

Aufgabenblatt 7 vom 1. 12.

Zur Besprechung in der Übung am 4. 12.

Besprechung der Autotool-Aufgaben (A3-1a), (A3-1b) sowie (A3-3a)–(A3-3c). (Bei Bedarf.)

Besprechung der Aufgaben (S5-1) und (S5-2).

Besprechung der Autotool-Aufgaben (A5-1), (A5-2) sowie (A5-3). (Bei Bedarf.)

Ü7-1 Wir betrachten den Ring der Gaußschen Zahlen $\mathbb{Z} + i\mathbb{Z} = \mathbb{Z}[i]$.

- Bestimme Quotient und Rest bei Division $(7 + 5i) : (2 + i)$.
- Wie sehen Ideale in $\mathbb{Z}[i]$ aus? (speziell $\langle 2 + i \rangle$, allgemein $\langle a + bi \rangle$)
- Beweise, daß $(\mathbb{Z}[i], | \cdot |)$ ein Euklidischer Ring ist. Dabei ist $|a + bi| = \sqrt{a^2 + b^2}$.
- Bestimme alle gcds von 6 und $3 + i$ in $\mathbb{Z}[i]$ und ihre Darstellung als Linearkombination von 6 und $3 + i$.

Ü7-2

Untersuche an Beispielen die Koeffizienten während der Rechnung des Euklidischen Algorithmus in $\mathbb{Q}[X]$ für Polynome mit zufällig gewählten Koeffizienten $\in \{-1, 0, 1\}$.

Ü7-3

- Bestimme die Länge der Diagonale des d -dimensionalen Einheitswürfels.
- Bestimme das Volumen der d -dimensionalen Einheitskugel (durch exakte Integration).
- Gib eine asymptotisch richtige Abschätzung für das Kugelvolumen an, die sich einfacher beweisen läßt (durch Betrachtung eines einbeschriebenen Würfels oder Polyeders).

Autotool-Aufgaben

A7-1 GCD von Polynomen

A7-2 GCD von Gaußschen Zahlen

A7-3 Kurzer Gittervektor

Zur schriftlichen Korrektur, Abgabe bis 15. 12., Besprechung am 18. 12.

S7-1 Falten Sie ein A4-Blatt ($x = \sqrt{2}$ LE – Länge der längeren Seite, 1 LE – Länge der kürzeren Seite) auf folgende Weise:

- Zuerst so, dass zwei gegenüberliegende Ecken des A4-Blatts aufeinander zu liegen kommen (es entsteht ein sehr breites Fünfeck mit zwei kurzen und drei langen Seiten).
- Nun dessen „Flügel“ so, dass die kurzen Seiten genau auf der Symmetrieachse dieser Figur zu liegen kommen.

Sie erhalten den Umriss eines „sehr regelmäßigen“ Fünfecks.

- a) Untersuchen Sie, ob es sich wirklich um ein regelmäßiges Fünfeck handelt. Bestimmen Sie exakte Werte für die Seitenlängen dieses Fünfecks in LE. Welche der Fünfecksseiten sind gleichlang?
- b) Bestimmen Sie das Verhältnis x der längeren zur kürzeren Seite des Ausgangsrechtecks, für welches das gefaltete Fünfeck regelmäßig ist. Geben Sie einen exakten Wurzelausdruck für x an.
- c) Bestimmen Sie exakte Formeln für die Seitenlängen des Fünfecks, wenn die längere Seite des Ausgangsrechtecks x LE und die kürzere 1 LE lang ist. Geben Sie auch hier exakte Wurzelausdrücke an.

S7-2 (nach: Joachim von zur Gathen und Jürgen Gerhardt: *Modern Computer Algebra*, Cambridge Univ. Press, 2013 <https://cosec.bit.uni-bonn.de/science/mca/>)

Dieser Algorithmus zur Bestimmung des gcd verwendet nur Subtraktionen und Halbieren (also Binärshifts):

```
gcd :: Integer -> Integer -> Integer
gcd a b =
  if a == b then a
  else case (even a, even b) of
    (True, True) -> 2 * gcd (div a 2) (div b 2)
    (True, False) -> gcd (div a 2) b
    (False, True) -> gcd a (div b 2)
    (False, False) ->
      if a > b
      then gcd (div (a - b) 2) b
      else gcd a (div (b - a) 2)
```

- a) Zeige Korrektheit und Termination.
- b) Gib eine gute obere Schranke für die Rekursionstiefe an (als Funktion der Bitlänge der Eingabe $\lceil \log_2(a) \rceil + \lceil \log_2(b) \rceil$).
- c) (autotool, Haskell-Lückentext) Ergänze den Algorithmus, so daß auch Zahlen p, q mit $ap + bq = \gcd(a, b)$ bestimmt werden.