Elementare Zahlentheorie mit Maple (01202) **WS 2013/14**

Klausur am 01.03.2014:

Musterlösungen

Aufgabe 1

(a) Seien $a, b \in \mathbb{Z}$ mit $a \neq 0 \neq b$. Eine ganze Zahl d heißt größter gemeinsamer Teiler von a und b, wenn gilt:

(1) $d \mid a$ und $d \mid b$, und

(2) wenn $c \in \mathbb{Z}$ ein gemeinsamer Teiler von a und b ist, dann gilt $c \leq d$.

(b) Wir berechnen zunächst mit dem Euklidischen Algorithmus den größten gemeinsamen Teiler von 56 und 72:

$$\begin{aligned} 72 &= 1 \cdot 56 + 16 \\ 56 &= 3 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 + 0. \end{aligned}$$

Es ist also $\mathrm{ggT}(56, 72) = 8$. Nun formen wir die Gleichungen nach dem ggT um:

$$\begin{aligned} 8 &= 1 \cdot 56 - 3 \cdot 16 = 1 \cdot 56 - 3 \cdot (1 \cdot 72 - 1 \cdot 56) \\ &= 4 \cdot 56 - 3 \cdot 72. \end{aligned}$$

Es folgt $x = 4, y = -3$.

Aufgabe 2

Seien $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = p$ und p ist eine Primzahl. Dann gibt es $a', b' \in \mathbb{Z}$ mit $a = a'p$ und $b = b'p$ und $\mathrm{ggT}(a', b') = 1$. Insbesondere folgt $p \nmid a'$ oder $p \nmid b'$. Wir behandeln die beiden Teilaufgaben gemeinsam.

Betrachten wir zunächst den Fall $p \nmid a'$. Gilt $p \nmid b'$, dann ist

$$\mathrm{ggT}(a^2, b) = \mathrm{ggT}(a'^2 p^2, b'p) = p$$

und

$$\mathrm{ggT}(a^2, b^2) = \mathrm{ggT}(a'^2 p^2, b'^2 p^2) = p^2.$$

Gilt $p \mid b'$, dann ist $b' = b''p$ für ein $b'' \in \mathbb{Z}$ mit $\mathrm{ggT}(a', b'') = 1$. Also ist

$$\mathrm{ggT}(a^2, b) = \mathrm{ggT}(a'^2 p^2, b''p^2) = p^2$$

und

$$\mathrm{ggT}(a^2, b^2) = \mathrm{ggT}(a'^2 p^2, b''^2 p^4) = p^2.$$

Gilt $p \mid a'$, dann ist $a' = a''p$ für ein $a'' \in \mathbb{Z}$ mit $\mathrm{ggT}(a'', b') = 1$, und $p \nmid b'$. Dann ist

$$\mathrm{ggT}(a^2, b) = \mathrm{ggT}(a''^2 p^4, b'p) = p$$

und

$$\mathrm{ggT}(a^2, b^2) = \mathrm{ggT}(a''^2 p^4, b'^2 p^2) = p^2.$$

Wir sehen also, dass für $\mathrm{ggT}(a^2, b)$ die Werte p und p^2, und für $\mathrm{ggT}(a^2, b^2)$ nur der Wert p^2 möglich sind.

Aufgabe 3

Seien $x, a, n \in \mathbb{N}$ und sei $n > 1$.

Behauptung: Unter der Voraussetzung $x \equiv a \,(\mathrm{mod}\, n)$ gilt $x \equiv a \,(\mathrm{mod}\, 2n)$ oder $x \equiv a + n \,(\mathrm{mod}\, 2n)$.

Beweis: Aus $x \equiv a \,(\mathrm{mod}\, n)$ folgt $n \mid (x-a)$. Das bedeutet, es gibt ein $v \in \mathbb{Z}$ mit $x-a = vn$. Wir unterscheiden nun die beiden Fälle v ist gerade und v ist ungerade.

Fall 1: v ist gerade.
Es gilt $v = 2r$ für ein $r \in \mathbb{Z}$. Daraus folgt $x - a = 2rn$, also $2n \mid (x - a)$, und somit $x \equiv a \,(\mathrm{mod}\, 2n)$.

Fall 2: v ist ungerade.
Sei $v = 2s + 1$ für ein $s \in \mathbb{Z}$. Dann folgt $x - a = (2s + 1)n = 2sn + n$, also $x - a - n = 2sn$. Damit gilt $2n \mid (x - a - n) = (x - (a + n))$, also $x \equiv a + n \,(\mathrm{mod}\, 2n)$.

□

Aufgabe 4

Die Teiler von p^n sind $1, p, p^2, \ldots, p^n$. Also ist

$$\sigma(p^n) = 1 + p + p^2 + \ldots + p^n = \frac{p^n - 1}{p - 1} + p^n.$$

Da $\frac{p^n-1}{p-1} < p^n$ gilt, folgt $\sigma(p^n) < 2p^n$.

Aufgabe 5

Sei (a, b, c) ein primitives pythagoreisches Tripel. Dann gibt es $m, n \in \mathbb{N}$ mit $m \not\equiv n \,(\mathrm{mod}\, 2)$ und $a = 2mn$ und $b = m^2 - n^2$ oder $a = m^2 - n^2$ und $b = 2mn$. In jedem Fall gilt $a + b = 2mn + m^2 - n^2 = 2mn + m^2 + n^2 - 2n^2 = (m + n)^2 - 2n^2$. Wir nehmen zunächst an, dass m gerade ist. Dann sind wegen $m \not\equiv n \,(\mathrm{mod}\, 2)$ die Zahlen n und $m + n$ ungerade. Mit dem gegebenen Hinweis folgt nun $(m + n)^2 \equiv 1 \,(\mathrm{mod}\, 8)$ und $2n^2 \equiv 2 \,(\mathrm{mod}\, 8)$, also $a + b \equiv -1 \equiv 7 \,(\mathrm{mod}\, 8)$. Ist m ungerade, so ist $m + n$ ebenfalls ungerade, aber n gerade, und damit $2n^2 \equiv 0 \,(\mathrm{mod}\, 8)$. Das ergibt $a + b \equiv 1 \,(\mathrm{mod}\, 8)$.

Aufgabe 6

Seien $z, w \in \mathbb{Z}[i]$ mit $\mathrm{ggT}(N(z), N(w)) = 1$. Sei $e = \mathrm{ggT}(z, w)$. Dann gilt $e \mid z$ und $e \mid w$, also gibt es Gauß'sche Zahlen x und y, so dass $z = xe$ und $w = ye$ gilt. Es folgt $N(z) = N(xe) = N(x)N(e)$ und $N(w) = N(ye) = N(y)N(e)$, also $N(e) \mid N(z)$ und

$N(e) \mid N(w)$. Wegen $\mathrm{ggT}\big(N(z), N(w)\big) = 1$ muss $N(e) = 1$ gelten. Also ist e eine Einheit in $\mathbb{Z}[i]$.

Aufgabe 7

(a) Der Fehler besteht darin, dass der `if`-Befehl hier nicht mit dem Befehl `fi;` abgeschlossen wird. Nach dem `return`-Befehl müsste in einer neuen Zeile der Befehl `fi;` eingefügt werden. Richtig sähe die Prozedur also folgendermaßen aus:

```
> # Die Zeilennummerierung dient zu Ihrer Orientierung

 1.  DoppelListe:=proc(L::list,M::list)
 2.  local N, i;
 3.  if nops(L) = nops(M) then
 4.    N:=[];
 5.    for i from 1 to nops(L) do
 6.      N:=[op(N),L[i],M[i]];
 7.    od;
 8.  else
 9.    return("Listen sind nicht gleich lang");
10.  fi;
11.  print(N);
12.  end:
> DoppelListe([1,2,3],[4,5,6]);
                          [1, 4, 2, 5, 3, 6]
```

(b) Eingabe sind die Listen `L`=$[1,2,3]$ und `M`=$[4,5,6]$. In Zeile 3 wird geprüft, ob beide Listen gleich viele Elemente besitzen. Dies ist der Fall, denn es gilt `nops(L)` $= 3 =$ `nops(M)`. Die lokale Variable `N` wird in Zeile 4 als leere Liste initialisiert. In Zeile 5 beginnt eine `for`-Schleife, in der eine neue Liste `N` zusammengesetzt wird. Und zwar werden die Elemente der Listen `L` und `M` abwechselnd eingefügt, beginnend mit der Liste `L`. Im ersten Schleifendurchlauf werden also in Zeile 6 das erste Element der Liste `L` (`L[1]` $= 1$) und das erste Element der Liste `M` (`M[1]` $= 4$) in die Liste `N` eingefügt. Nach dem ersten Durchlauf gilt somit `N`$= [1,4]$. Im zweiten Schleifendurchlauf werden die Elemente `L[2]` $= 2$ und `M[2]` $= 5$ in `N` eingefügt, jetzt gilt `N`$= [1,4,2,5]$. Im dritten und letzten Durchlauf der `for`-Schleife kommen die Elemente `L[3]` $= 3$ und `M[3]` $= 6$ hinzu, also `N`$= [1,4,2,5,3,6]$. Nach Beendigung der `for`-Schleife springt die Prozedur in Zeile 10 (neu 11) und gibt $[1,4,2,5,3,6]$ am Bildschirm aus.

(c) Es ist `N[2]`$= 4$ und `N[5]`$= 3$.

(d) Eine mögliche Prozedur könnte folgendermaßen aussehen:

```
> Ergebnis:=proc()
  local p, i, L;
  p:=unapply(x^6-24*x^4+72*x+12,x);
  L:=[];
  for i from -5 to 2 do
    L:=[op(L),p(i)];
  od;
  return(L);
  end:
> Ergebnis();
```

$$[277, -2324, -1419, -452, -83, 12, 61, -164]$$