Elementare Zahlentheorie mit Maple (01202) **SoSe 2011**

Klausur am 10.09.2011:

Musterlösungen

Aufgabe 1

Wir verwenden den Euklidischen Algorithmus. Es ist

$$\begin{aligned} 299 &= 247 + 52 \\ 247 &= 4 \cdot 52 + 39 \\ 52 &= 39 + 13 \\ 39 &= 3 \cdot 13. \end{aligned}$$

Es folgt $\mathrm{ggT}(299, 247) = 13$. Jetzt stellen wir die Gleichungen oben nach den Resten um, setzen ein und erhalten:

$$\begin{aligned} 52 &= 299 - 247 \\ 39 &= 247 - 4 \cdot 52 \\ &= 247 - 4(299 - 247) = -4 \cdot 299 + 5 \cdot 247 \\ 13 &= 52 - 39 \\ &= (299 - 247) - (-4 \cdot 299 + 5 \cdot 247) = 5 \cdot 299 - 6 \cdot 247. \end{aligned}$$

Mit $s = 5$ und $t = -6$ gilt $13 = 299s + 247t$.

Aufgabe 2

Sei $n \in \mathbb{N}$, und sei p eine Primzahl. Sei $d = \mathrm{ggT}(n, n + p)$, Dann gilt $d \mid n$ und $d \mid n + p$, also $d \mid n + p - n$. Somit ist d ein Teiler von p, also $d = 1$ oder $d = p$. Ist p kein Teiler von n, so ist p auch kein Teiler von d, denn jede Primzahl, die d teilt, teilt auch n. Es folgt, dass $d = 1$ ist, sofern p kein Teiler von n ist. Ist p ein Teiler von n, dann ist p auch ein Teiler von $n + p$ und somit von $\mathrm{ggT}(n, n + p) = d$. Es folgt, dass $d = p$ ist, sofern p ein Teiler von n ist.

Aufgabe 3

Nach Annahme gilt $m \mid x - a$ und $n \mid x - b$. Da $d = \mathrm{ggT}(m, n)$ ist, folgt $d \mid x - a$ und $d \mid x - b$, also $d \mid (x - b) - (x - a)$. Es folgt $d \mid a - b$, also ist $a \equiv b (\mathrm{mod} d)$.

Aufgabe 4

Wir multiplizieren die Kongruenz $x \equiv ca^{\varphi(m)-1} (\mathrm{\ mod\ } m)$ mit a. Dies liefert $ax \equiv ca^{\varphi(m)} (\mathrm{\ mod\ } m)$. Mit dem Satz von Euler ist $a^{\varphi(m)} \equiv 1 (\mathrm{mod} m)$, also $ax \equiv c (\mathrm{mod} m)$.

Aufgabe 5

Sei $a^{p-1} + b^{p-1} = c^{p-1}$. Angenommen, p ist kein Teiler von abc. Dann ist p weder ein Teiler von a noch von b noch von c. Mit dem Kleinen Satz von Fermat gilt $a^{p-1} \equiv 1 (\mathrm{mod} p)$, $b^{p-1} \equiv 1 (\mathrm{mod} p)$ und $c^{p-1} \equiv 1 (\mathrm{mod} p)$. Es folgt $a^{p-1} + b^{p-1} \equiv 2 (\mathrm{mod} p)$, aber $c^{p-1} \equiv 1 (\mathrm{mod} p)$. Das ist ein Widerspruch, und es folgt $p \mid abc$.

Aufgabe 6

Angenommen, $R_k = m^2$ für ein $k \in \mathbb{N}$. Ist $m = 2n$ gerade, so ist $m^2 = 4n^2$ kongruent zu 0 modulo 4. Ist $m = 2n + 1$ ungerade, so ist $m^2 = 4n^2 + 4n + 1$ kongruent zu 1 modulo 4.

Sei $R_k = p_1 \cdots p_k + 1$. Die Zahl $p_1 \cdots p_k$ ist durch 2, aber nicht durch 4 teilbar. Somit gilt $p_1 \cdots p_k \equiv 2(\text{mod}4)$, und es folgt $R_k \equiv 3(\text{mod}4)$ für alle $k \in \mathbb{N}$. Es folgt, dass $R_k \neq m^2$ ist.

Aufgabe 7

Sei z ein Teiler von z'. Dann gibt es ein $w \in \mathbb{Z}[i]$ mit $zw = z'$. Dann gilt

$$N(z') = N(zw) = N(z)N(w),$$

das heißt, $N(z)$ ist ein Teiler von $N(z')$. Die Umkehrung dieser Aussage gilt nicht. Die Gauß'schen Zahlen $1 + 4i$ und $1 - 4i$ sind Gauß'sche Primzahlen, denn ihre Norm ist 17. Ihre Normen sind also Teiler voneinander, als Primzahlen sind sie allerdings keine Teiler voneinander.

Aufgabe 8

1. Wird die Prozedur mit der Eingabe $a = b = 1$ gestartet, dann wird zunächst in Zeile 3 geprüft, ob $a^2 + b^2 = 0$ gilt. Das ist nicht der Fall, also wird in Zeile 5 weitergemacht. Dort wird x auf $\frac{a}{a^2} + b^2$ gesetzt (es sind keine Klammern gesetzt!), also $x := 2$. Analog wird in Zeile 6 dann y auf $\frac{-b}{a^2} + b^2$, also auf 0 gesetzt. In Zeile 7 wird dann also $2, 0$ ausgegeben.

2. Bei den Zuweisungen in den Zeilen 5 und 6 müssen Klammern gesetzt werden. Richtig muss es heißen:

```
>  #Die Zeilennummerierung ist zu Ihrer Orientierung
1.  klausur:=proc(a::integer,b::integer)
2.      local x,y;
3.      if a^2+b^2=0 then
4.       print("nicht invertierbar");
5.       else x:= a/(a^2+b^2);
6.        y:= -b/(a^2+b^2);
7.        print(x,y);
8.     fi;
9.   end:
```

3. Eine Prozedur, wie in der Aufgabe gefordert, wäre:

```
>  #Die Zeilennummerierung ist zu Ihrer Orientierung
1.  mult:=proc(a::integer,b::integer,c::integer,d::integer)
2.      local x,y;
3.        x:= a*c-b*d;
4.        y:= a*d+b*c;
5.        print(x,y);
6.   end:
```