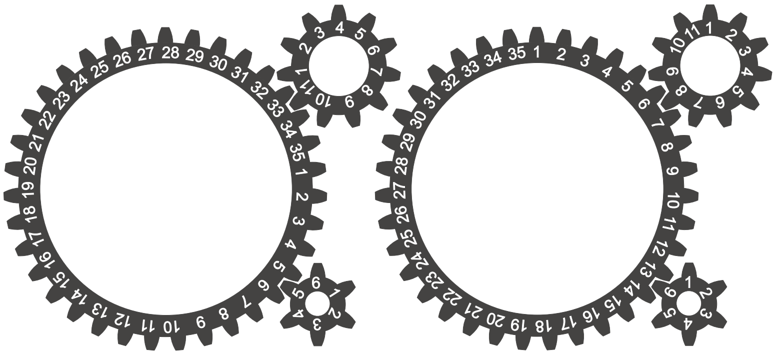
Einführung in das symbolische Rechnen
Übungsblatt 2

Abgabetermin Donnerstag, den 26.04.2018 vor der Vorlesung.

1. Lassen sich die beiden Konfigurationen von Zahnrädern durch Drehung ineinander überführen? Falls ja, um wieviele Schritte muss man dafür drehen?



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

$$x \equiv a_1 \operatorname{mod} n_1 \qquad x \equiv a_2 \operatorname{mod} n_2$$

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

$$x \equiv 1 \operatorname{mod} 108 \qquad x \equiv 13 \operatorname{mod} 40$$

3. Der öffentliche RSA-Schlüssel von Alice ist

$$n_A = 191372480359498044048987808676864667665690167017...$$
$$...150163809808649670406431450799396239185563819 63$$
$$e_A = 2^{16} + 1$$

Bob hat eine verschlüsselte Nachricht

$$c = 104312521081637151245645238123736275048732320 94...$$
$$...4648382247543264024938984089121141146755251112 65$$

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

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

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 P_N die Wahrscheinlichkeit, dass zufällig gewählte natürliche Zahlen $n, m \le N$ teilerfremd sind. Zeigen Sie, dass für den Grenzwert gilt

$$\lim_{N \to \infty} P_N = \frac{6}{\pi^2} \approx 60.7\%$$

Hinweis: Verwenden Sie ohne Beweis die Formel

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{6}\pi^2$$

die man z.B. mit Hilfe von Fourierreihen beweisen kann.