

Präsenzübung zur Vorlesung

**Diskrete Mathematik**

WS 04/05

Blatt 6

**Aufgabe 6.1**

Berechne mit Polynomdivision:

a)  $(x^3 - x^2 - 4x) : (x^2 - 3x)$

b)  $(2x^6 + x^5 - 6x^4 - 7x^3 + x + 1) : (x^2 - 3)$

**Aufgabe 6.2**

Berechne die CRC-8 Prüfsumme der binären Nachricht

10010110110

Das CRC-8-Generatorpolynom ist  $g(x) = x^8 + x^4 + x^3 + x^2 + x$

**Aufgabe 6.3**

Bob hat den folgenden öffentlichen RSA Schlüssel:  $N = 51, e = 3$ .

a) Verschlüssel die Nachricht

08 15 47 11

mit Bob's öffentlichem Schlüssel.

b) Wie lautet der geheime Schlüssel von Bob?

**Aufgabe 6.4**

Beweise:

a)  $p^2 - 1 \equiv 0 \pmod{24}$  für alle Primzahlen  $p \geq 5$ .

b)  $n = \sum \varphi(d)$ , wobei die Summe alle positiven Teiler von  $n$  durchläuft.