Hans U. Simon
Björn Schuster
Malte Darnstädt

Bochum, den 6.12.2013
Abgabe: 17.12.2013 (bis 10:00 Uhr)

Übungen zur Vorlesung

Diskrete Mathematik

WS 13/14

Übungsblatt 08

Hinweis: Für jede der Hausaufgaben ist eine vollständige mathematische Argumentation verlangt.

Aufgabe 8.1 Multipliziere die Polynome x^2-3x+3 und $2x-1$ mit Hilfe der schnellen diskreten Fouriertransformation.

Aufgabe 8.2 Beim Auslesen des Bordcomputers von Fahrzeugen wird u.a. der CRC-8 Prüfcode mit Generatorpolynom $g(x) = x^8 + x^4 + x^3 + x^2 + 1$ verwendet. Berechne (von Hand) die CRC-8 Prüfbits der binären Nachricht

1101101101

Aufgabe 8.3 Folgende Nachricht wurde mit dem öffentlichen Schlüssel $n = 3763$ und $k = 2427$ gemäß RSA verschlüsselt.

1679 0584 2246 3594

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: $53|n$)

Aufgabe 8.4 Sei $p \geq 3$ prim und $a \in \mathbb{N}$.

a) Zeige, dass gilt:

$2p$ teilt $a^p - a$

b) Zeige, dass die letzte Ziffer in der Dezimaldarstellung von a^5 und a identisch ist.