

**Aufgabe 16 (modulare Arithmetik, SAT) [4 Punkte]**

Geben Sie an, wie ein aussagenlogisches Erfüllbarkeitsproblem in konjunktiver Normalform über den Aussagevariablen  $X_1, \dots, X_n$  als eine Kongruenz der Form  $p(x_1, \dots, x_n) \equiv 0 \pmod{2}$  für ein multivariates Polynom  $p$  (mit Koeffizienten aus  $\{0, 1\}$ ) codiert werden kann.

Was folgt daraus für die Komplexität des Basisfalls ( $k = 1$ ) im multivariaten Hensel-Lifting?

Was lässt sich über die Komplexität der Lösung multivariater diaphantischer Gleichungen ableiten?

**Aufgabe 17 (Hensel-Lifting) [6 Punkte]**

Lösen Sie die Kongruenzen

$$x^3 + 8x^2 - 6x - 13 \equiv 0 \pmod{16} \quad \text{and} \\ x^2 - x + 8 \equiv 0 \pmod{32}$$

mittels Hensel-Lifting. Geben Sie sämtliche Lösungen an, falls mehrere existieren.

**Aufgabe 18 (Hensel-Lifting für  $\mathbb{Z}/2^k\mathbb{Z}$ ) [10 Punkte]**

Implementieren Sie ein Entscheidungsverfahren für univariate Polynomgleichungen über  $\mathbb{Z}/2^k\mathbb{Z}$  in einer Programmiersprache Ihrer Wahl. Verwenden Sie den auf Hensel-Lifting basierenden Algorithmus aus der Vorlesung.

Die Eingabe Ihres Programms soll eine Liste von  $n + 2$  Ganzzahlen,  $a_n \dots a_0$ , sein, die für die Kongruenz

$$\sum_{i=0}^n a_i \cdot x^i \equiv 0 \pmod{2^k}$$

stehen, die Ausgabe soll aus einer Liste der Lösungen (jeweils eine pro Zeile) bestehen oder UNSAT sein, falls keine Lösung existiert.

Evaluieren Sie Ihr Programm anhand der Kongruenzen aus Aufgabe 16 und weiterer eigener.

**Der Abgabetermin für Aufgabe 18 ist am 03.02.2020.**