TECHNISCHE UNIVERSITÄT MÜNCHEN
Zentrum Mathematik

PROF. DR.DR. JÜRGEN RICHTER-GEBERT, DR. HERMANN VOGEL, PETER LEBMEIR

Lineare Algebra und analytische Geometrie 1, Mathematik für Physiker 1 (WS 2005/06)
— Aufgabenblatt 2 (7. November 2005) —

— Multiple choice - Aufgaben —

M 13. Handelt es sich bei den folgenden Mengen mit Verknüpfung um Gruppen?

$(\mathbb{Z}[i],+)$ $(\pi\mathbb{Z},+)$ $(18\mathbb{Z},+)$ $(\mathbb{Z}_{13}^*,\bigodot_{13})$ $(17\mathbb{Z}^*,\cdot)$

M 14. Welche der folgenden Strukturen sind zu Gruppen aus Aufgabe P 7 isomorph?

$(\mathbb{Z}_2,\bigoplus_2)$, $(\mathbb{Z}_3^*,\bigodot_3)$, $(\mathbb{Z}_4^*,\bigodot_4)$, $(\mathbb{Z}_4,\bigoplus_4)$, $(\mathbb{Z}_5^*,\bigodot_5)$

— Präsenzaufgaben —

P 15. Rechnen kongruent n
Für $a,b\in\mathbb{Z}$ und $n\in\mathbb{N}^*$ sei $a=_n b$ genau dann, wenn ein $k\in\mathbb{Z}$ mit $(a-b)=k\cdot n$ existiert.
Zeigen Sie für $a,b,c\in\mathbb{Z}$ und $n\in\mathbb{N}^*$:

i) $a=_n a$

ii) $a=_n b \quad\Rightarrow\quad b=_n a$

iii) $a=_n b \quad\wedge\quad b=_n c \quad\Rightarrow\quad a=_n c$

iv) $a=_n a' \quad\wedge\quad b=_n b' \quad\Rightarrow$

$\alpha)$ $a+b=_n a'+b'$ (d.h. $a\bigoplus_n b=a'\bigoplus_n b'$)

$\beta)$ $ab=_n a'b'$ (d.h. $a\bigodot_n b=a'\bigodot_n b'$)

v) $a=_n b \quad\Rightarrow\quad a^m=_n b^m$ für ein beliebiges $m\in\mathbb{N}$

P 16. Der euklidische Algorithmus.

a) Bestimmen Sie den größten gemeinsamen Teiler (ggT) der Zahlen $a=4620$ und $b=225$, und finden Sie Zahlen $m,n\in\mathbb{Z}$ mit $ggT(a,b)=ma+nb$.

b) Bestimmen Sie den größten gemeinsamen Teiler (ggT) der Polynome
$f(X)=X^5+X^4-2X^2-9X-22$ und $g(X)=X^3+X^2-3X-6$.

P 17. RSA-Freaks.

1) Berechnen Sie die Zahlen

$$(17+13)\mod 3,\quad (17\cdot 6)\mod 7,\quad 5^9\mod 11,\quad 13^{25}\mod 23.$$

2) Der öffentliche Schlüssel $(N,k)=(55,3)$ sei für das RSA-Verfahren gegeben.

a) Überprüfen Sie, ob der Schlüssel die Voraussetzungen des RSA-Verfahrens erfüllt und finden Sie den privaten Schlüssel (N,s).

b) Chiffrieren Sie mit (N,k) die Nachricht "RSA", wobei $A\mapsto 0, B\mapsto 1,\ldots$.

c) Dechiffrieren Sie mit (N,s) die von Ihnen in b.) chiffrierte Nachricht.

— Hausaufgaben —

H 18. Der ggT

a) Seien $a, b \in \mathbb{N}^*$ und $t \in \mathbb{N}^*$ ein ggT von a und b. (Definition siehe Vorlesung!)
Zeigen Sie: t ist eindeutig.

b) Seien $a, b \in \mathbb{N}^*$ mit $a > b$ und $a = q \cdot b + r$ mit $q \in \mathbb{N}^*$ und $0 \leq r < b$.
Zeigen Sie: $ggT(a, b) = ggT(a - qb, b)$

H 19. Zeigen Sie, dass für ein nicht primales $n \in N$ $(\mathbb{Z}_n \backslash \{0\}, \bigodot_n)$ keine Gruppe ist.

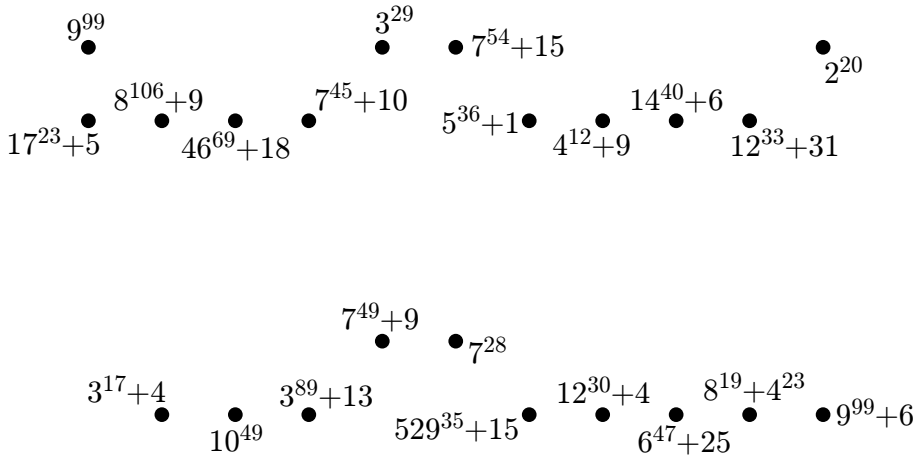
H 20. Der beste Algorithmus der Welt.

a) Bestimmen Sie den größten gemeinsamen Teiler (ggT) der Zahlen $a = 1234575$ und $b = 1234503$, und finden Sie Zahlen $m, n \in \mathbb{Z}$ mit $\text{ggT}(a, b) = ma + nb$.

b) Bestimmen Sie den grten gemeinsamen Teiler (ggT) der Polynome
$f(X) = 14X^5 - 5X^4 - 15X^3 + 19X^2 + 10X + 1$ und $g(X) = 14X^3 - 5X^2 - X$.

c) Geben Sie zwei Zahlen $a, b < 1000$ an, so dass sich bei Division von a und b mit einem Taschenrechner der Näherungswert $2,3088235$ einstellt.

H 21. Malen nach Zahlen modulo 23.



Schliessen Sie Ihre Augen und versetzen Sie sich in die Zeit, in der Malbücher noch eine große Faszination auf Sie ausüben konnten. Blättern Sie in Gedanken in einem solchen Buch. Öffnen Sie nun wieder Ihre Augen — Erinnert Sie unser "Bild" nun an eines aus Ihrem Malbuch?

Falls nicht: Berechnen Sie die angegebenen Zahlen modulo 23. Jeder dicke schwarze Punkt erhält danach eine Nummer zwischen 0 und 22. Verbinden Sie nun die Punkte in der richtigen Reihenfolge. ... und die Realität wird Sie wieder begrüssen. Viel Spass!

Abgabetermin ist der 14.11.2005 in der Zentralübung.

Terminänderung wegen Überschneidung: Klausur Mi, 15.02.2006 um 9-11Uhr