Mathematik II für Informatiker — Sommer 2016
Übungsblatt 10
Dozent: PD Dr. Markus Junker. Assistent: Dr. Juan Diego Caycedo.

1. **Chinesischer Restsatz**.

   (a) Finden Sie (falls möglich) eine ganze Zahl z so, dass die folgenden Kongruenzen erfüllt sind:

$$\begin{aligned} z &\equiv 0 \pmod 2 \\ z &\equiv 4 \pmod 9 \\ z &\equiv 9 \pmod{11} \end{aligned}$$

   (b) Finden Sie (falls möglich) eine ganze Zahl z so, dass die folgenden Kongruenzen erfüllt sind:

$$\begin{aligned} 3 \cdot z &\equiv 4 \pmod 5 \\ 5 \cdot z &\equiv 2 \pmod 6 \\ 2 \cdot z &\equiv 3 \pmod 7 \end{aligned}$$

   (c) Finden Sie (falls möglich) eine ganze Zahl z so, dass die folgenden Kongruenzen erfüllt sind:

$$\begin{aligned} z &\equiv 1 \pmod 2 \\ z &\equiv 2 \pmod 9 \\ z &\equiv 7 \pmod{15} \end{aligned}$$

2. **Der Euklidischer Algorithmus.**

   (a) Wenden Sie den euklidischen Algorithmus auf die Zahlen 26 und 42 an, und finden Sie damit eine Darstellung

$$k \cdot 26 + l \cdot 42 = \mathrm{ggT}(26, 42)$$

   mit ganzen Zahlen k und l.

   (b) Wenden Sie den euklidischen Algorithmus im Polynomring $\mathbb{R}[X]$ auf die Polynome

$$p := X^4 + X^2 + X + 1 \text{ und } q := X^4 + X^3 + X + 1$$

   an, und finden Sie damit eine Darstellung

$$k \cdot p + l \cdot q = \mathrm{ggT}(p, q)$$

   mit $k, l \in \mathbb{R}[X]$.

Bitte wenden!

3. **Satz von Euler.** Berechnen Sie, ohne den Computer/Taschenrechner zu verwenden:

$$123456702^{17722} \text{ modulo } 100.$$

4. **Zyklische Einheitengruppen, diskreter Logarithmus.** Bestimmen Sie für alle Elemente der multiplikative Gruppe $(\mathbb{Z}/13\mathbb{Z})^*$ die Ordnung. Sie werden feststellen, dass $(\mathbb{Z}/13\mathbb{Z})^*$ zyklisch ist.

   Wählen Sie sich einen der Erzeuger ξ und geben Sie explizit den Gruppenisomorphismus

$$\mathbb{Z}/12\mathbb{Z} \to (\mathbb{Z}/13\mathbb{Z})^*,$$

   welcher $\overline{1}$ auf ξ abbildet, als Werttabelle an und auch sein Inverses α_ξ. (Es gilt also $\bar{x} = \alpha_\xi(\xi^{\bar{x}})$, deshalb heißt α_ξ auch diskreter Logarithmus zur Basis ξ).

Abgabe bis Fr. 8.7.2016, 12:00 in die Kästen im EG des Instituts für Informatik, Geb. 51.