MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
May 12, 2005

Cryptography
Problem Sheet #4

Problem 13 As in problem 11, let

$$\mathcal{P} := \{\vec{p} = (p_i)_{i\in\mathbb{Z}_m} \in \mathbb{R}^m : \sum_{i\in\mathbb{Z}_m} p_i = 1 \text{ and } p_i \geq 0 \text{ for all } i \in \mathbb{Z}_m\}$$

be the set of all probability distributions on $\mathbb{Z}_m$. Suppose that $\vec{p} \in \mathcal{P}$ satisfies $p_i > 0$ for all $i \in \mathbb{Z}_m$. Show that

$$\vec{p}^{\,n} := \underbrace{\vec{p} * \ldots * \vec{p}}_{n \text{ factors}}$$

converges for $n \to \infty$ to the uniform distribution $\vec{u} \in \mathcal{P}$, where $u_i = 1/m$ for all i.

Hint. Define $M_n := \max_{i\in\mathbb{Z}_m}\{(\vec{p}^{\,n})_i\}$ and prove that $(M_n)_{n\in\mathbb{N}}$ is monotonically decreasing.

Problem 14

a) Let $p \in \mathbb{N}$ be a prime and $f(X) = X^2 - X - 1 \in \mathbb{F}_p[X]$. For which p is f irreducible?

b) Determine all primes $p < 100$ such that the Fibonacci sequence mod p

$$x_{i+2} = (x_{i+1} + x_i) \bmod p, \quad x_0 = 0, x_1 = 1,$$

has maximal period $p^2 - 1$.

Problem 15 a) Let

$$f(T) = T^n + a_{n-1}T^{n-1} + a_{n-2}T^{n-2} + \ldots + a_1T + 1 \in \mathbb{F}[T]$$

be a polynomial of degree n over a field $\mathbb{F}$. Show that $f(T)$ is irreducible if and only if the polynomial

$$\check{f}(T) = T^n + a_1T^{n-1} + a_2T^{n-1} + \ldots + a_{n-1}T + 1$$

is irreducible.

b) Determine all irreducible polynomials of degree $n = 2, 3, 4, 5$ over the field $\mathbb{F}_2$.

Problem 16

The following cipher text, which is a byte string of length 99 in hexadecimal notation

```
A10B 1479 666C 5F12 BA5E 4DD9 EB07 8093 CCFB 92FC 07C2 91E2 3E2C DE3B
C4CF E27C 36F7 B7FB FB39 9BA7 0B9A 1723 FA03 E65C B841 4687 54A9 F004
FF96 6655 5DD6 82C2 1D46 36E7 EF52 F02F C0A3 2A13 DB13 0D28 D706 06D1
A684 BE70 B3F5 18B0 7F44 254A ECF3 C3
```

was obtained from an English ASCII plaintext by bitwise `XOR`ing with a byte string

$$(z_0, z_1, \ldots, z_{98}) \in \mathbb{Z}_{256}^{99}$$

The bytes $z_i \in \{0, 1, \ldots, 255\}$ were constucted by a linear recursion relation

$$z_{k+2} = a \cdot z_{k+1} + b \cdot z_k$$

over the field $\mathbb{F}_{257}$. The elements $z \in \mathbb{F}_{257}$ are interpreted as bytes $\in \mathbb{Z}_{256}$ in the obvious way, with $\overline{256} \in \mathbb{F}_{257}$ corresponding to the zero byte.

The plaintext begins with '`The `', which has ASCII code `54686520`. Calculate $a, b, z_0, z_1 \in \mathbb{F}_{257}$ and decrypt the cipher text.

Due: Thursday, May 19, 2005, 14:10 h