Technische Hochschule Deggendorf
Prof. Dr. P. Ullrich WS 2014/15

Übungen zur Vorlesung „Mathematik 1“

Angewandte Informatik/Infotronik

Blatt 4

Aufgabe 31. Welche Aussagen sind in $\mathbb{R}$ wahr, welche falsch?

a) $\forall x\ x \geq 0$ b) $\forall x_1\, \exists x_2\ x_1 \cdot x_2 = 1$ c) $\forall x_1\, \exists x_2\ (x_1 \neq 0) \to (x_1 \cdot x_2 = 1)$

d) $\exists x_1\, \forall x_2\ x_1 \geq x_2$ e) $\forall x_1\, \exists x_2\ x_1 \geq x_2$ f) $\forall x_1\, \exists x_2\, \exists x_3\ x_2^2 + X_3^2 = X_1^2$

g) $\forall x_1\, \exists x_2\, \forall x_3\ x_3^2 + x_1 > x_2$ h) $\forall x_1\, \exists x_2\ x_1 x_2^2 - x_2 = 0$ k) $\forall x\ (x^2 - 3x + 2 = 0) \to (x > 0)$

Aufgabe 32. Skizzieren Sie die Erfüllungsmengen folgender Formeln (über $\mathbb{R}$).

a) $\varphi(x_1, x_2) := (x_1 \geq 0) \wedge (x_2 \geq 0)$ b) $\varphi(x_1, x_2) := (x_1^2 + x_2^2 - 1 = 0) \wedge (x_2 \geq 0)$

c) $\varphi(x_1, x_2) := (x_1^2 - 1 = 0)$ d) $\varphi(x_1, x_2) := (x_2 \geq x_1^2 - 1) \wedge (x_2 \leq -x_1^2 + 1)$

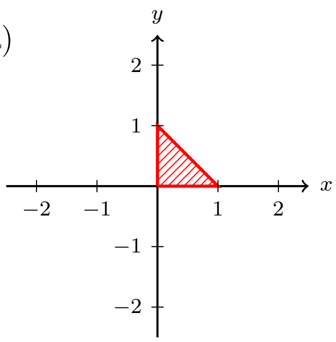
e) $\varphi(x_1) := (\exists x_2\ \frac{x_2^2}{4} - \frac{x_1^2}{9} = 1)$ f) $\varphi(x_1) := (\exists x_2\ x_2^2 - 4x_1 \geq 0)$

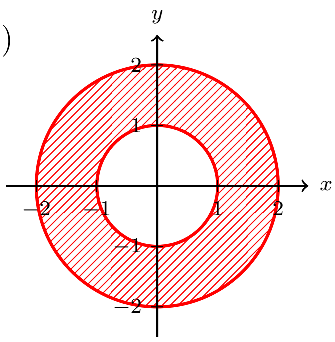
g) $\varphi(x_1, x_2) := (x_2 \leq -x_1 + 1) \wedge (x_2 \leq x_1 + 1) \wedge (x_2 \geq -x_1 - 1) \wedge (x_2 \geq x_1 - 1)$

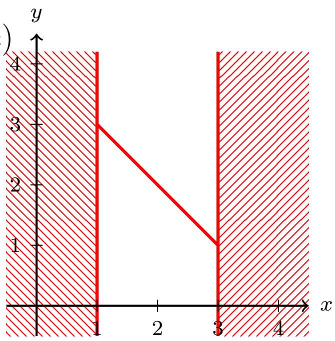
h) $\varphi(x_1, x_2) := (x_1 \leq 1) \wedge (x_1 \geq -1) \to (x_2 = x_1^2 - 1)$

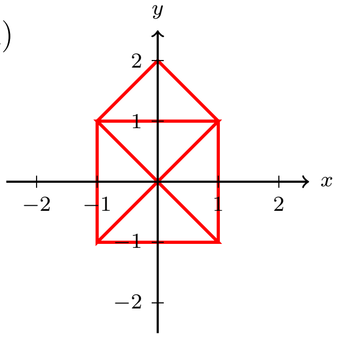
l) $\varphi(x_1, x_2) := ((x_2 \geq 0) \wedge ((x_1 + 1)^2 + x_2^2 - 1 = 0)) \vee ((x_2 \leq 0) \wedge ((x_1 - 1)^2 + x_2^2 - 1 = 0))$

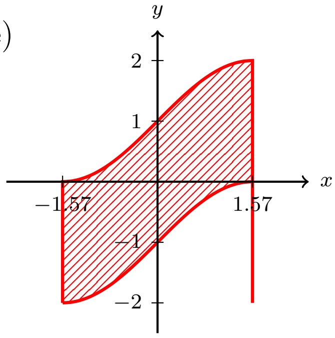
Aufgabe 33. Geben Sie jeweils eine Formel $\varphi(x_1, x_2)$ zur Beschreibung folgender Mengen an.

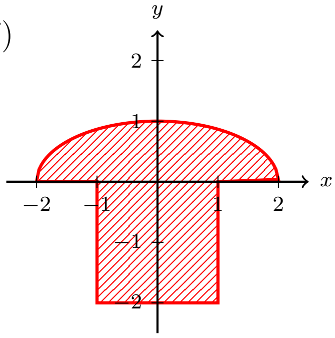
a)


b)


c)


d)


e)


f)


Aufgabe 34. Zeigen Sie unter Anwendung der vollständigen Induktion.

a) Die Summe der ersten n ungeraden Zahlen ist gleich n^2

b) Die Summe der ersten n geraden Zahlen ist gleich $n^2 + n$

c) $\sum_{i=0}^{n-1} 2^i = 2^n - 1$

d) $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

e) $\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$

f) $\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$ $\quad (q \neq 1)$ (geometrische Summenformel)

g) $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ (Binomischer Lehrsatz)

h) Eine n-el. Menge besitzt genau $\binom{n}{k}$ k-el. Teilmengen

Aufgabe 35. Bestimmen Sie jeweils ggT und kgV unter Verwendung der Primfaktorzerlegung.

a) 56, 49 b) 128, 96 c) 500, 525 d) 2205, 22275 e) 68600, 67375, 11011

Aufgabe 36. Bestimmen Sie jeweils den ggT unter Verwendung des erweiterten euklidischen Algorithmus und stellen Sie diesen linear dar.

a) 48, 162 b) 1323, 3087 c) 13475, 2541 d) 24310, 31395 e) 242000, 4695327

Aufgabe 37. Berechnen Sie folgende Terme im jeweiligen Restklassenring.

a) $\bar{3}^2 \cdot (\bar{7} - \bar{8})^3$ in $\mathbb{Z}/4\mathbb{Z}$

b) $(\bar{8} - \bar{3})^4 - (\bar{4} - \overline{10})^{-1}$ in $\mathbb{Z}/13\mathbb{Z}$

c) $-\frac{\bar{8}}{\bar{9}} + \left(\frac{\bar{2}}{\bar{3}} - \frac{\bar{8}}{\bar{5}}\right)^2 - \left(\bar{1} - \frac{\bar{1}}{\overline{18}}\right)$ in $\mathbb{Z}/23\mathbb{Z}$

d) $\left[(-\bar{3})^2\right]^{-3} - \left(-\frac{\bar{2}}{\bar{5}}\right)^4 + \frac{1}{\bar{6}}$ in $\mathbb{Z}/7\mathbb{Z}$

Aufgabe 38.

a) Bestimmen Sie zu den jeweiligen Restklassenringen alle Einheiten und zu jeder Einheit das zugehörige multiplikative Inverse.

i) $\mathbb{Z}/4\mathbb{Z}$ ii) $\mathbb{Z}/6\mathbb{Z}$ iii) $\mathbb{Z}/7\mathbb{Z}$ iv) $\mathbb{Z}/8\mathbb{Z}$ v) $\mathbb{Z}/9\mathbb{Z}$ vi) $\mathbb{Z}/12\mathbb{Z}$ vii) $\mathbb{Z}/15\mathbb{Z}$ viii) $\mathbb{Z}/30\mathbb{Z}$

b) Bestimmen Sie das multiplikative Inverse von $\overline{13}$ in $\mathbb{Z}/9797\mathbb{Z}$

Aufgabe 39. Beim RSA-Kryptosystem wählt man zwei große Primzahlen p und q, und setzt $N = p \cdot q$. Der sog. öffentliche Schlüssel ist eine zufällig gewählte natürliche Zahl e mit $1 < e < \varphi(N)$, die teilerfremd zu $\varphi(N) = (p-1)(q-1)$ ist. Für den sog. geheimen Schlüssel d $(1 < d < \varphi(N))$ gilt: $\bar{d}$ ist das multiplikative Inverse von $\bar{e}$ in $\mathbb{Z}/\varphi(N)\mathbb{Z}$. Die zu verschlüsselnden Daten werden durch natürliche Zahlen $0 \leq m < N$ dargestellt. Die Daten m werden durch Potenzieren $\bar{c} = \bar{m}^e$ in $\mathbb{Z}/N\mathbb{Z}$ verschlüsselt und durch $\bar{m} = \bar{c}^d$ in $\mathbb{Z}/N\mathbb{Z}$ wieder entschlüsselt.

a) Zeigen Sie, dass $e = 35$ ein öffentlicher Schlüssel für $p = 13$ und $q = 17$ ist und bestimmen Sie den zugehörigen geheimen Schlüssel.

b) Verschlüsseln Sie den Text „RSA“, indem Sie zunächst jedem Buchstaben seinen ASCII-Code zuordnen; entschlüsseln Sie anschließend den verschlüsselten Text.

Aufgabe 40. Rechnen Sie in das jeweilige Zahlensystem um.

a) 99 (3-adisch) b) 645 (8-adisch) c) 2048 (16-adisch) d) 1234 (2-adisch)

e) $(756)_8$ (5-adisch) f) $(10AD)_{16}$ (8-adisch) g) $(121212)_3$ (2-adisch) h) $(33333)_4$ (16-adisch)

k) $(1011011101)_2$ (16-adisch, direkt) l) $(AF381ED90D)_{16}$ (2-adisch, direkt)