Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
30. Jan. 2019

Übungen zur Vorlesung Kryptographie

Blatt 14

Aufgabe 53

Die reguläre Kettenbruch-Entwicklung einer nicht-ganzen reellen Zahl $x \in \mathbb{R}$ ist wie folgt definiert. Sei

$$a_0 := \lfloor x \rfloor, \qquad \text{also} \quad x = a_0 + \xi_1 \text{ mit } 0 < \xi_1 < 1.$$

Nun setze man $x_1 := 1/\xi_1 > 1$ und

$$a_1 := \lfloor x_1 \rfloor \in \mathbb{N}_1, \qquad \text{also} \quad x_1 = a_1 + \xi_2 \text{ mit } 0 \leqslant \xi_2 < 1.$$

Falls $\xi_2 = 0$, ist $x = a_0 + \dfrac{1}{a_1}$ die Kettenbruch-Entwicklung von x.

Falls aber $\xi_2 > 0$, setzt man wieder $x_2 := 1/\xi_2$ und $a_2 := \lfloor x_2 \rfloor$, d.h. $x_2 = a_2 + \xi_3, \ldots$.

Solange der Rest $\xi_n > 0$, setzt man $x_n := 1/\xi_n$ und $a_n := \lfloor x_n \rfloor$, d.h. $x_n = a_n + \xi_{n+1}$ mit $0 \leqslant \xi_{n+1} < 1$. Falls $\xi_{n+1} = 0$, gilt

$$(*) \qquad x = \operatorname{cfrac}(a_0, a_1, \ldots, a_n) := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \quad a_{n-1} + \cfrac{1}{a_n}}}}$$

Im allgemeinen Fall (d.h. nicht notwendig $\xi_{n+1} = 0$) heißt die rationale Zahl

$$\operatorname{cfrac}(a_0, a_1, \ldots, a_n)$$

der n-te Näherungsbruch der Kettenbruch-Entwicklung von x.

a) Man berechne die Kettenbruch-Entwicklung von $\sqrt{2}$ und $\sqrt{5}$ sowie jeweils die ersten drei Näherungsbrüche.

b) Man beweise durch Induktion nach n: Ist u_n/v_n der n-te Näherungsbruch von $x \in \mathbb{R}$, $(\gcd(u_n, v_n) = 1)$, so gilt

$$\left| x - \frac{u_n}{v_n} \right| < \frac{1}{v_n^2}.$$

Bemerkung. Es gilt auch folgende teilweise Umkehrung von b): Seien u, v ganze Zahlen mit $\gcd(u, v) = 1$, $v > 0$ und

$$\left| x - \frac{u}{v} \right| < \frac{1}{2v^2},$$

so ist u/v ein Näherungsbruch der Kettenbruch-Entwicklung von x.

b.w.

Aufgabe 54

Gegeben sei ein RSA-Modul $N = pq$, wobei p, q ungerade Primzahlen mit $q < p < 2q$ sind. Weiter seien $1 < e, d < \varphi(N)$ ganze Zahlen mit $ed \equiv 1 \bmod \varphi(N)$, also $ed = 1 + k\varphi(N)$ mit einer ganzen Zahl k.

a) Man beweise die Abschätzung

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{3}{\sqrt{N}}.$$

b) Man zeige: Falls $d < \frac{2}{5} N^{1/4}$, so ist k/d ein Näherungsbruch der Kettenbruch-Entwicklung von e/N.
Man benutze dabei (ohne Beweis) die Bemerkung am Ende von Aufgabe 53.

Dies kann nach M.J. Wiener (1990) dazu dienen, den Entschlüsselungs-Exponenten d aus (N, e) zu berechnen.

c) Man führe den in b) angedeuteten sog. Wiener-Angriff in folgendem Beispiel durch: In hexadezimaler Schreibweise sei (N, e) gegeben als

```
 N = AA12 5101 C475 659A 4764 76F2 2B5D 89AC 8EF0 83AE 65EF F3EA 2BCE 4A99
1F17 2C1C 3651 66C1 9D4F C0DA DEEA C46A 2547 0C52 CE70 0F3D 1549 FDB9 9D7F
1D73 85AB E5A8 7AA4 B882 374F 4727 BFF1 EC2A 01BB CE85 3053 87F8 EDE2 7086
7B8D 85CA E6D0 7BB5 8218 E640 9B5F 552B 87EA A1F0 5BE1 F1CC AE71 9B68 0309
62B0 B2B9 08C0 E3EA E79D;

 e = 8BF0 0D77 7084 5320 6BC1 91CC 072A 7CA2 CD0D 46D8 1546 5BF3 DBAA F322
9201 040A 3FFA BA77 C535 95F6 CC12 79B1 4E98 5291 6512 FBB4 B33A EA2A 2548
9908 AF0F F50A D31A 2ACE 2D35 FF54 53C4 FE57 F7A8 0F10 B03E B2E3 6F0E 0217
C3F7 3BA8 C428 19B8 50D2 C980 13F6 5093 AB92 B47A F80C CC8E 6E9A BEBB 328D
4EB2 7A40 3845 3561 E439.
```

Es sei bekannt, dass $d < 2^{250}$. Man berechne d und finde die Faktorzerlegung von N.

Aufgabe 55

Sei $\omega \in \mathbb{C}^*$ eine primitive n-te Einheitswurzel, also $\omega = \exp(\frac{2\pi i \kappa}{n})$ mit $\kappa \in \mathbb{Z}$, $\gcd(\kappa, n) = 1$ (z.B. $\kappa = 1$). Man zeige: Die Matrix

$$A := \frac{1}{\sqrt{n}} \left(\omega^{\ell k}\right)_{\substack{1 \leqslant \ell \leqslant n \\ 1 \leqslant k \leqslant n}} \in M(n \times n, \mathbb{C})$$

ist unitär, d.h. $AA^* = E_n$, wobei $A^* := \overline{A}^\top$ (A konjugiert-komplex und transponiert) und E_n die n-reihige Einheitsmatrix bezeichnet.

Aufgabe 56

Man zeige, wie man die diskrete Fourier-Transformation der Ordnung $3m$ auf drei diskrete Fourier-Transformationen der Ordnung m zurückführen kann.