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

WS 2015/16
11. Nov. 2015

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 4

Aufgabe 13

Seien $\ell, m > 1$ natürliche Zahlen. Man zeige:

a) Genau dann sind die Zahlen $M_\ell := 2^\ell - 1$ und $M_m := 2^m - 1$ teilerfremd, wenn ℓ und m teilerfremd sind.

b) Die Zahl $M_\ell = 2^\ell - 1$ ist höchstens dann prim, wenn ℓ prim ist.

Aufgabe 14

a) Die LFSR-Folge $(s_\nu)_{\nu \geqslant 0}$ des Grades ℓ über dem Körper $\mathbb{F}_2$ habe die maximale Periodenlänge $2^\ell - 1$. Man zeige: Innerhalb einer Periode gibt es genau $2^{\ell-1} - 1$ Glieder $s_\nu = 0$.

b) Sei $(x_\nu)_{\nu \geqslant 0}$ eine zweite LFSR-Folge des Grades m über $\mathbb{F}_2$ mit maximaler Periodenlänge $2^m - 1$ und es gelte $\gcd(\ell, m) = 1$. Die Folge (s_ν) aus a) werde verwendet, um die Folge (x_ν) zu "schrumpfen": Es werden alle diejenigen Folgenglieder x_μ aus der Folge entfernt, für die $s_\mu = 0$. Man zeige: Die entstehende Folge ist periodisch mit Periodenlänge $2^{\ell-1}(2^m - 1)$.

c) Man illustriere die Konstruktion aus b) mit einem Mini-Beispiel $\ell = 2$ und $m = 3$.

Aufgabe 15

Sei $p \geqslant 3$ eine Primzahl und $b \geqslant 2$ eine zu p teilerfremde ganze Zahl. (Z.B. $p = 7$ und $b = 10$.) Man betrachte die b-adische Entwicklung von $1/p$

$$\frac{1}{p} = \sum_{\nu=1}^{\infty} \frac{q_\nu}{b^\nu}, \qquad q_\nu \in \{0, 1, \ldots, b-1\},$$

in Kurzschreibweise $1/p = 0.q_1q_2q_3q_4q_5\ldots$.

a) Man zeige: Die b-adische Entwicklung ist periodisch und die Periodenlänge r ist ein Teiler von $p - 1$. Genau dann ist die Periodenlänge maximal, d.h. $r = p - 1$, wenn b eine Primitivwurzel modulo p ist.

b) Man bestimme alle Primzahlen $p < 100$, $(p \neq 2, 5)$, für die $b = 10$ Primitivwurzel ist.

c) Sei b Primitivwurzel modulo p. Man beweise: Für jede ganze Zahl a mit $1 \leqslant a < p$ hat die b-adische Entwicklung von a/p ebenfalls die Periodenlänge $p - 1$ und die Periode ist gegenüber der Entwicklung von $1/p$ zyklisch vertauscht, d.h.

$$\frac{a}{p} = \sum_{\nu=1}^{\infty} \frac{q_{\nu+\ell}}{b^\nu} \quad \text{mit einer (von } a \text{ abhängigen) ganzen Zahl } \ell \geqslant 0.$$

Aufgabe 16 (Fortsetzung von Aufgabe 15)

Sei weiter vorausgesetzt, dass b Primitivwurzel modulo p ist.

Wegen der großen Periodenlänge (z.B. bei $p > 10^9$) könnte man daran denken, einen Abschnitt der b-adischen Entwicklung von a/p (mit geheim zu haltendem a) als Pseudo-One-Time-Pad zu verwenden. Ein solches OTP ist aber kryptographisch schwach, wie im Folgenden gezeigt werden soll.

a) Die Primzahl p sei bekannt und es sei k eine natürliche Zahl mit $b^k > p$. Dann kann man aus einem bekannten Abschnitt $q_{\nu+1}q_{\nu+2}\dots q_{\nu+k}$ der b-adischen Entwicklung von a/p alle vorhergehenden und folgenden Ziffern q_i mit $i \leqslant \nu$ bzw. $i > \nu + k$ berechnen (und damit ist auch a bekannt).

b) Man kann sogar bei unbekannten p und a diese Größen rekonstruieren, wenn ein genügend langer Abschnitt der b-adischen Entwicklung von $\dfrac{a}{p}$ bekannt ist, genauer sei $q_{\nu+1}q_{\nu+2}\dots q_{\nu+m}$ bekannt, wobei m so groß ist, dass $2p^2 < b^m$. Man benutze dabei (ohne Beweis) den folgenden Satz aus der Theorie der Kettenbrüche (siehe z.B. Forster: *Algorithmische Zahlentheorie*, 2. Aufl., Satz 27.6 [1. Aufl. Satz 25.6] oder Hardy/Wright: *Introduction to the theory of numbers*, Theorem 184):

Sei x eine reelle Zahl und seien u, v teilerfremde ganze Zahlen mit $v > 0$ und

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

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

c)* Man betrachte den folgenden Geheimtext der Länge von 253 Bytes (hexadezimale Schreibweise)

```
D3F4 2C13 F095 8681 12DF 7A29 AEA9 8799 D321 2653 84D0 1D6E 81A5 2FF8 1404
1EF9 4CDB A680 EA6C C65A 9A7D 7521 0E42 210B 72A4 8999 8B44 24E9 F6CD 6DDC
BEB1 133D 6D8F 8B87 8B73 FC49 6D10 A8DE B893 7CFC 421F 0F40 EBB1 95EC B911
FC6B 99D3 1EE4 B34D 2C17 B807 8C75 26D8 A75E DE2C 4EAD 4B71 CD05 1ED8 9879
D429 C438 5907 4B4E 2073 FDCC 04EA AFC9 B3B2 AC8E C589 7117 45E8 2766 0484
7B89 1713 F9FC 0D1A 70D9 FF85 2A82 E048 0902 3B8E 3C5B C091 43F3 2AC8 5CA6
8D5B 4F2F 8727 1755 7EB1 9FB3 4C4A 41C8 C928 60F5 65FC BBFD 3AF4 8E91 C232
B542 09AB FCAB 6DBC 53A6 649A 36AE 2A2F 2E50 0D25 8473 DE36 23D5 25FE 6CDE
3E55 4BF8 E3C1 8C39 6478 D44F FB
```

Er entstand aus einem englischen ASCII-Klartext durch bitweises `xor` mit einem Pseudo-One-Time-Pad aus den ersten $253 \cdot 8 = 2024$ Stellen der Binär-Entwicklung (d.h. Basis $b = 2$) von

$$a/p = 0.q_1q_2q_3q_4\dots q_{2024}\dots \qquad q_i \in \{0, 1\}.$$

Dabei ist p eine geheime Primzahl mit 16 Dezimalstellen und a eine ganze Zahl mit $1 \leqslant a < p$. Jeweils 8 Bits $q_{8k+1}q_{8k+2}\dots q_{8k+8}$ wurden zu einem Byte $x_k := \sum_{\nu=1}^{8} q_{8k+\nu}2^{\nu-1}$ zusammengefasst. Der Klartext enthielt den Teilstring `Sharm el-Sheikh`, hexadezimal `5368 6172 6D20 656C 2D53 6865 696B 68`.

Man berechne p und a, sowie den gesamten Klartext.