Hans U. Simon
Malte Darnstädt
Thorsten Doliwa

Bochum, den 12.12.2011

Abgabe: 19.12.2011 (bis 15:15 Uhr)

Übungen zur Vorlesung

Diskrete Mathematik

WS 11/12

Übungsblatt 09

Aufgabe 9.1

a) Berechne den ggT von $f(x) = 2x^4 - 2x^3 + 2x^2 - 2x$ und $g(x) = x^3 + x^2 + x + 1$ mit dem erweiterten Euklidischen Algorithmus.

b) Stelle den ggT als Linearkombination von $f(x)$ und $g(x)$ dar.

c) Zeige, dass der ggT nicht eindeutig ist.

Aufgabe 9.2 Multipliziere die Polynome $4x^2+x-2$ und $3x+2$ mit Hilfe der schnellen diskreten Fouriertransformation.

Aufgabe 9.3 Beim UMTS-Funk wird u.a. der CRC-8 Prüfcode mit Generatorpolynom $g(x) = x^8 + x^7 + x^4 + x^3 + x + 1$ verwendet. Berechne (von Hand) die CRC-8 Prüfbits der binären Nachricht

11011100101001

Aufgabe 9.4 Folgende Nachricht wurde mit dem öffentlichen Schlüssel $n = 2773$ und $k = 1779$ gemäß RSA verschlüsselt.

1379 1663 0162 0682 0162 0776

Dabei wurde folgende Codierung von Buchstaben verwendet und jeweils 2 aufeinander folgende Buchstaben (also vier 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: $47|n$)