Elementare Zahlentheorie mit Maple (01202) SoSe 2012

Klausur am 08.09.2012:

Musterlösungen

Aufgabe 1

Mit der Division von a durch b mit Rest erhalten wir zwei Zahlen $q', r' \in \mathbb{Z}$, so dass $a = q'b + r'$ und $0 \leq r' < b$ gilt. Setzen wir $q = q' - 2$ und $r = r' + 2b$, dann gilt $2b \leq r' + 2b = r < b + 2b = 3b$. Weiter gilt

$$a = q'b + r' = (q+2)b + (r - 2b) = qb + r.$$

Aufgabe 2

Sei $p \geq 5$ eine Primzahl. Wir teilen p durch 3 mit Rest und erhalten $p = 3k + r$ mit $k \in \mathbb{N}$ (denn $p \geq 5$) und $r = 1$ oder $r = 2$. Der Fall $r = 0$ kann nicht auftreten, denn $p \geq 5$ und daher nicht durch 3 teilbar. Im Fall $p = 3k+1$ gilt $p^2+2 = 9k^2+6k+3 = 3(3k^2+2k+1)$. Da $k \geq 1$ ist, ist $3k^2+2k+1 > 1$. Es folgt, dass p^2+2 keine Primzahl ist. Im Fall $p = 3k+2$ gilt $p^2 + 2 = 9k^2 + 12k + 6 = 3(3k^2 + 4k + 6)$, und dies zeigt, dass $p^2 + 2$ keine Primzahl ist. Somit ist $p^2 + 2$ für $p \geq 5$ eine zusammengesetzte Zahl.

Aufgabe 3

Wir zeigen zunächst, dass für alle $a \in \mathbb{Z}$ entweder $a^2 \equiv 0 \,(\mathrm{mod}\, 4)$ oder $a^2 \equiv 1 \,(\mathrm{mod}\, 4)$ gilt. Wir betrachten die möglichen Reste von a modulo 4 und deren Quadrate:

$a \mod 4$	$a^2 \mod 4$
0	0
1	1
2	$4 \equiv 0 \,(\mathrm{mod}\, 4)$
3	$9 \equiv 1 \,(\mathrm{mod}\, 4)$

Seien nun $x = 2m+1$ und $y = 2n+1$ ungerade mit $m, n \in \mathbb{Z}$. Dann gilt $x^2 = 4m^2+4m+1$ und $y^2 = 4n^2+4n+1$. Weiter gilt $x^2+y^2 = 4m^2+4n^2+4m+4n+2$. Mit der Division von $x^2 + y^2$ durch 4 mit Rest erhalten wir $(x^2 + y^2) \bmod 4 = 2$. Da aber alle Quadratzahlen modulo 4 nur den Rest 0 oder 1 haben können, ist $x^2 + y^2$ keine Quadratzahl.

Aufgabe 4

Wir betrachten zunächst den Spezialfall $n = 1$. Wir zeigen, dass für jede multiplikative Funktion $h\colon \mathbb{N} \to \mathbb{N}$ gilt: $h(1) = 1$. Wegen $\mathrm{ggT}(1, 1) = 1$ folgt $h(1) = h(1\cdot 1) = h(1)h(1)$. Da $0 \neq h(1) \in \mathbb{N}$ können wir auf beiden Seiten der Gleichung kürzen und erhalten $h(1) = 1$. Damit gilt $f(1) = 1 = g(1)$.

Sei nun $n \in \mathbb{N}, n > 1$ und sei $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ die kanonische Primfaktorzerlegung von n.

Dann folgt

$$\begin{aligned} f(n) &= f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) && \text{(Primfaktorzerlegung von } n\text{)} \\ &= f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_r^{e_r}) && \text{(Multiplikativität von } f\text{)} \\ &= g(p_1^{e_1}) g(p_2^{e_2}) \cdots g(p_r^{e_r}) && \text{(Voraussetzung } f(p^k) = g(p^k)\text{)} \\ &= g(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) && \text{(Multiplikativität von } g\text{)} \\ &= g(n) && \text{(Primfaktorzerlegung von } n\text{).} \end{aligned}$$

Es gilt also $f(n) = g(n)$ für alle $n \in \mathbb{N}$.

Aufgabe 5

Sei $d = kp$ für ein $k \in \mathbb{N}$. Wir nehmen an, dass die Gleichung $X^2 - dY^2 = -1$ eine Lösung (x_0, y_0) besitzt. Daraus folgt dann

$$x_0^2 + 1 = dy_0^2 = kpy_0^2 \equiv 0 \,(\mathrm{mod}\, p).$$

Da $p > 2$ und $p \equiv 3 \,(\mathrm{mod}\, 4)$ gilt, folgt aber mit Satz 6.2.3, dass die Kongruenz $X^2 \equiv -1 \,(\mathrm{mod}\, p)$ keine Lösung hat. Also war unsere Annahme falsch. Somit folgt in diesem Fall, dass die Gleichung $X^2 - dY^2 = -1$ keine Lösung hat.

Aufgabe 6

Sei $n = a^2 - b^2$. Dann gilt $n = (a + b)(a - b)$. Wir betrachten die folgenden vier Fälle:

1. a und b sind gerade:
   Dann ist $a + b$ gerade und auch $a - b$ ist gerade.
2. a und b sind ungerade:
   Dann sind wieder $a + b$ und auch $a - b$ gerade.
3. a ist gerade, b ist ungerade:
   Die Summe $a + b$ ist dann ungerade, genauso wie die Differenz $a - b$.
4. a ist ungerade, b ist gerade:
   Dieser Fall wird analog behandelt.

Insgesamt ergibt sich, dass $n = a^2 - b^2 = (a + b)(a - b)$ das Produkt aus zwei ganzen Zahlen ist, die entweder beide gerade oder beide ungerade sind.

Aufgabe 7

Eine mögliche Prozedur könnte folgendermaßen aussehen:

```
> divrest:=proc(z::complex,w::complex) # berechnet die Gauss'schen
Zahlen q und r bei Division mit Rest von z durch w
   local b, e, f, u, v, g, h, q, r;
   b:=z/w;
   e:=Re(b);
   f:=Im(b);
   u:=floor(e);
   v:=u+1;
   if abs(u-e) <= 1/2 then
      g:=u;
   else
      g:=v;
   fi;
   u:=floor(f);
   v:=u+1;
   if abs(u-e) <= 1/2 then
      h:=u;
   else
      h:=v;
   fi;
   q:= g+h*I;
   r:= z-q*w;
   print(q);
   print(r);
   end:
```

Eine kürzere Alternative existiert, wenn Sie die Maple-Prozedur `round()` kennen:

```
> divrest:=proc(z::complex,w::complex) # berechnet die Gauss'schen
Zahlen q und r bei Division mit Rest von z durch w
   local b, e, f, g, h, q, r;
   b:=(z/w);
   e:=Re(b);
   f:=Im(b);
   g:=round(e);
   h:=round(f);
   q:= g+h*I;
   r:= z-q*w;
   print(q);
   print(r);
   end:
```