

Kryptographie

Blatt 9, 10.06.05, Abgabe 17.06.05

Aufgabe 1. Sei $N = \prod_{i=1}^k p_i^{e_i}$ mit paarweise verschiedenen Primzahlen p_i .

Zeige: Der LCG

$$x_{i+1} := ax_i + c \pmod{N}$$

hat Periode N genau dann, wenn gilt:

- i) $a \equiv 1 \pmod{p_i}$ für alle i ;
- ii) $(c, N) = 1$;
- iii) wenn $4|N$, dann $a \equiv 1 \pmod{4}$.

Insbesondere ist die Periode unabhängig vom Startwert.

Aufgabe 2. Sei $l(x) \in \mathbf{Z}[x]$ ein Polynom und F ein Pseudozufallsgenerator vom Typ $x + 1$.

Zeige: $F_{l(x)}$ (wie in der Vorlesung definiert) ist ein Pseudozufallsgenerator vom Typ $l(x)$.

Aufgabe 3. Seien $a, b, c, N \in \mathbf{Z}$.

Zeige: Die Iteration

$$x_{i+1} := ax_i + bx_{i-1} + c$$

mit x_{-1}, x_0 unabhängig und gleichverteilt auf \mathbf{Z}_N ist nicht pseudozufällig.

Ist sie deshalb genauso schlecht wie der LCG ?