Einführung in das symbolische Rechnen
Übungsblatt 2

Abgabetermin Mittwoch, den 12.05.2019 bis 23:59 in OpenOlat.

1. Sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p = \{\overline{0}, ..., \overline{p-1}\}$ der Körper mit p Elementen.

   (a) Finden Sie, analog zum Sieb von Eratosthenes, alle irreduziblen Polynome in $\mathbb{F}_2[x]$ vom Grad ≤ 3.

   (b) Faktorisieren Sie $x^5+x^2+x+1 \in \mathbb{F}_2[x]$ in ein Produkt von irreduziblen Polynomen.

2. (a) Seien $a_1, a_2 \in \mathbb{Z}$ und $n, m \in \mathbb{Z}_{>0}$. Zeigen Sie: Die simultanen Kongruenzen

   $$\begin{aligned} x &\equiv a_1 \operatorname{mod} n_1 \\ x &\equiv a_2 \operatorname{mod} n_2 \end{aligned}$$

   sind genau dann lösbar, wenn

   $$a_1 - a_2 \equiv 0 \operatorname{mod} \operatorname{ggT}(n_1, n_2)$$

   Die Lösung ist eindeutig modulo dem $\operatorname{kgV}(n_1, n_2)$.

   (b) Bestimmen Sie die Menge $L \subset \mathbb{Z}$ aller Lösungen x der simultanen Kongruenzen

   $$\begin{aligned} x &\equiv 1 \operatorname{mod} 108 \\ x &\equiv 13 \operatorname{mod} 40 \end{aligned}$$

3. Der öffentliche RSA-Schlüssel von Alice ist

   $$\begin{aligned} n_A &= 1913724803594980440489878086768646676656901670 17... \\ &\quad ...15016380980864967040643145079939623918556381963 \\ e_A &= 2^{16} + 1 \end{aligned}$$

   Bob hat eine verschlüsselte Nachricht

   $$\begin{aligned} c = &\ 91643741584965620886854549236149874152432635 06... \\ &...154322973187971112340254063352076215726187151593 \end{aligned}$$

   an Alice geschickt. Was war der Inhalt der Nachricht?

   Hinweise:

   - Alice hat ungeschickterweise einen Primfaktor p von $n_A = p \cdot q$ gewählt, sodass $\varphi(p)$ nur Primpotenzfaktoren ≤ 200000 hat.
   - Um für $a, b, n \in \mathbb{N}$ effizient $a^b \operatorname{mod} n$ zu berechnen, gibt es in JULIA/NEMO das Kommando

     `powmod(a,b,n)`.

   Testen Sie, ob auch die JULIA/NEMO-Funktion `factor` zum Ziel führt.

4. (a) Sei $R = \mathbb{Z}[i] = \{a_1 + i \cdot a_2 \mid a_1, a_2 \in \mathbb{Z}\} \subset \mathbb{C}$ mit $i^2 = -1$. Zeigen Sie, dass R zusammen mit

$$\begin{array}{cccc} d: & R\backslash\{0\} & \to & \mathbb{N}_0 \\ & a + b \cdot i & \mapsto & a^2 + b^2 \end{array}$$

ein euklidischer Ring ist. Geben Sie ein Verfahren an, um die Division mit Rest durchzuführen.

(b) Bestimmen Sie den grössten gemeinsamen Teiler

$$\mathrm{ggT}(3 + 4i,\ \ 1 - 4i) \in \mathbb{Z}[i]\,.$$

Hinweis: Berechnen Sie zur Division mit Rest von $a + b \cdot i$ durch $c + d \cdot i$ zunächst

$$\frac{a + b \cdot i}{c + d \cdot i} \in \mathbb{Q}[i] = \{a_1 + i \cdot a_2 \mid a_1, a_2 \in \mathbb{Q}\}\,.$$

5. (4 Zusatzpunkte) Sei R ein kommutativer Ring mit 1. Ein Element $q \in R$, $q \neq 0$, $q \notin R^\times$ heißt irreduzibel, wenn gilt

$$q = a \cdot b \text{ mit } a, b \in R \Longrightarrow a \in R^\times \text{ oder } b \in R^\times.$$

Ein Integritätsring R heißt faktoriell, wenn jedes $a \in R$, $a \neq 0$, $a \notin R^\times$ ein bis auf Permutation und Einheiten eindeutiges Produkt von irreduziblen Elementen ist.

(a) Bestimmen Sie die Einheitengruppe $\mathbb{Z}[\sqrt{-3}]^\times$.

(b) Zeigen Sie, dass $\mathbb{Z}[\sqrt{-3}]$ nicht faktoriell ist.

(c) Beweisen Sie, dass Hauptidealringe faktoriell sind.

(d) Zeigen Sie, dass jeder Euklidische Ring ein Hauptidealring ist.

(e) Folgern Sie, dass $\mathbb{Z}[\sqrt{-3}]$ nicht Euklidisch ist.