Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 14
30. Januar 2019

Übungen zur Kryptographie
Lösung

Aufgabe 53

a) Sei $a = \sqrt{2}$. Dann ist $a_0 = 1$ und $\xi_1 = a - a_0 = 0,41\ldots$. Wir setzen $x_1 = \xi_1^{-1} = 2,41\ldots$ und erhalten $a_1 := \lfloor x_1 \rfloor = 2$, $\xi_2 := 0,41\ldots$. Weiter ist $x_2 = \xi_2^{-1} = 2,41\ldots$ und erhalten $a_2 := \lfloor x_2 \rfloor = 2$, $\xi_3 := 0,41\ldots$. Ebenso $x_3 = \xi_3^{-1} = 2,41\ldots$ und erhalten $a_3 := \lfloor x_3 \rfloor = 2$. Wir erhalten

$$\mathrm{cfrac}(a_0, a_1, a_2, a_3) = \mathtt{a_0} + \frac{\mathtt{1}}{\mathtt{a_1} + \frac{\mathtt{1}}{\mathtt{a_2} + \frac{\mathtt{1}}{\mathtt{a_3}}}} = \mathtt{1} + \frac{\mathtt{1}}{\mathtt{2} + \frac{\mathtt{1}}{\mathtt{2} + \frac{\mathtt{1}}{\mathtt{2}}}}$$

Allgemein ist $\mathrm{cfrac}(a_0, \ldots, a_n) = (1, 2, \ldots, 2)$. Dazu beachte man, dass $\xi_2 = \frac{1}{\sqrt{2}-1} - 2 = \frac{(\sqrt{2}-1)^2}{\sqrt{2}-1} = \xi_1$ und entsprechend $\xi_n = \xi_{n-1}$ für alle $n \geq 2$. Die ersten Nährungsbrüche sind

$$\mathrm{cfrac}(a_0) = 1, \mathrm{cfrac}(a_0, a_1) = \frac{3}{2}, \mathrm{cfrac}(a_0, a_1, a_2) = \frac{7}{5}, \mathrm{cfrac}(a_0, a_1, a_2, a_3) = \frac{17}{12}.$$

Für $b = \sqrt{5}$ ergibt sich $b_0 = 2$ und $\xi_1 = \sqrt{5} - 2$, $\xi_2 = x_1 - 4 = \frac{1}{\sqrt{5}-2} - 4 = \frac{(\sqrt{5}-2)^2}{\sqrt{5}-2} = \xi_1$. Somit ist $\mathrm{cfrac}(b_0, b_1, b_2, b_3) = (4, 2, \ldots, 2)$ und die ersten Nährungsbrüche sind

$$\mathrm{cfrac}(a_0) = 2, \mathrm{cfrac}(a_0, a_1) = \frac{9}{4}, \mathrm{cfrac}(a_0, a_1, a_2) = \frac{38}{17}, \mathrm{cfrac}(a_0, a_1, a_2, a_3) = \frac{161}{72}.$$

$$\mathrm{cfrac}(a_0, a_1, a_2, a_3 = \mathtt{a_0} + \frac{\mathtt{1}}{\mathtt{a_1} + \frac{\mathtt{1}}{\mathtt{a_2} + \frac{\mathtt{1}}{\mathtt{a_3} + \ldots}}}$$

b) Wir zeigen zunächst, dass $u_n = a_n u_{n-1} + u_{n-2}$ und $v_n = a_n v_{n-1} + v_{n-2}$ mit $u_{-1} = v_{-2} = 1$ und $u_{-2} = v_{-1} = 0$. Weiter gilt $v_n u_{n-1} - u_n v_{n-1} = (-1)^n$.[1] Offensichtlich ist $\frac{u_0}{v_0} = a_0$ und $v_{-1}u_{-2} - u_{-1}v_{-2} = 0 - 1 = (-1)^{-1}$. Der Schritt $n \to n+1$ folgt aus

$$\begin{aligned} v_n u_{n-1} - u_n v_{n-1} &= (-1)^n = a_n(v_{n-1}u_{n-1} - u_{n-1}v_{n-1}) - v_{n-1}u_{n-2} - u_{n-1}v_{n-2} \\ &= (-1) \cdot (-1)^{n-1} = (-1)^n \end{aligned}$$

und

$$\begin{aligned} \mathrm{cfrac}(a_0, \ldots, a_{n+1}) = \mathrm{cfrac}(a_0, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}) &= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) u_{n-1} + v_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) v_{n-1} + v_{n-2}} \\ = \frac{a_n u_{n-1} + v_{n-2} + \frac{u_{n-1}}{a_{n+1}}}{a_n v_{n-1} + v_{n-2} + \frac{v_{n-1}}{a_{n+1}}} &= \frac{u_n + \frac{u_{n-1}}{a_{n+1}}}{v_n + \frac{v_{n-1}}{a_{n+1}}} = \frac{u_{n+1}}{v_{n+1}}. \end{aligned}$$

[1] Man beachte, dass u_n und v_n insbesondere teilerfremd sind, da $\gcd(u_n, v_n) \mid (-1)^n(v_n u_{n-1} - u_n v_{n-1}) = 1$.

Weiter ist

$$u_n v_{n-2} - u_{n-2} v_n = a_n(u_{n-1} v_{n-2} - u_{n-2} v_{n-1}) = a_n(-1)^n, \quad n \geq 0.$$

Jetzt folgt $\frac{u_{n+2}}{v_{n+2}} - \frac{u_n}{v_n} = \frac{(-1)^n a_n}{v_n v_{n+2}}$, d.h. die Teilfolge der gerade indizierten Kettenbrüche steigt und die der ungerade indizierten fällt. Aus $\frac{u_{n+1}}{v_{n+1}} - \frac{u_n}{v_n} = \frac{(-1)^{n-1}}{v_n v_{n+1}}$ folgt insbesondere, dass die gerade indizierten stets kleiner sind als die ungerade indizierten. Die beiden Teilfolgen nähren sich also von unten und oben dem Grenzwert an.[2] Zusammengefasst folgt

$$\left| x - \frac{u_n}{v_n} \right| \leq \left| \frac{u_{n+1}}{v_{n+1}} - \frac{u_n}{v_n} \right| < \frac{1}{v_n v_{n+1}} \leq \frac{1}{v_n^2}.$$

Aufgabe 54

a) Man beachte $k \geq 1$ da $e, d > 1$. Es folgt zunächst

$$\frac{1 + k\varphi(N)}{N} < \frac{1 + k(N-1)}{N} = k + \frac{1-k}{N} \leq k$$

und damit

$$\left| \frac{e}{N} - \frac{k}{d} \right| = \frac{1}{d} \left| \frac{1 + k\varphi(N)}{N} - k \right| = \frac{1}{d} \left(k - \frac{1 + k\varphi(N)}{N} \right)$$

Wir schätzen $\varphi(N)$ nach unten ab. Gegeben unserer Nebenbedingung $q < p < 2q$ liefert $p = 2q \Rightarrow 2q^2 = N \Rightarrow q = \sqrt{N/2}$ die untere Schranke[3]

$$\varphi(N) > (\sqrt{N/2} - 1)(\sqrt{2N} - 1) = N + 1 - 3\sqrt{N/2}.$$

Wir erhalten

$$\begin{aligned} \frac{1}{d} \left(k - \frac{1 + k\varphi(N)}{N} \right) &< \frac{1}{d} \left(k - \frac{1 + k(N + 1 - 3\sqrt{N/2})}{N} \right) = \frac{1}{d} \left(\frac{3k}{\sqrt{2N}} - \frac{(1+k)}{N} \right) \\ &< \frac{3}{\sqrt{N}}, \end{aligned}$$

da $d = \frac{1 + k\varphi(N)}{e} > \frac{k\varphi(N)}{e} > k$.

b) Es gilt

$$\frac{1}{2d^2} > \frac{1}{2(2\sqrt[4]{N}/5)^2} = \frac{25}{8\sqrt{N}} = \frac{3}{\sqrt{N}} \cdot \frac{25}{24} > \frac{3}{\sqrt{N}} > \left| \frac{e}{N} - \frac{k}{d} \right|$$

und somit ist k/d ein Kettenbruch.

c) Wir erhalten

```
function cfrac_appr(A,B,dbound: integer): array[2];
var
u0,u1,v0,v1,x0,x1,q,r: integer;
begin
```

[2] Man beachte, dass nach dem Bildungsgesetz der Abstand $\sim q_n^{-1} q_{n+1}^{-1}$ gegen 0 geht.

[3] $N - q - N/q + 1 \xrightarrow{\partial_q} -1 + N/q^2 < 0$ fällt monoton für $q < \sqrt{N}$. Wähle q minimal mit $qp = N, p < 2q$.

```
    (u0,v0) := (1,0);
    (u1,v1) := (0,1);
    (x1,x0) := (A,B);
    while x1 /= 0 do
        (q,r) := divide(x0,x1);
        (u1,u0) := (q*u1 + u0, u1);
        (v1,v0) := (q*v1 + v0, v1);
        (x1,x0) := (r,x1);
        if v1 > dbound then break; end;
        if floor((u1/v1-A/B)*(2*(dbound**2)) )  = 0 then
            return (u1,v1);
        end;
    end;
    return (0,0);
end;

==> cfrac_appr(e,N,2**250).
-:
(1_55391_67413_70527_82914_19343_90027_56573_28051_17261_92676_33134_46718,
1_88853_33701_63134_89175_04431_07318_92661_40042_86123_55649_53830_58897
```

Man verwende die Beziehung

$$ed = 1 + k(p-1)(q-1) = 1 + k(N+1-p-q) \Rightarrow p+q = (N+1) + \frac{1-ed}{k}.$$

```
p+q=
23146_91887_17176_89788_44681_24851_38268_13029_91622_78977_71436_44224_
96224_10789_87674_49624_04951_22775_10723_69851_20558_82125_81893_38784_
73371_07413_64116_92289_78455_45234_34978
```

Jetzt kann die quadratische Gleichung $X^2 - (p+q)X + pq = 0$ wie üblich gelöst werden. Wir erhalten die Diskriminante

```
7620_14710_19795_59319_63732_95745_39945_32295_61150_60813_63357_47580_
16273_37046_80909_65916_55831_52655_32417_53264_48589_87036_42182_45147_
73427_51086_09452_77156_45525_36201_28804
```

und damit

```
q=
7763_38588_48690_65234_40474_14552_99161_40367_15236_09082_04039_48322_
39975_36871_53382_41853_74559_85059_89153_08293_35984_47544_69855_46818_
49971_78163_77332_07566_66465_04516_53087

p=
15383_53298_68486_24554_04207_10298_39106_72662_76386_69895_67396_95902_
56248_73918_34292_07770_30391_37715_21570_61557_84574_34581_12037_91966_
23399_29249_86784_84723_11990_40717_81891.
```

Aufgabe 55

Es ist

$$(AA^*)_{jk} = \sum_{l=1}^{n} a_{jl}a^*_{lk} = \sum_{l=1}^{n} a_{jl}\overline{a}_{kl} = \frac{1}{n}\sum_{l=1}^{n} e^{\frac{2\pi ijl\kappa}{n}} e^{\frac{-2\pi ikl\kappa}{n}} = \frac{1}{n}\sum_{l=1}^{n} e^{\frac{2\pi i(j-k)l\kappa}{n}} = \delta_{jk}$$

Wir haben verwendet, dass für $j = k$ die Summe offensichtlich n ist; für $j \neq k$ durchläuft die Summe die $\gcd(j-k,n)$-ten Einheitswurzeln genau $\frac{n}{\gcd(j-k,n)}$-fach. Die Summe über alle d-ten Einheitswurzeln ist aber immer 0: $\sum_{j=0}^{d-1} e^{2\pi j/d} = \frac{1-e^{2\pi d/d}}{1-e^{2\pi/d}} = 0$ (geometrische Reihe).

Aufgabe 56

Sei A kommutativer Ring, $N > 1$ eine natürliche Zahl und $\omega \in A$ mit $\omega^N = 1, 1-\omega^k \in A^\times, \forall 0 < k < N$ sowie $N \cdot 1_A$ invertierbar. Sei $\Omega = (\omega^{kn})_{0\leq k,n<N}$ und $\Omega^{-1} = \frac{1}{N}\overline{\Omega} = (\frac{\omega^{-kn}}{N})_{0\leq k,n<N}$. Es ist $\mathcal{F} : A^N \to A^N, f \mapsto \Omega f$ die diskrete Fouriertransformation der Ordnung N. Sei nun $N = 3m$ und $\sigma = \omega^3$. Dann ist σ eine m-te Einheutswurzel bzgl. der Ordnung m. Weiter beachte man, dass m invertierbar ist, da $m \cdot (3N^{-1}) = 1_A$.
Sei $f \in A_N$ und $c := \mathcal{F}_N f$. Es ist $c(k) = \sum_{j=0}^{N-1} f(j)\omega^{jk}$. Wir zerlegen die Summe in drei Teile für die Restklassen mod 3:

$$\begin{aligned} c(k) &= \sum_{j=0}^{m-1} f(3j)\omega^{3jk} + \sum_{j=0}^{m-1} f(3j+1)\omega^{(3j+1)k} + \sum_{j=0}^{m-1} f(3j+2)\omega^{(3j+2)k} \\ &= \sum_{j=0}^{m-1} f(3j)\sigma^{jk} + \omega^k \sum_{j=0}^{m-1} f(3j+1)\sigma^{jk} + \omega^{2k} \sum_{j=0}^{m-1} f(3j+2)\sigma^{jk} \\ &= \mathcal{F}_m f_0 + \omega^k \mathcal{F}_m f_1 + \omega^{2k} \mathcal{F}_m f_2 \end{aligned}$$

wobei $f_l = (f(3j+l))_{0\leq j<m} \in A^m, l = 0, 1, 2$.