Mathematisches Institut
der Universität München
Pascal Reisert

Wintersemester 2015/2016
Übungsblatt 4
18. November 2015

Übungen zur Algorithmischen Zahlentheorie
Lösung

Aufgabe 13

a) Man beachte, dass für ganze Zahlen $l > m \geqslant 1$ mit $l = q \cdot m + r$ gilt

$$\begin{aligned}\gcd(2^l - 1, 2^m - 1) &= \gcd(2^l - 1 - (2^m - 1), 2^m - 1) = \gcd(2^m(2^{l-m} - 1), 2^m - 1) \\ &= \gcd(2^{l-m} - 1, 2^m - 1) = \ldots = \gcd(2^m - 1, 2^r - 1),\end{aligned}$$

wobei wir verwendet haben, dass die ungerade Zahl $2^m - 1$ und 2^m keinen Primfaktor teilen. Anschließend wurde iteriert. Parallel zum euklidischen Algorithmus angewendet auf l und m erhält man den euklidischen Algorithmus angewendet auf $2^l - 1, 2^m - 1$. D.h. $\gcd(2^l - 1, 2^m - 1) = 2^{\gcd(l,m)} - 1$. Man beachte insbesondere

$$2^l - 1 = (2^d - 1) \cdot \left(\sum_{k=0}^{l/d-1} (2^d)^k \right), \; 2^m - 1 = (2^d - 1) \cdot \left(\sum_{k=0}^{m/d-1} (2^d)^k \right).$$

b) Angenommen l ist reduzibel - $l = q \cdot m, \; m, q > 1$ - dann erhalten wir wie oben

$$2^l - 1 = (2^q - 1) \cdot \left(\sum_{k=0}^{m-1} (2^q)^k \right)$$

und $\sum_{k=0}^{m-1} (2^q)^k \geqslant 2^q > 2^q - 1 > 2$. Damit ist $2^l - 1$ keine Primzahl.

Bemerkung. Eine vergleichbare Lösung wurde von Ludwig Fürst in der Zentralübung vorgerechnet.

Aufgabe 14

a) Sei $(s_\nu)_{0 \leqslant \nu \leqslant 2^l - 2}$ eine maximale Periode von $(s_\nu)_{\nu \geqslant 0}$. Dann kommt jede Folge $(a_0, \ldots, a_{l-1}) \in \mathbb{F}_2^l$ genau einmal vor. Das heißt insbesondere kommt eine Abfolge $(a_0, \ldots, a_k)$ für $0 \leqslant k \leqslant l - 1$ genau so oft vor, wie es (eindeutige) Fortsetzungen zu einem l-Tupel gibt. Also

$$\#\{(a_0, \ldots, a_k) = (s_{0+t}, \ldots, s_{k+t} : \exists 0 \leqslant t \leqslant 2^l - 2 - k) = 2^{l-k-1}$$

solange $(a_0, \ldots, a_k) \neq (0, \ldots, 0)$. Für $(a_0, \ldots, a_k) = (0, \ldots, 0)$ muss die Fortsetzung zu $(0, \ldots, 0) \in \mathbb{F}_2^l$ ausgeschlossen werden. In diesem Fall gibt es folglich nur $2^{l-k-1} - 1$ Möglichkeiten. Wendet man diese allgemeine Überlegung auf $k = 0$ an erhält man die Anzahl der $s_\nu = 0$ in einer maximalen Periode zu $2^{l-1} - 1$.
Anders ausgedrückt, jedes $s_\nu, \; 0 \leqslant \nu \leqslant 2^l - 2$ ist der erste Eintrag eines eindeutigen Vektors in $\mathbb{F}_2^l \setminus 0$.

b) Wir betrachten die Folge der Paar $(v_{\nu,\kappa}) := (s_\nu, x_\kappa)$. Da nach Aufgabe 13, $S := 2^l - 1$ und $X := 2^m - 1$ teilerfremd sind, hat $v_{\nu,\kappa}$ die Periode $(2^l - 1)(2^m - 1)$. Bei der geschrumpften Folge,z_μ resp. $v_{\nu,\mu}$ wurden $2^{l-1} - 1$ Einträge in jeder der $2^m - 1$ Perioden von s_ν gestrichen. D.h. die resultierende Folge wiederholt sich nach $(2^l - 1 - (2^{l-1} - 1))(2^m - 1) = 2^{l-1}(2^m - 1)$ Einträgen. Wir müssen zeigen, dass dies tatsächlich die Periode ist.
Sei im folgenden κ_μ die Position der μ-ten 1 in $(s_\nu)_\nu$, sodass $x_{\kappa_\mu} = z_\mu$. Zur Vereinfachung der Notation benennen wir mit $E_S = 2^{l-1}$ die Anzahl der Einsen in einer Periode von $(s_\nu)_\nu$, mit $N_S = 2^{l-1} - 1$ die Anzahl der Nullen. Wir zeigen die Aussage **nur** für den Fall $l \leqslant 2^m - 1 = X$. Nach Konstruktion gilt:

1. Für alle $\mu, \lambda \in \mathbb{Z}$ gilt $z_{\mu+\lambda E_S} = x_{\kappa_\mu + \lambda S}$.

Die Folge $x_{\kappa+\lambda S}$ hat ebenfalls Periode $X = 2^m - 1$, denn $x_{\kappa+\lambda S}$ durchläuft die komplette Periode für $0 \leqslant \lambda < |X|$, da $\gcd(X, S) = 1$. Somit erhalten wir

2. Sei κ, κ' fest. Gilt für alle $\lambda \in \mathbb{Z}$ gilt $x_{\kappa+\lambda S} = x_{\kappa'+\lambda S}$, so teilt $X|(\kappa - \kappa')$.

Sei jetzt Z die (minimale) Periode von (z_μ). Wir müssen zeigen, dass $E_S X = 2^{l-1}(2^m - 1)|Z$. Es gilt offensichtlich für alle μ, λ: $z_{\mu+\lambda E_S} = z_{\mu+Z+\lambda E_S}$ und dann nach *1.* $x_{\kappa_\mu+\lambda S} = x_{\kappa_{\mu+Z}+\lambda S}$ sowie nach *2.* $X|(\kappa_{\mu+Z} - \kappa_\mu)$. Subtrahiert man diese Relation für μ und $\mu + 1$ so gilt

$$\kappa_{\mu+Z+1} - \kappa_{\mu+Z} = \kappa_{\mu+1} - \kappa_\mu + q_\mu \cdot X, \quad \exists q \in \mathbb{Z}.$$

Angenommen $q_\mu \neq 0$, dann gibt es mindestens $|q_\mu| \cdot X$ aufeinander folgende Nullen in (s_ν) was nach Annahme nicht möglich ist. Es folgt $\kappa_{\mu+Z+1} - \kappa_{\mu+Z} = \kappa_{\mu+1} - \kappa_\mu$ und die folgen $1 = s_{\kappa_\mu}, \ldots$ und $1 = s_{\kappa_{\mu+Z}}, \ldots$ sind gleich, also $S|(\kappa_{\mu+Z} - \kappa_\mu)$. Zwischen $s_{\kappa_\mu+1}$ und $s_{\kappa_{\mu+Z}}$ liegen dann $q' \cdot E_S = Z$ Einsen. Wendet man nochmals *1.* an, so erhält man für alle λ und alle μ

$$x_{\kappa_\mu} = z_0 = z_{\mu+\lambda Z} = z_{\mu+\lambda q' E_S} = x_{\kappa_\mu + \lambda q' S}$$

Da κ_μ die komplette Periode von (x_κ) durchläuft folgt $X|q'S$ und wegen Teilerfremdheit $X|q'$, also $XE_S|q'E_S = Z$.

Nähere Informationen zum Shrinking generator finden sich im gleichnamigen Artikel von Coppersmith, Krawczyk, Mansour verfügbar z.B. unter

`www.seas.gwu.edu/~poorvi/Classes/CS284_2008/ShrinkingGenerator.pdf.`

c) Sei $p_0 = 1, p_1 = 1$ und $s_0 = 1, s_1 = 0$, dann ist $s_2 = 1, s_3 = 1, s_4 = 0, s_5 = 1, s_6 = 1, \ldots$ mit Periode $(1, 0, 1)$. Sei $q_0 = q_1 = 1, q_2 = 0$ und $t_0 = 1, t_1 = t_2 = 0$. Dann ist $t_3 = 1, t_4 = 0, t_5 = 1, t_6 = 1, t_7 = 1, t_8 = 0, t_9 = 0, t_{10} = 1$ mit Periode $(1, 0, 0, 1, 0, 1, 1)$. Wir erhalten die geschrumpfte Sequenz $(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, \ldots)$ mit Periode $(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$ der Länge $14 = 2 \cdot (2^3 - 1)$.

Aufgabe 16

a) Aus Teil c) der vorangegangenen Aufgabe wissen wir, dass es ein ν gibt, sodass $b^\nu a/p = 0.q_{\nu+1} \ldots q_{\nu+k} \ldots$.

Nach Voraussetzung wissen wir, dass $1/p > 1/b^k$. Somit gibt es in jedem Interval $[j/b^k, (j+1)/b^k[$, $0 \leqslant j \leqslant b^k - 1$ maximal ein r/p, $0 \leqslant r \leqslant p - 1$. Somit liefert $b^\nu a/p$ ein eindeutiges r und wir können rekursiv a berechnen zu $b^{-\nu} r \bmod p$.

b) Betrachte wieder $x = u/v$ mit $u = q_{\nu+1} \dots q_{\nu+m}$ und $v = b^m$. Wie zuvor wissen wir, dass es maximal ein r gibt mit $r/p = 0.q_{\nu+1} \dots q_{\nu+m}$. Ist dies der Fall so ist r/p ein Nährungsbruch für x, denn

$$\left| x - \frac{r}{p} \right| < \frac{1}{b^m} < \frac{1}{2p^2}.$$

Man berechne dann Nährungsbrüche s/t von x rekursiv mittels

$$s_n = b_n s_{n-1} + s_{n-2}, s_{-1} = 1, s_{-2} = 0$$
$$t_n = b_n t_{n-1} + t_{n-2}, t_{-1} = 0, t_{-2} = 1$$

wobei $x = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \frac{1}{b_3 + \dots}}}$. Die b_i können rekursiv berechnet werden durch $b_0 = \lfloor x \rfloor$ und $b_i = \lfloor c_i \rfloor, c_0 = x, c_i = 1/(c_{i-1} - b_{i-1})$. Man beachte, dass induktiv

$$\begin{aligned}(-1)^n = t_n s_{n-1} - s_n t_{n-1} &= (b_n t_{n-1} + t_{n-2}) s_{n-1} - (b_n s_{n-1} + s_{n-2}) t_{n-1} \\ &= -(t_{n-1} s_{n-2} - s_{n-1} t_{n-2})\end{aligned}$$

folgt und damit $\gcd(s_n, t_n) | (-1)^n \Rightarrow \gcd(s_n, t_n) = 1$. Da r und p teilerfremd sind, folgt bereits $p = t_k$ für ein k. Sobald p bekannt ist, kann wie in a) aufgelöst werden.

c)* Wir verfahren wie in Teilaufgabe b): Sei $(v_i)_{1 \leqslant i \leqslant 253}$ die Folge der Bytes. Man betrachte jeweils $c_i = (v_i, \dots, v_{i+14})$ für $1 \leqslant i \leqslant 239$. Dann bestimme man das bitweise `xor` z_i mit $k = (\texttt{53}, \texttt{68}, \texttt{61}, \texttt{72}, \texttt{6D}, \texttt{20}, \texttt{65}, \texttt{6C}, \texttt{2D}, \texttt{53}, \texttt{68}, \texttt{65}, \texttt{69}, \texttt{6B}, \texttt{68})$. $z_i/(16^{30})$ liefert dann eine rationale Zahl. Man entwickle z_i in einen Kettenbruch und überprüfe, ob eine Primzahl $10^{15} < p < 10^{16}$ existiert, sodass der Nenner $t_{i,k}$ eines k-ten Nährungsbruchs gleich p ist und $s_{i,k}/t_{i,k}$ den Wert z_i genügend gut approximiert.
Anschließend kann rekursiv durch Multiplikation mit $b = 2$ bzw. $b^{-1} = \frac{p+1}{2} \bmod p$ der Schlüssel bestimmt werden. Der entstehende Klartext muss wieder in ASCII umgewandelt werden und sollte nur Textzeichen enthalten. Man erhält so,

```
U.S. officials have told CNN that intelligence suggests that ISIS or its
affiliates planted a bomb on the Russian plane, which broke apart in
midair, killing all 224 people on board. The flight was heading from
Sharm el-Sheikh to St. Petersburg, Russia.
```