Dr. Gerhard Baur
Laura Gellert

Wintersemester 2015/2016
Blatt 7

Übungen zur Angewandten diskreten Mathematik

(https://www.uni-ulm.de/mawi/mawi-stukom/baur/ws1516/angewandte-diskrete-mathematik.html)

(Abgabe und Besprechung am Freitag, den 05.02.16 um 14:15 in H22)

24. Erläutere den Diffie-Hellman-Schlüsselaustausch anhand von $p = 11$, $g = 5$ und $a = 3, b = 10$.

(3 Punkte)

25. Betrachte das Polynom $p \in \mathbb{R}[x]$ mit $p(x) = x^3 - 3x^2 + 4$ und seine erste Ableitung $p'(x)$.

    (a) Berechne denn größten gemeinsamen Teiler $g(x)$ von $p(x)$ und $p'(x)$. Hierbei soll $g(x)$ normiert sein, das heißt, der Führungskoeffizient soll gleich 1 sein.

    (b) Finde Polynome $f(x)$ und $h(x)$ sodass $g(x) = f(x)p(x) + h(x)p'(x)$.

    (c) Verifiziere, dass $\frac{p(x)}{g(x)}$ nur einfache Nullstellen besitzt.

(6 Punkte)

26. Stelle die Verknüpfungstabellen (Addition und Multiplikation) für $\mathbb{F}_9$ auf.

    Hinweis: Zeige, dass $x^2 + x + 2$ irreduzibel über $\mathbb{Z}_3$ ist.

(6 Punkte)

27. Berechne, welche Elemente in $R = \mathbb{Z}_3[x]/(x^2 + x + 1)$ ein multiplikatives Inverses haben.

(4 Punkte)

28. Zeige, dass die folgenden Polynome irreduzibel über $\mathbb{Z}$ sind:

    (a) $f_1(x) = x^3 + 10x^2 + 9x - 15$

    (b) $f_2(x) = x^3 + 6x^2 - 17x + 8$

    (c) $f_3(x) = x^6 + 12$

(6 Punkte)

29. Sei $q = p^n$ für eine Primzahl p und eine natürliche Zahl n. Betrachte $f \in \mathbb{F}_q[x]$ mit $f(x) = x^q - x$.

    (a) Zeige, dass alle $\alpha \in \mathbb{F}_q \setminus \{0\}$ Nullstelle von f sind.

    (b) Zeige, dass $f(x) = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$.

(5 Punkte)