\mathcal{O}(k\dot{m}^2)$

- Von links nach rechts:

  $$(a_1, ..., a_k) \mapsto x$$

  k-mal Extended Euklid anwenden und die Summe

  $$x = \left(\sum_{i=1}^{k} a_i \cdot \left(\frac{n}{n_i}\right)^{-1}_{\bmod n_i} \cdot \frac{n}{n_i} \right) \bmod n$$

  bilden: $\mathcal{O}(k \cdot m^3)$

Beziehung zwischen $\mathbb{Z}_m^*$, $\mathbb{Z}_n^*$ und $\mathbb{Z}_{mn}^*$

Wir wollen zeigen: Für $m \perp n$ ist $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*|$.

Wir zeigen: Für $x \in \mathbb{Z}_{mn}^*$ ist

$$\psi(x) \coloneqq (x \bmod m, x \bmod n) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*.$$

Wir zeigen $x \bmod m \in \mathbb{Z}_m^*$. Der zweite Parameter kann analog geschlussfolgert werden.

$$\begin{aligned}
x \perp mn \quad &\Rightarrow \quad x \perp m \ \wedge \ x \perp n \\
&\Rightarrow \quad \mathrm{ggT}(x, m) = 1 \\
&\overset{\text{Euklid}}{\Rightarrow} \quad \mathrm{ggT}(x, m) = \mathrm{ggT}(m, x \bmod m) = 1 \\
&\Rightarrow \quad (x \bmod m) \perp m
\end{aligned}$$

Analog zu oben zeigt man, das $\psi : \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ bijektiv ist.

Folgerung 4. *Für $m \perp n$ ist $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*|$.*

Profil

Es gelte $a^{n-1} \equiv 1 \pmod n$, n ungerade und nicht unbedingt prim, $a \not\equiv 1 \pmod n$. Ferner sei $n - 1 = 2^k \cdot u,\ 2 \nmid u,\ k \geq 1$. Das *Profil* von a modulo n ist dann

$$\widetilde{a} = \left(\underbrace{\underbrace{a^{n-1}}_{\equiv 1}, a^{\frac{n-1}{2}}}_{\text{Q.-wurzel}}, ..., a^{\frac{n-1}{2^k}} \right) \pmod n$$

Reguläres Profil:

$$\widetilde{a} = (1, 1, ..., 1) \text{ oder } \widetilde{a} = (1, 1, ..., 1, -1, ...)$$

Irreguläres Profil:

$$\widetilde{a} = (1, 1, ..., 1, \underbrace{a}_{\neq \pm 1}, ...) \quad \Rightarrow \quad n \text{ keine Primzahl}$$

Grundlage für Miller-Rabin-Primzahltest (später):

- n prim $\Rightarrow$ a hat reguläres Profil $\forall a < n$.
- n nicht prim $\Rightarrow$ a hat irreguläres Profil für *viele* $a < n$.

Modulare Quadratzahlen und Quadratwurzeln

Beispiel.

$\mathbb{Z}_{15}^*$	1	2	4	7	8	11	13	14
zum Quadrat	1	4	16	49	64	121	169	196
modulo 15	1	4	1	4	4	1	4	1

d.h. nur die Zahlen 1 und 4 sind modulare Quadratzahlen (sprich: *quadratische Reste / quadratic residues*). Wenn a kein quadratischer Rest ist, so heißt a *quadratischer Nichtrest* modulo n.

Notation: QR_n, also $\mathrm{QR}_{15} = \{1, 4\}$.
QNR_n, also $\mathrm{QNR}_{15} = \{2, 7, 8, 11, 13, 14\}$

Jede Zahl in QR_{15} hat 4 Quadratwurzeln:

$$1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 \equiv 1 \pmod{15}$$
$$2^2 \equiv 7^2 \equiv 8^2 \equiv 13^2 \equiv 4 \pmod{15}$$

Beispiel. Falls n, $n \neq 2$ prim ist, so ist für $a \neq 0$ $(-a)^2 = a^2$. Daher ist die Hälfte der Zahlen in $\mathbb{Z}_n^*$ ein quadratischer Rest und jeder quadratische Rest besitzt genau 2 Quadratwurzeln, d.h.

$$|\mathrm{QR}_n| = |\mathrm{QNR}_n| = \frac{n-1}{2}$$

$\mathbb{Z}_{13}^*$	1	2	3	4	5	6	7	8	9	10	11	12
zum Quadrat	1	4	9	16	25	36	49	64	81	100	121	144
modulo 13	1	4	9	3	12	10	10	12	3	9	4	1

Wenn w primitives Element in $\mathbb{Z}_n^*$ ist, dann ist w^i genau dann quadratischer Rest, wenn i gerade ist.
Die Quadratwurzeln von w^i sind dann $w^{i/2}$ und $-w^{i/2}$.

Definition 5. *Für n prim und $a \in \mathbb{Z}_n^*$ ist das* Legendresymbol $\left(\frac{a}{n}\right)$ *definiert mit*

$$\left(\frac{a}{n}\right) = \begin{cases} 1 & \textit{falls } a \in \mathrm{QR}_n \\ -1 & \textit{falls } a \in \mathrm{QNR}_n \end{cases}$$

Satz 6 (Euler-Kriterium). *Für alle Primzahlen $n > 2$ und alle $a \in \mathbb{Z}_n^*$ ist*

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Beweis.

- Falls $a \in \mathrm{QR}_n$, also $a \equiv b^2 \pmod{n}$, dann ist

$$a^{(n-1)/2} \equiv (b^2)^{(n-1)/2} \equiv b^{n-1} \overset{\text{Fermat}}{\equiv} 1 \equiv \left(\frac{a}{n}\right) \pmod{n}$$

- Falls $a \in \mathrm{QNR}_n$, dann ist für alle $b \in \mathbb{Z}_n^*$:

$$\begin{aligned} & a \not\equiv b^2 \\ \Rightarrow\ & a^{(n-1)/2} \not\equiv (b^2)^{(n-1)/2} \equiv b^{n-1} \equiv 1 \pmod{n}. \end{aligned}$$

  Da $a^{n-1} \equiv 1$ folgt $a^{(n-1)/2} \equiv -1 \equiv \left(\frac{a}{n}\right) \pmod{n}$.

□

Folgerung 7. *Für n prim und $x \in \mathbb{Z}_n^*$ kann $\left(\frac{x}{n}\right)$ in $\mathcal{O}(m^3)$ berechnet werden (m: Länge der Binärzahlen).*

Berechung von Quadratwurzel
Sei n prim. Wie kann eine Quadratwurzel für einen quadratischen Rest a errechnet werden?

- 1. Fall: $n \equiv 3 \pmod{4}$, d.h. $n+1$ ist durch 4 teilbar. Laut Eulerkriterium ist $a^{\frac{n-1}{2}} \equiv 1$, also $a^{\frac{n+1}{2}} \equiv a \pmod{n}$. Dann ist

$$\Big(\underbrace{a^{\frac{n+1}{4}}}_{=:b}\Big)^2 \equiv a^{\frac{n+1}{2}} \equiv a \pmod{n}$$

  und b ist Quadratwurzel von a. D.h. $b \equiv a^{\frac{n+1}{4}} \pmod{n}$ kann in $\mathcal{O}(m^3)$ mittels modularer Exponentation berrechnet werden.

- 2. Fall: $n \equiv 1 \pmod{4}$, d.h. $\frac{n-1}{2}$ ist gerade, also

$$\frac{n-1}{2} = 2^k \cdot u,\ \ k \geq 1, 2 \nmid u.$$

  Wir ziehen sukzessive die Quadratwurzel , indem wir $a^{2^{k-i}\cdot u}$ für $i = 1, ..., k$ berechnen. Genauer gesagt: Wir ziehen solange die Wurzel aus der 1, bis wir evtl. -1 errechnen.

  Wenn man

$$\widetilde{a} = \Big(\underbrace{a^{n-1}}_{\equiv 1}, a^{\frac{n-1}{2}}, ..., a^{\frac{n-1}{2^k}}\Big) \pmod{n}$$

  betrachtet, so ist dies, da n prim, ein *reguläres Profil.*

  - $\widetilde{a} = (1, 1, ..., 1)$: Dann ist $a^u \equiv 1 \pmod{n}$ und somit $a^{u+1} \equiv a \pmod{n}$. Da $u+1$ gerade ist, ist $a^{\frac{u+1}{2}}$ Quadratwurzel.

– Wenn $\widetilde{a} = (1, 1, ..., 1, -1, ...)$.
Finde $b \in \text{QNR}_n$. Da die Hälfte der Zahlen in $\mathbb{Z}_n^*$ quadratische Nicht-Reste sind, findet man b nach durchnittlich 2 versuchen. (Somit ist dies ein probabilistischer LasVegas-Algorithmus). Dann ist $b^{\frac{n-1}{2}} \equiv b^{2^k \cdot u} \equiv -1$ (Euler-Kriterium).

Sei i minimal, sodass $a^{2^{k-i} \cdot u} \equiv -1 \pmod{n}$. Dann ist

$$a^{\overbrace{2^{k-i} \cdot u}^{=:e}} \cdot b^{\overbrace{2^k \cdot u}^{=:f}} \equiv (-1) \cdot (-1) \equiv 1$$

e und f sind gerade, d.h. wir können aus $a^e b^f \equiv 1$ wieder die Wurzel mit $a^{e/2} b^{f/2}, a^{e/4} b^{f/4}, ...$ ziehen bis

  * entweder $a^u b^g \equiv 1 \pmod{n}$, u ungerade, g gerade. Dann ist $a^{u+1} b^g \equiv a$ und $a^{(u+1)/2} b^{g/2}$ ist Quadratwurzel,
  * oder es gibt ein $i < j \leq k$ mit $\underbrace{a^{2^{k-j} \cdot u} b^h}_{=:z} \equiv -1 \pmod{n}$ (h gerade). Dann wird z mit $-1 \equiv b^{(n-1)/2}$ multipliziert, und wie oben beschrieben fortgefahren.

$e \leftarrow n - 1,\ f \leftarrow 0;$
repeat
  $e \leftarrow \frac{e}{2};$
  $f \leftarrow \frac{f}{2};$
  if $a^e b^f \equiv -1 \pmod{n}$ **then**
    $f \leftarrow f + \frac{n-1}{2};$
until e *ungerade*;
return $a^{\frac{e+1}{2}} \cdot b^{\frac{f}{2}} \pmod{n}$
