Elementare Zahlentheorie mit Maple (01202) **WS 16/17**

Klausur am 11.03.2017:

Musterlösungen

Aufgabe 1

Da $ab \equiv cd (\mathrm{mod}\, m)$ und $\mathrm{ggT}(m,n)$ ein Teiler von m ist, folgt auch $ab \equiv cd (\mathrm{mod}\, \mathrm{ggT}(m,n))$. Analog folgt aus $b \equiv d (\mathrm{mod}\, n)$ auch $b \equiv d (\mathrm{mod}\, \mathrm{ggT}(m,n))$. Damit gilt

$$ab \equiv cd \equiv cb (\mathrm{mod}\, \mathrm{ggT}(m,n)).$$

Nun gilt $\mathrm{ggT}(b,n) = 1$, also auch $\mathrm{ggT}(b, \mathrm{ggT}(m,n)) = 1$, denn wäre

$$e = \mathrm{ggT}(b, \mathrm{ggT}(m,n)) \neq 1,$$

dann folgte $e \mid b$ und $e \mid \mathrm{ggT}(m,n)$, also $e \mid b$ und $e \mid n$, also auch $e \mid \mathrm{ggT}(b,n)$ und damit wäre $\mathrm{ggT}(b,n) \neq 1$. Wenn nun aber $\mathrm{ggT}(b, \mathrm{ggT}(m,n)) = 1$ gilt, dann gibt es ein $b^{-1} \in \mathbb{Z}$, so dass $bb^{-1} \equiv 1 (\mathrm{mod}\, \mathrm{ggT}(m,n))$ gilt. Wir multiplizieren die Kongruenz $ab \equiv cb (\mathrm{mod}\, \mathrm{ggT}(m,n))$ auf beiden Seiten mit b^{-1} und erhalten

$$a \equiv c (\mathrm{mod}\, \mathrm{ggT}(m,n)).$$

Aufgabe 2

Wir zeigen die Behauptung durch Induktion nach n.

Induktionsanfang: Für $n = 1$ gilt $M_{2^1} = M_2 = 3$ und $\prod_{k=0}^{0} F_k = F_0 = 2^{2^0} + 1 = 3$. Damit stimmt der Induktionsanfang.

Induktionsannahme: Für ein $n \geq 1$ gelte $M_{2^n} = \prod_{k=0}^{n-1} F_k$.

Induktionsschluss: Zu zeigen ist $M_{2^{n+1}} = \prod_{k=0}^{n} F_k$. Es ist

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k \right) F_n = M_{2^n} F_n = (2^{2^n} - 1)(2^{2^n} + 1) = (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1 = M_{2^{n+1}}.$$

Dabei wurde beim zweiten Gleichheitszeichen die Induktionsannahme verwendet und beim vierten die dritte binomische Formel.

Mit dem Prinzip der vollständigen Induktion folgt nun die Behauptung.

Aufgabe 3

(a) Die Primfaktorzerlegung von 1202 ist $1202 = 2 \cdot 601$. Also gilt $\varphi(1202) = \varphi(2)\varphi(601) = 1 \cdot 600 = 600$. Da $\mathrm{ggT}(3, 1202) = 1$ gilt, lässt sich der Satz von Euler anwenden, und es gilt $3^{600} \equiv 1 (\mathrm{mod}\, 1202)$. Es folgt

$$3^{1202} \equiv 3^{2 \cdot 600 + 2} \equiv (3^{600})^2 3^2 \equiv 1^2 9 \equiv 9 (\mathrm{mod}\, 1202).$$

(b) Da 2017 eine Primzahl ist, lässt sich das Korollar des kleinen Satzes von Fermat anwenden, und es folgt $3^{2017} \bmod 2017 = 3$.

(c) Da 78 weder eine Primzahl ist noch $\mathrm{ggT}(78, 3) = 1$ gilt, helfen der kleine Satz von Fermat und der Satz von Euler hier nicht weiter. Wenn wir ein paar Potenzen von 3 berechnen, fällt allerdings auf, dass $3^4 = 81 \equiv 3 (\mathrm{mod}\, 78)$ gilt. Es folgt

$$3^{78} \equiv 3^{64} \cdot 3^{12} \cdot 3^2 \equiv (3^4)^{16} \cdot (3^4)^3 \cdot 3^2 \equiv 3^{16} \cdot 3^3 \cdot 3^2 \equiv (3^4)^4 \cdot 3^4 \cdot 3 \equiv 3^4 \cdot 3 \cdot 3 \equiv 3^3 \equiv 27 (\mathrm{mod}\, 78).$$

Aufgabe 4

Sei $n \in \mathbb{N}$ und sei $n = 2^k \prod_{i=1}^{r} p_i^{e_i}$ die kanonische Primfaktorzerlegung von n, wobei die Primzahlen $p_1, \ldots, p_r$ ungerade sind, $k \geq 0$ und $e_i > 0$ für $1 \leq i \leq r$ gilt. Genau dann ist d ein ungerader, positiver Teiler von n, wenn $n = \prod_{i=1}^{r} p_i^{f_i}$ gilt, wobei $0 \leq f_i \leq e_i$ für alle $1 \leq i \leq r$ gilt. Es ist also $f(n) = \prod_{i=1}^{r} (e_i + 1)$. Seien nun $n, m \in \mathbb{N}$ mit $\mathrm{ggT}(n, m) = 1$ und seien $n = 2^k \prod_{i=1}^{r} p_i^{e_i}$ und $m = 2^l \prod_{j=1}^{s} q_j^{f_j}$ die kanonischen Primfaktorzerlegungen von n und m. Wegen $\mathrm{ggT}(n, m) = 1$ sind die p_i und die q_j alle verschieden. Die kanonische Primfaktorzerlegung von nm ist also

$$nm = 2^{k+l} \prod_{i=1}^{r} p_i^{e_i} \prod_{j=1}^{s} q_j^{f_j}.$$

Damit folgt $f(nm) = \prod_{i=1}^{r} (e_i + 1) \prod_{j=1}^{s} (f_j + 1) = f(n) f(m)$.

Aufgabe 5

Sei $n \in \mathbb{N}$, und es gelte $n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$. Dann folgt $n = \frac{a^2}{b^2} + \frac{c^2}{d^2}$. Wir multiplizieren die Gleichung mit $b^2 d^2$ und erhalten $b^2 d^2 n = a^2 d^2 + b^2 c^2 = (ad)^2 + (bc)^2$. Die natürliche Zahl $b^2 d^2 n$ ist also Summe von zwei Quadraten. Dies bedeutet, dass in der Primfaktorzerlegung von $b^2 d^2 n$ keine Primzahl p mit $p \bmod 4 = 3$ mit ungeradem Exponenten vorkommt. Die Primfaktorzerlegungen von n, b, d seien $n = \prod_{i=1}^{r} p_i^{e_i}$, $b = \prod_{i=1}^{r} p_i^{f_i}$ und $d = \prod_{i=1}^{r} p_i^{g_i}$, wobei $0 \leq e_i, f_i, g_i$ für alle $1 \leq i \leq r$ gilt. Die Primfaktorzerlegung von $b^2 d^2 n$ ist dann

$$b^2 d^2 n = \prod_{i=1}^{r} p_i^{e_i + 2f_i + 2g_i}.$$

Ist also $1 \leq i \leq r$ und p_i eine ungerade Primzahl mit $p_i \bmod 4 = 3$, dann ist $e_i + 2f_i + 2g_i$ gerade, und damit ist auch e_i gerade. In der Primfaktorzerlegung von n kommt also keine ungerade Primzahl p_i mit $p_i \bmod 4 = 3$ mit ungeradem Exponenten vor. Damit ist n die Summe von zwei Quadraten.

Aufgabe 6

Ist z eine Gauß'sche Primzahl, dann ist $N(z) = 2$ oder $N(z) = p$, wobei p eine ungerade Primzahl mit $p \bmod 4 = 1$ ist oder $N(z) = p^2$, wobei p eine Primzahl mit $p \bmod 4 = 3$ ist.

Wenn $N(z) \leq 5$ gelten soll, kommen also für $N(z)$ nur 2 und 5 in Frage. Gilt $N(a+bi) = a^2 + b^2 = 2$, wobei $a, b \in \mathbb{Z}$ gilt, dann folgt $a = \pm 1$ und $b = \pm 1$, also $z = 1 + i$, $z = 1 - i$, $z = -1 + i$ oder $z = -1 - i$. Gilt $N(a+bi) = a^2 + b^2 = 5$ mit $a, b \in \mathbb{Z}$, dann folgt $a = \pm 1$ und $b = \pm 2$ oder $a = \pm 2$ und $b = \pm 1$. Es ergeben sich die Gauß'schen Zahlen

$$1 + 2i, 1 - 2i, -1 + 2i, -1 - 2i, 2 + i, 2 - i, -2 + i, -2 - i.$$

Zusammen erhält man also 12 Gauß'sche Zahlen, deren Norm 2 oder 5 ist. Da in jedem Fall die Norm eine Primzahl ist, sind diese 12 Zahlen auch wirklich Gauß'sche Primzahlen.

Aufgabe 7

(a) In eine sinnvolle Reihenfolge gebracht sieht die Prozedur folgendermaßen aus (mit Einrückungen):

```
with(GaussInt):
aufgabe7:=proc()
 local z,i,j,L;
 L:=[];
 i:=-2;
 while i <= 2 do
   for j from -2 to 2 do
     z:=i+I*j;
     if GInorm(z)<= 5 then
       if GIprime(z) then
         L:=[op(L),z]
       fi;
     fi;
   od;
   i:=i+1;
 od;
print(L);
end:
```

Eine (aber nicht die einzige) sinnvolle Reihenfolge der Zeilen aus der Aufgabe wäre also 10,1,7,16,17,5,15,18,12,14,3,4,8,9,13,6,11,2.

(b) Die Prozedur berechnet alle Gauß'schen Primzahlen, deren Norm kleiner oder gleich 5 ist, und gibt diese in einer Liste aus.

Aufgabe 8

Eine mögliche Lösung der Aufgabe wäre die folgende Prozedur:

```
with(numtheory):
Teilersumme:=proc(a::posint)
   #Untersucht, ob es wahr ist, dass für mehr als 3/4 aller Zahlen n
   #zwischen 1 und a die Teilersumme < 2n ist.
   local i,j;
   j:=0;
   for i from 1 to a do
      if sigma(i)< 2*i then j:=j+1 fi;
   od;
   print(j/a);
   if j/a > 3/4 then print(true)
      else print(false)
   fi;
end:
```

```
> Teilersumme(10375);
```

$$\frac{7793}{10375}$$

$$\mathit{true} \qquad (1)$$