Hans U. Simon
Nikolas List

Abgabe bis 9.12.2004
in den Übungsgruppen

Übungen zur Vorlesung

Diskrete Mathematik

WS 04/05

Blatt 7

Aufgabe 7.1

Berechne (von Hand) die CRC-12 Prüfsumme der binären Nachricht

$$111100100110000101111000$$

Das CRC-12-Generatorpolynom ist $g(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$.

Aufgabe 7.2

Folgende Nachricht wurde mit dem öffentlichen Schlüssel $n = 3127$ und $e = 2011$ gemäß RSA verschlüsselt.

$$1073\,1010\,3050\,0765\,1442\,2959$$

Dabei wurde folgende Codierung von Buchstaben verwendet und jeweils vier aufeinander folgende Klartextziffern verschlüsselt.

	A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	!
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Bestimme den Klartext! (Kleiner Tipp: $53|n$)

Aufgabe 7.3

Sei $p \geq 3$ eine Primzahl. Beweise dass für jede Zahl a aus $\mathbb{Z}_p^*$ gilt

$$x^2 \equiv a \pmod{p} \text{ besitzt eine Lösung } x \;\Leftrightarrow\; a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Hinweis: Nutze aus dass es ein Element $\xi \in \mathbb{Z}_p^*$ gibt mit $\mathbb{Z}_p^* = \{\xi^0, \xi^1, \xi^2, \ldots, \xi^{p-2}\}$.

Aufgabe 7.4

(Siehe auch Aufgabe 3.10 im Buch zur Vorlesung.)
Auf einer Insel leben g grüne, r rote und b braune Chamäleons. Wenn sich zwei verschiedenfarbige Chamäleons begegnen, ändern sie beide ihre Farbe in die dritte Farbe. Ist es für folgende Anzahlen möglich, daß durch eine Folge von Begegnungen alle Chamäleons dieselbe Farbe erhalten? Begründe!!

a) $g = 17, r = 7, b = 12$

b) $g = 12, r = 8, b = 21$

Zusatzaufgabe zum Knobeln: Verallgemeinere das Szenario auf beliebige $g, b, r > 0$ und gib notwendige und hinreichende Bedingungen an, so dass alle Chamäleons dieselbe Farbe erhalten. Beweise!