Aufgabenblatt 4

40 Punkte

Aufgabe 1 (ganzzahlige Lösungen)

a) Bestimme alle ganzzahligen Lösungen der Gleichung

I) $39 \cdot x + 312 \cdot y + 182 \cdot z = 455$. 3

b) Bestimme alle $b \in \mathbb{Z}$, so dass die Gleichung

II) $121 \cdot x + 66 \cdot y + 264 \cdot z = b$

ganzzahlige Lösungen hat. Bestimme alle diese Lösungen (in Abhängigkeit von b). 3

c) Betrachte das Gleichungs*system* bestehend aus den Gleichungen I) & II) in 1 a) und 1 b). Bestimme das kleinste $b \in \mathbb{N}$, für das dieses Gleichungssystem eine ganzzahlige Lösung hat. (Gauß) 2

d) Bestimme für das in 1 c) gefundene kleinste $b \in \mathbb{N}$ alle Lösungen des Gleichungssystems I) & II). 2

Bemerkung: Siehe Unterabschnitt 2.1.2 im Skript. **10**

Aufgabe 2 (Kreise)

Wir betrachten Kreise mit Mittelpunkt $(0 \mid 0)$ und Radius $r \in \mathbb{R}$ in der xy–Ebene. Der kleinste solche Kreis mit Punkten mit *ganzzahligen Koordinaten* geht durch die vier Punkte $(\pm 1 \mid 0)$, $(0 \mid \pm 1)$ und hat Radius $r = 1$.

a) Gib einen möglichst kleinen solchen Kreis mit mindestens 5 ganzzahligen Punkten. Gib *alle* seine ganzzahligen Punkte und seinen Radius r_a . 1

b) Gib einen möglichst kleinen solchen Kreis mit mindestens 9 ganzzahligen Punkten. Gib *alle* seine ganzzahligen Punkte und seinen Radius r_b . 2

c) Benutze allenfalls die Tabelle auf S.40 um einen möglichst kleinen solchen Kreis zu finden mit mindestens 17 ganzzahligen Punkten. Gib *alle* seine ganzzahligen Punkte und seinen Radius r_c . 3

d) Gib mehrere solche Kreise mit mindestens 13 ganzzahligen Punkten und Radien r mit $r_b < r < r_c$, mit r_b aus 2 b) bzw. r_c aus 2 c). Gib *alle* ihre ganzzahligen Punkte. 4

10

Aufgabe 3 (stereographische Projektion)

Die Gerade $g: y = 1 - x/13$ schneidet den Einheitskreis $K: x^2 + y^2 = 1$ im Punkt $(x_1 \mid y_1) = (0 \mid 1)$.

a) Berechne den zweiten Schnittpunkt $(x_2 \mid y_2)$. $(T \mid 0) = (13 \mid 0)$ ist seine sog. *stereographische Projektion.* 1

b) Welchem pythagoräischen Zahlentripel entpricht also der Parameter $T = 13$. 1

c) Die Parameter $(\bar{u}, \bar{v}) = (1, 13)$ mit $T = \bar{v}/\bar{u} = 13/1$ kommen so nicht vor. Welche Parameter (u, v) mit $T' = v/u > 1$ entsprechen dem pythagoräischen Zahlentripel in 3 b) gemäss S.40 im Skript? 1

d) Die (unendliche) Tabelle auf S.40 ist vollständig. An wievielter stelle steht das Zahlentripel aus 3 b) ? 1

e) Beweise die Formeln für $X(T) = 2T/(T^2 + 1)$ und $Y(T) = (T^2 - 1)/(T^2 + 1)$ auf S.43. 2

6

Aufgabe 4 (Näherungen)

In Kapitel 2.2.2 findet sich eine vollständige Liste $(x_n \mid z_n) \in \mathbb{N}^2$ der ganzzahligen Lösungen von $z^2 - 2 \cdot x^2 = \pm 1$.
Und in Kapitel 2.3.1 wird erklärt, dass $(1 + \sqrt{2})^{n+1} = z_n + \sqrt{2} \cdot x_n$ für $n \in \mathbb{N}_0$.
Zum Beispiel ergibt sich für $n = 2$: $(1 + \sqrt{2})^3 = 7 + 5 \cdot \sqrt{2} = z_2 + x_2 \cdot \sqrt{2}$, also $(x_2 \mid z_2) = (5 \mid 7)$.
In der Tat: $z_2^2 - 2 \cdot x_2^2 = 7^2 - 2 \cdot 5^2 = -1$.
Daraus ergeben sich zwei Näherungen für rechtwinklig, gleichschenklige Dreiecke mit ganzzahligen Seiten:

I) $(a_n, b_n, c_n) = (a_n, a_n + 1, x_n)$ mit $a_n^2 + b_n^2 = c_n^2$ (rechtwinklig, nicht ganz gleichschenklig) , $a_n + b_n = z_n$,

II) $(\tilde{a}_n, \tilde{b}_n, \tilde{c}_n) = (x_n, x_n, z_n)$ mit $a_n^2 + b_n^2 = c_n^2 + 1$ (gleichschenklig, nicht ganz rechtwinklig) .

a) Berechne alle Winkel der zwei Dreiecke $(a_2, b_2, c_2) = (3, 4, 5)$ und $(\tilde{a}_2, \tilde{b}_2, \tilde{c}_2) = (5, 5, 7)$. 2

b) Berechne alle Seiten und Winkel der zwei Dreiecke (a_4, b_4, c_4) und $(\tilde{a}_4, \tilde{b}_4, \tilde{c}_4)$. 4

6

Aufgabe 5 (RSA)

Aus A werden nach R illegal verschlüsselte Dokumente versandt. Agent C vermutet, dass D dahintersteckt.

a) $N = 9991$ und $e = 11$ sind öffentlich. C schafft es, $N = p \cdot q$ zu faktorisieren. 1

b) Zum Verschlüssel $e = 11$ berechnet C nun den Entschlüssel $d = ?$ 2

c) Ein abgefangenes verschlüsseltes Dokument ist mit $4042 = m_1^e \bmod N$ und $6005 = m_2^e \bmod N$ signiert. C weiss, dass m_1 und m_2 zwei Buchstabenblöcke à je drei Buchstaben sind, codiert wie auf S.49 im Skript. Wie berechnet er nun m_1 und m_2 aus m_1^e und m_2^e ? Wer ist D ? 5

8