wiedemann@dhbw-mannheim.de (1)

Aufwärm-Übungen

(1) Berechnen Sie mit Hilfe des erweiterten EUKLIDischen Algorithmus das multiplikative Inverse

$19^{-1} \bmod 251$ | x mit $19 \cdot x \equiv 1 \bmod 251$

(2) Lösen Sie die Kongruenz

$7x + 3 \equiv 2 \bmod 11$

(3) Berechnen Sie

$7^{15} \bmod 11$.

Lösungen

(1) Wende den Eukl. Alg. an.

$X_1 \leftarrow 1$ $\qquad Y_1 \leftarrow 0$

$X_2 \leftarrow 0$ $\qquad Y_2 \leftarrow 1$

$X_3 \leftarrow 251$ $\qquad Y_3 \leftarrow 19$

$Y_3 \neq 0, \; Y_3 \neq 1$

$$Q = \left\lfloor \frac{251}{19} \right\rfloor = 13 \qquad \left\lfloor \frac{X_3}{Y_3} \right\rfloor$$

$$T_1 = X_1 - QY_1 = 1$$

$$T_2 = X_2 - QY_2 = -13$$

$$T_3 = X_3 - QY_3 = 251 - 19 \cdot 13 = 4$$

190
57
247

$x_1 \leftarrow 0 \qquad y_1 \leftarrow 1$

$x_2 \leftarrow 1 \qquad y_2 \leftarrow -13$

$x_3 \leftarrow 19 \qquad y_3 \leftarrow 4$

$$Q = \left\lfloor \frac{x_3}{y_3} \right\rfloor = \left\lfloor \frac{19}{4} \right\rfloor = 4$$

$T_1 = x_1 - Qy_1 = -4$

$T_2 = x_2 - Qy_2 = 1 - 4 \cdot (-13) = 53$

$T_3 = x_3 - Qy_3 = 19 - 16 = 3$

$x_1 \leftarrow 1 \qquad y_1 \leftarrow -4$

$x_2 \leftarrow -13 \qquad y_2 \leftarrow 53$

$x_3 \leftarrow 4 \qquad y_3 \leftarrow 3$

$$Q = \left\lfloor \frac{4}{3} \right\rfloor = 1$$

$T_1 = x_1 - Qy_1 = 1 - 1 \cdot (-4) = 5$

$T_2 = x_2 - Qy_2 = -13 - 53 = -66$

$T_3 = x_3 - Qy_3 = 4 - 3 = 1$

$x_1 \leftarrow -4 \qquad y_1 \leftarrow 5$

$x_2 \leftarrow 53 \qquad y_2 \leftarrow -66$

$x_3 \leftarrow 3 \qquad y_3 \leftarrow 1$

$\rightarrow$ Terminiert da $y_3 = 1$

$$y_2 = -66 = \underline{\underline{19^{-1} \bmod 251}}$$

-66 ist in der gleichen Restklasse wie

$$-66 + 251 = 185$$

$$19^{-1} \bmod 251 = \underline{185 \bmod 251}$$

Check: $19 \cdot 19^{-1} \equiv 1 \bmod 251$

$19 \cdot 19^{-1} = \underline{k \cdot 251 + 1}$ $\quad k \in \mathbb{Z}$

$185 \cdot 19 = 3515 = 3514 + 1$

$= \underline{14 \cdot 251 + 1}$

$7x + 3 \equiv 2 \bmod 11$

$7x \equiv (2-3) \bmod 11 \equiv -1 \bmod 11 \equiv 10 \bmod 11$

$\Rightarrow \quad x = (7^{-1} \cdot 10) \bmod 11$ ist gerechtfertigt,
da $ggT(7, 11) = 1$

$7^{-1} \bmod 11$ ist die Zahl in $\mathbb{Z}_{11} \setminus \{0\}$ mit

$7 \cdot 7^{-1} \equiv 1 \bmod 11$

Raten: $7^{-1} = 8$, da $7 \cdot 8 = 56 = 55 + 1$
$= 5 \cdot 11 + 1$

$\Rightarrow \quad x = (7^{-1} \cdot 10) \bmod 11$

$= (8 \cdot 10) \bmod 11$

$= 80 \bmod 11 \equiv \underline{\underline{3 \bmod 11}}$

Für $7^{15} \bmod 11$ ~~betra~~ wie gehabt mit
fastexp : $= 10 \bmod 11$.

Berechnen Sie:

$2^{10} \bmod 11 = 1$ $\qquad 6^{12} \bmod 13 = 1$

$5^{6} \bmod 7 = 1$

dem:

$$2^{10} \bmod 11 = (2^3)(2^3)(2^3)(2) \bmod 11$$

$$= (8 \cdot 8 \cdot 8 \cdot 2) \bmod 11$$

$$\equiv (9 \cdot 5) \bmod 11 = 1 \bmod 11$$

$$5^6 \bmod 7 = (5^2)(5^2)(5^2) \bmod 7$$

$$\cancel{= (4 \cdot 3 \cdot 3) \bmod 7}$$

$$= (4 \cdot 4 \cdot 4) \bmod 7$$

$$= (2 \cdot 4) \bmod 7 \equiv 1 \bmod 7$$

$$6^{12} \bmod 13 = (6^2)^6 \bmod 13$$

$$= \left[(6^2 \bmod 13)^6\right] \bmod 13$$

$$= (10^6) \bmod 13$$

100

65

78

91

$$= \left((10^2 \bmod 13)^3\right) \bmod 13$$

$$= 9^3 \bmod 13$$

$$= 9 \cdot 81 \bmod 13$$

$$= 9 \cdot 3 \bmod 13$$

$$= 27 \bmod 13 \equiv 1 \bmod 13.$$

Es gilt (Kleine Satz von FERMAT)

Falls p eine Primzahl ist und a eine positive ganze Zahl, die nicht durch p geteilt wird, dann gilt

$$\boxed{a^{p-1} \bmod p \equiv 1 \bmod p}$$

(oder $a^{p} \bmod p \equiv a \bmod p$)

Hilft z. B. bei

$$
\begin{aligned}
7^{15} \bmod 11 &= 7^{10} \cdot 7^{5} \bmod 11 \\
&= [(7^{10} \bmod 11)(7^{5} \bmod 11)] \bmod 11 \\
&= 7^{5} \bmod 11 \\
&= (7^{2} \cdot 7^{2} \cdot 7) \bmod 11 \\
&\equiv (5 \cdot 5 \cdot 7) \bmod 11 \\
&\equiv (3 \cdot 7) \bmod 11 \\
&= 21 \bmod 11 \equiv \underline{10 \bmod 11}
\end{aligned}
$$

Der Kleine Satz von FERMAT ist die Grundlage aller <u>Primzahltests</u>, diese prüfen (ohne zu faktorisieren), ob eine Zahl eine Primzahl ist oder nicht.

p soll getestet werden

Falls für irgendwelche zufällig gewählten Zahlen a der Ausdruck $a^{p-1} - a$ kein Vielfaches von p ist, dann ist p <u>keine</u> Primzahl.

Zeige: Eine ganze Zahl z ist durch 3 teilbar, wenn ihre Quersumme ein Vielfaches von 3 ist.

$$z = 12345 = 1\cdot 10^4 + 2\cdot 10^3 + 3\cdot 10^2 + 4\cdot 10^1 + 5\cdot 10^0$$

$$z = \sum_{i=1}^{4} a_i 10^i \qquad a_i \in \{0,\dots,9\}$$

$$z \bmod 3 \equiv \left(\sum_{i=1}^{4} a_i 10^i\right) \bmod 3$$

$10 \bmod 3 = 1$

$100 \bmod 3 = 1$

$1000 \;\; - \;\; = 1$

$$= \left(\sum_{i=1}^{4} a_i\right) \bmod 3$$

$$= 0 \bmod 3$$

Beispiel:

Ein bayrischer Bauer will seine Kuhherde auf einem Volksfestzug präsentieren.

Wenn er die Kühe in 3er Reihen aufstellt bleiben 2 Kühe übrig. $x = 2 \bmod 3$

$x = 1 \bmod 4$

Stellt er sie in 4er-Reihen auf, bleibt eine Kuh übrig.

$x = 0 \bmod 7$.

Stellt er sie in 7er Reihen auf, bleibt keine Kuh mehr übrig.

Wie groß ist die Kuhherde?

Satz (Chinesischer Rest-Satz)

Gegeben sind die simultanen Kongruenzen

$$x \equiv a \bmod m$$

$$x \equiv b \bmod n$$

und $ggT(m,n) = 1$.

(mit $1 = \underline{\breve{u}}\, m + \underline{v}\, n$) (Lemma von Bézout)

dann ist

$$\boxed{x = (v \cdot n \cdot a + \breve{u} \cdot m \cdot b) \bmod (m \cdot n)}$$

<u>Beweis:</u>

Ausgangspunkt $x \equiv a \bmod m$

$x \equiv b \bmod n$.

aus $x \equiv a \bmod m \Rightarrow x = t \cdot m + a$, $t \in \mathbb{Z}$.

einsetzen: in 2. Gl.

$$a + m \cdot t \equiv b \bmod n$$

oder $\underline{m \cdot t \equiv (b - a) \bmod n}$

Nach Voraus. $ggT(m, n) = 1$

und gemäß Lemma von Bézout existieren Zahlen $u, v \in \mathbb{Z}$ mit $1 = \breve{u} \cdot m + v \cdot n$ (u, v werden über Euklid berechnet, wenn Euklid. terminiert $\underline{Y_1, Y_2}$)

Weil $ggT(m, n) = 1$

$$t \equiv m^{-1} (b - a) \bmod n$$

wegen $1 = u \cdot m + v \cdot n$

$$u \cdot m \equiv 1 \bmod n$$

$$\Rightarrow u = m^{-1}$$

$$\Rightarrow t = u \cdot (b - a) \bmod n$$

$\Longleftrightarrow \quad t = u(b-a) + l \cdot n \qquad l \in \mathbb{Z}.$

in $\quad x = t \cdot m + a$

setze dieses t ein:

$$x = [u(b-a) + l \cdot n] \cdot m + a$$

$$= u \cdot b \cdot m - u a \cdot m + l \cdot n \cdot m + a$$

$$= u \cdot b \cdot m + a \underbrace{(1 - u \cdot m)}_{= v \cdot n} + l \cdot m \cdot n$$

$$= u \cdot b \cdot m + a \cdot v \cdot n + \underline{l \cdot m \cdot n}$$

$$= [u \cdot b \cdot m + a \cdot v \cdot n] \bmod (m \cdot n)$$

<u>Lösen damit das Kuh-Problem</u>

$$x \equiv 2 \bmod 3$$
$$x = 1 \bmod 4$$
$$x = 0 \bmod 7$$

$$x \equiv 2 \bmod 3$$
$$x = 1 \bmod 4$$

$$\begin{cases} x = a \bmod m \\ y = b \bmod n \end{cases}$$

$$a = 2 \quad m = 3$$
$$b = 1 \quad n = 4$$

$z = \sum_i a_i 10^i$

$z \bmod 3 = \left(\sum_i a_i 10^i\right) \bmod 3$ $\qquad 10 \bmod 3 = 1$

$100 \quad - \quad 1$

$= \sum (a_i 10^i) \bmod 3$ $\qquad 10^i = 1 \bmod 3$

$\equiv \sum a_i \bmod 3$

$= \left(\sum a_i\right) \bmod 3 = 0 \Rightarrow \sum_i a_i = k \cdot 3$

$$ggT(m,n) = ggT(3,4) = 1 = 1 \cdot 4 - 1 \cdot 3$$

$$= u \cdot m + v \cdot n$$

$$\Rightarrow u = -1, \quad v = +1$$

$$x = [u b m + a v n] \bmod (m \cdot n)$$

$$= [-1 \cdot 1 \cdot 3 + 2 \cdot 1 \cdot 4] \bmod (3 \cdot 4)$$

$$= (-3 + 8) \bmod 12 \equiv \underline{\underline{5}} \bmod 12$$

Check: Es gilt in der Tat.

$$\boxed{5} \equiv 2 \bmod 3$$
$$\boxed{5} \equiv 1 \bmod 4$$

Weiter:

$$x \equiv 5 \bmod 12 \qquad a = 5 \quad m = 12$$
$$x \equiv 0 \bmod 7 \qquad b = 0 \quad n = 7$$

$$ggT(m,n) = ggT(12,7) = 1 = 3 \cdot 12 - 7 \cdot 5$$

$$u = 3, \quad v = -5$$

$$x = (v \cdot n \cdot a + u \cdot m \cdot b) \bmod (m \cdot n)$$

$$= -175 \bmod 84 \equiv \underline{\underline{77 \bmod 84}}$$

$$77 \equiv 2 \bmod 3$$
$$77 \equiv 1 \bmod 4$$
$$\underline{77 \equiv 0 \bmod 7}$$

d.h. der Bauer hat 77 Kühe oder davon ein Vielfaches von 84

Mit diesen Werkzeugen kann man den RSA-Algorithmus durchrechnen. Dieser lautet:

① Man wähle zwei zufällige Primzahlen p, q, (512, 1024, 2048, 4096 Bit) und berechne

$$n = p \cdot q.$$

② Berechne $$\phi(n) = (p-1)\cdot(q-1)$$

③ Wähle ein e mit $1 < e < \phi(n)$, $ggT(e, \phi(n)) = 1$

④ Berechne d mit

$$e \cdot d \equiv 1 \mod \phi(n).$$

⑤ $$K_{pub} = (e, n), \quad K_{priv} = (d, n)$$

Verschlüsselung: M geeignet als Zahl codiert $M < n$

$$C = M^e \mod n$$

Entschlüsselung:

$$M = C^d \mod n.$$

Beispiel: $p = 7$, $q = 17$ $\qquad \mathbb{Z}_{119}$

$$n = 7 \cdot 17 = 119$$

Dann ist $\phi(n) = \phi(119) = 6 \cdot 16 = \underline{\underline{96}}$

Wähle ein e mit $1 < e < 96$ $\quad ggT(96, e) = 1$

$e = 5$. $\qquad \boxed{K_{pub} = (5, 119)}$

Dann ist

$$d: \quad \frac{5 \cdot d \equiv 1 \bmod 96}{d = 5^{-1} \bmod 96}$$

Erweiteter Euklid mit $a = 5$, $b = 96$

$x_1 \leftarrow 1$ $\quad y_1 \leftarrow 0$

$x_2 \leftarrow 0$ $\quad y_2 \leftarrow 1$

$x_3 \leftarrow 96$ $\quad y_3 \leftarrow 5$

$$Q = \left\lfloor \frac{x_3}{y_3} \right\rfloor = \left\lfloor \frac{96}{5} \right\rfloor = 19$$

$T_1 = x_1 - Q y_1 = 1$

$T_2 = x_2 - Q y_2 = -19$

$T_3 = x_3 - Q y_3 = 96 - 95 = 1$

$x_1 \leftarrow 0$ $\quad y_1 \leftarrow 1$

$x_2 \leftarrow 1$ $\quad y_2 \leftarrow -19$

$x_3 \leftarrow 5$ $\quad y_3 \leftarrow 1$

STOP : Return $d = -19 \equiv 5^{-1} \bmod 96$

Also: $d \equiv 77$

Check: $5 \cdot 77 = 385 = 384 + 1$

$= 4 \cdot 96 + 1$ ✓

$$\boxed{K_{priv} = (77, 119)}$$

Klartext : BA → wird als Zahl dargestellt, z.B. über ASCII - Werte

$A = 65$, $B = 66$

Beachte: Wegen der kleinen Primzahlen $p = 7$, $q = 17$ ist $n = 119$

~~denn~~ da $M < n$ sein muss, kann damit nur ein Zeichen verschlüsselt werden.

Ist $n > 6665$, kann BA als Block verschlüsselt werden.

$M = B \mathrel{\hat{=}} 66$

Dann ist $C = M^e \bmod n$

$$= 66^5 \bmod 119$$

$$= 66^2 \cdot 66^2 \cdot 66 \bmod 119$$

$$= \left[(66^2 \bmod 119)(66^2 \bmod 119)(66)\right] \bmod 119$$

$$= (72 \cdot 72 \cdot 66) \bmod 119$$

$$= \underline{\underline{19}}$$

Die fachgerechte Entschlüsselung ist:

Klartext $= C^d \bmod n$ $\qquad K_{priv} = (77, 119)$

$$= 19^{77} \bmod 119$$

$$77 = 64 + 8 + 4 + 1$$

$$19^2 = 361 \bmod 119 = 4$$

$$19^4 = 16$$

$$19^8 = 256 \bmod 119 = 18$$

$$19^{16} = 18^2 \bmod 119 = 86$$

$$19^{32} = 86^2 \bmod 119 \equiv 18$$

$$19^{64} = 86.$$

$$\Rightarrow \quad 19^{77} \bmod 119$$

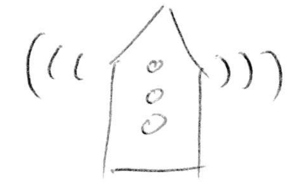
$$= 19^{64+8+4+1} \bmod 119$$

$$= \left[(19^{64} \bmod 119)(19^{8} \bmod 119)(19^{4} \bmod 119)\cdot 19\right] \bmod 119$$

$$\equiv (86 \cdot 18 \cdot 16 \cdot 19) \bmod 119$$

$$\equiv 66$$

Übung



Rechnen Sie den RSA-Alg. durch mit

$$p = 13, \quad q = 23, \quad e = 13$$

Verschlüsseln Sie den Klartext $M = 42$ und führen Sie eine fachgerechte Entschlüsselung durch.

$$n = 299$$

$$\phi(n) = 264$$

Euklid

$$e = 13, \quad d = 13^{-1} \bmod 264 = 61 \bmod 264$$

da $13 \cdot 61 = 793 = 792 + 1$

$= 3 \cdot 264 + 1$

Dann ist

$$42^{13} \bmod 299 = 237 = c$$

und

$$237^{61} \bmod 299 = 237^{32+16+8+4+1} \bmod 299$$

$$= 42$$