

Kryptographie II – Lösungsvorschläge zum Übungsblatt 2

Aufgabe 1: Kettenbruchentwicklung (ir)rationaler Zahlen

A. (i) Bemerkung: $\frac{2007}{1971} = \frac{223}{219}$

i	x	q_i	r_i
0	$\frac{2007}{1971}$	1	$\frac{36}{1971}$
1		54	$\frac{27}{36}$
2		1	$\frac{9}{27}$
3		3	$\frac{0}{9}$

$\Rightarrow$

$$\langle 1, 54, 1, 3 \rangle = 1 + \frac{1}{54 + \frac{1}{1 + \frac{1}{3}}}$$

(ii) **Erste Lösung**

(Fein)

Wir wissen schon, dass die Kettenbruchentwicklung von $\sqrt{7} + 2$ periodisch sein muss.

Dies bedeutet, dass $(q_i, r_i) = (q_{i+k}, r_{i+k})$ für alle $i > i_0 \in \mathbb{N}$ und ein entsprechendes k .

$q_0 = 4$	$r_0 = (\sqrt{7} + 2) - 4 = \sqrt{7} - 2$
$q_1 = \left\lfloor \frac{1}{\sqrt{7}-2} \right\rfloor = \left\lfloor \frac{\sqrt{7}+2}{3} \right\rfloor = 1$	$r_1 = \frac{\sqrt{7}+2}{3} - 1 = \frac{\sqrt{7}-1}{3}$
$q_2 = \left\lfloor \frac{3}{\sqrt{7}-1} \right\rfloor = 1$	$r_2 = \frac{3}{\sqrt{7}-1} - 1 = \frac{4-\sqrt{7}}{\sqrt{7}-1} = \frac{\sqrt{7}-1}{2}$
$q_3 = \left\lfloor \frac{2}{\sqrt{7}-1} \right\rfloor = 1$	$r_3 = \frac{2}{\sqrt{7}-1} - 1 = \frac{3-\sqrt{7}}{\sqrt{7}-1} = \frac{\sqrt{7}-2}{3}$
$q_4 = \left\lfloor \frac{3}{\sqrt{7}-2} \right\rfloor = 4$	$r_4 = \frac{3}{\sqrt{7}-2} - 4 = \frac{11-4\sqrt{7}}{\sqrt{7}-2} = \sqrt{7} - 2$

Nun beobachten wir, dass, falls $(q_i, r_i) = (q_{i+k}, r_{i+k})$, auch $(q_{i+1}, r_{i+1}) = (q_{i+k+1}, r_{i+k+1})$, also wiederholt sich die Folge ab q_4 mit dem Wert von q_0 , d.h.

$$\sqrt{7} + 2 = \langle 4, 1, 1, 1 \rangle .$$

Zweite Lösung

(Langweilig)

Es gilt $\sqrt{7} + 2 = 4.64575131106459059050161575364$. Da $\sqrt{7} + 2$ irrational ist, wird sich keine endliche Kettenbruchentwicklung ergeben. Es ergibt sich die folgende Kettenbruchentwicklung:

i	q_i	r_i
0	4	0.645751311
1	1	0.548583770
2	1	0.822875657
3	1	0.215250435
4	4	0.645751355
5	1	0.548583665
6	1	0.822876006
7	1	0.215249919
8	4	0.645762492
9	1	0.548556958
10	1	0.822964754
11	1	0.215118868
12	4	0.648592703
$\vdots$	$\vdots$	$\vdots$

Wir vermuten also, dass

$$\sqrt{7} + 2 = \langle 4, 1, 1, 1, 4, 1, 1, 1, 4, \dots \rangle$$

Eine Möglichkeit, die letzte Relation zu beweisen, ist, die Gleichung

$$\alpha = 4 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\alpha}}}}$$

zu lösen. In der Tat läßt diese Gleichung sich in folgender Form bringen

$$\alpha = \frac{14\alpha + 9}{3\alpha + 2}$$

und schliesslich zu

$$X^2 - 4X - 3$$

und $\sqrt{7} + 2$ ist doch Nullstelle dieses Polynoms.

Bemerkung: Daran, dass sich die Kettenbruchentwicklung periodisch wiederholt, sieht man, dass $\sqrt{7} + 2$ eine algebraische, irrationale Zahl ist, die Lösung einer quadratischen Gleichung ist.

- B.** (i) Für $x = \langle q_0, \dots, q_m \rangle$ definieren wir $n_0 = q_0$, $n_1 = q_0 q_1 + 1$, $d_0 = 1$, $d_1 = q_1$ und

$$n_i = q_i n_{i-1} + n_{i-2}, \quad d_i = q_i d_{i-1} + d_{i-2} .$$

Also is

$$\begin{aligned} n_2 &= q_2 n_1 + n_0 = 3 \cdot 3 + 1 = 10 , & d_2 &= q_2 d_1 + d_0 = 3 \cdot 2 + 1 = 7 , \\ n_3 &= q_3 n_2 + n_1 = 4 \cdot 10 + 3 = 43 , & d_3 &= q_3 d_2 + d_1 = 4 \cdot 7 + 2 = 30 , \\ n_4 &= q_4 n_3 + n_2 = 5 \cdot 43 + 10 = 225 , & d_4 &= q_4 d_3 + d_2 = 5 \cdot 30 + 7 = 157 \dots \end{aligned}$$

Die Tabelle mit allen Werten ist:

i	q_i	n_i	d_i
0	1	1	1
1	2	3	2
2	3	10	7
3	4	43	30
4	5	225	157
5	6	1 393	972
6	7	9 976	6 961
7	8	81 201	56 660
8	9	740 785	516 901
9	10	7 489 051	5 225 670

und schliesslich $\langle 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \rangle = \frac{7\,489\,051}{5\,225\,670}$.

(ii) Aus der periodischen Kettenbruchentwicklung

$$\alpha = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3 + \dots}}}}}$$

folgt, dass

$$\alpha = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{\alpha}}} = \frac{10\alpha + 3}{7\alpha + 2}.$$

Somit ist α eine Nullstelle des Polynom $7X^2 - 8X - 8$. Es gibt zwei Nullstellen, $\frac{4 \pm \sqrt{37}}{7}$, aber nur eine ist positiv, also

$$\alpha = \frac{4 + \sqrt{37}}{7} \approx 1,44039 \dots$$

Aufgabe 2: RSA mit kleinem privaten Exponent

Die Kettenbruchzerlegung von $\frac{e}{n}$ ist:

$$\langle 0, 2, 4, 7, 2, 1, 2, 3, 1, 4 \rangle$$

Die Tabelle zeigt die Approximierungsschritte:

i	Kettenbruch	a_i	k	dg
0	$\langle 0 + 1 \rangle$	$\frac{1}{1}$	1	1
1	$\langle 0, 2 \rangle$	$\frac{1}{2}$	1	2
2	$\langle 0, 2, 4 + 1 \rangle$	$\frac{5}{11}$	5	11

Für $i = 0$ und $i = 1$ gilt $\lfloor \frac{edg}{k} \rfloor = edg$ und somit $edg = edg + g$ woraus $g = 0$ folgen würde. Offensichtlich ist die Approximation in diesen beiden Fällen zu unscharf. Für $i = 2$ tritt kein Widerspruch auf und man kann nun

$$(p + q) = - \left\lfloor \frac{edg}{k} \right\rfloor + n + 1 = -11200 + 11413 + 1 = 214$$

berechnen. Die daraus resultierende quadratische Gleichung $x^2 + (p + q)x + n = 0$ hat die Lösungen:

$$x_{1,2} = \begin{cases} 113 \\ 101 \end{cases}$$

Tatsächlich gilt $11413 = 113 \cdot 101$.
