Hans U. Simon
Malte Darnstädt
Thorsten Doliwa

Bochum, den 6.12.2010

Abgabe: 13.12.2010 (bis 14:15 Uhr)

Übungen zur Vorlesung

Diskrete Mathematik

WS 10/11

Übungsblatt 08

Aufgabe 8.1

a) Berechne den ggT von $f(x) = 4x^4 - 4x^3 + 3x^2 - x$ und $g(x) = 2x^3 - 3x^2 + 2x - 1$ 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 8.2 Multipliziere die Polynome $2x^2 - x + 1$ und $2x + 2$ mit Hilfe der schnellen diskreten Fouriertransformation.

Aufgabe 8.3 Auf SD-Karten wird u.a. der CRC-7 Prüfcode mit Generatorpolynom $g(x) = x^7 + x^3 + 1$ verwendet. Berechne (von Hand) die CRC-7 Prüfbits der binären Nachricht

101101100110001

Aufgabe 8.4 Folgende Nachricht wurde mit dem öffentlichen Schlüssel $n = 3127$ und $k = 2011$ gemäß RSA verschlüsselt.

1073 0854 0079 1969 1843 1933 1085 0444

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: $53|n$)