Hans U. Simon
Björn Schuster
Malte Darnstädt

Bochum, den 8.12.2014
Abgabe: 15.12.2014 (bis 16 Uhr)

Übungen zur Vorlesung

# Diskrete Mathematik

WS 14/15

## Übungsblatt 09

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

**Aufgabe 9.1** Beim USB-Protokoll wird u.a. der CRC-5 Prüfcode mit Generatorpolynom $g(x) = x^5 + x^2 + 1$ verwendet. Berechne (von Hand) die CRC-5 Prüfbits der binären Nachricht

$$110001101011$$

**Aufgabe 9.2** Folgende Nachricht wurde mit dem öffentlichen Schlüssel $n = 6319$ und $k = 4107$ gemäß RSA verschlüsselt.

$$4732\,6018\,4361\,2216\,3079$$

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: $89|n$)

**Aufgabe 9.3** Zeige:

a) Sind $k, n$ natürliche Zahlen mit $n \equiv 0 \bmod k$, so ist das Polynom $x^k - 1$ ein Teiler des Polynoms $x^n - 1$.

b) Seien $a, n, m$ natürliche Zahlen und $d = \mathrm{ggT}(n, m)$. Dann gilt

$$\mathrm{ggT}(a^m - 1, a^n - 1) = a^d - 1\,.$$

Hinweis: es gibt ganze Zahlen $r, s$ (von denen eine positiv und eine negativ ist) mit $d = rm + sn$.

**Aufgabe 9.4** Um das Maximum und das Minimum einer Menge mit $n = 2^k$ Elementen zu bestimmen, kann man nach dem *Divide-and-Conquer* Verfahren rekursiv Minima und Maxima einer Aufteilung der Menge in zwei gleich große Teilmengen bestimmen und das Ergebnis daraus zusammensetzen.

Gib einen Algorithmus an, der diese Idee so umsetzt, dass die Anzahl an benötigten Vergleichen kleiner als $2n - 2$ ist. Gib in deiner Lösung auch an, wie du die Anzahl an Vergleichen bestimmt hast.