Elementare Zahlentheorie mit Maple (01202) SS 2014

Klausur am 23.08.2014:

Musterlösungen

Aufgabe 1

(a) Aus $a \mid b$ bzw. $b \mid a$ folgt, dass es $x, y \in \mathbb{Z}$ gibt mit $b = ax$ bzw. $a = by$. Wir setzen ein und erhalten $a = by = (ax)y = a(xy)$. Daraus folgt $xy = 1$, also $x = y = \pm 1$. Wir erhalten damit $a = \pm b$, die Behauptung.

(b) Wir betrachten folgendes Gegenbeispiel: $a = 3, b = 6, c = 9$. Es gilt $3 \mid 6$ und $3 \mid 9$, aber $6 \nmid 9$.

(c) Aus $a \mid c$ folgt, dass es ein $x \in \mathbb{Z}$ gibt mit $c = ax$. Wir quadrieren und erhalten $c^2 = (ax)^2 = a^2x^2$. Es gilt also $a^2 \mid c^2$. Mit $c^2 \mid d^2$ folgt dann $a^2 \mid d^2$.

Aufgabe 2

Da p und q beide ungerade sind, ist $p + q$ gerade. Daher können wir schreiben

$$p + q = 2 \cdot \frac{p+q}{2}.$$

Da p und q aufeinanderfolgende Primzahlen sind und $\frac{p+q}{2}$ zwischen diesen beiden Primzahlen liegt, muss $\frac{p+q}{2}$ eine zusammengesetzte Zahl sein. Daraus folgt, dass die Zahl das Produkt von mindestens zwei Primzahlen ist. Damit ist $2 \cdot \frac{p+q}{2} = p + q$ das Produkt von mindestens drei Primzahlen.

Aufgabe 3

Wegen $\mathrm{ggT}(5, 11) = 1$ ist der Kleine Satz von Fermat anwendbar.

Damit gilt $5^{10} \equiv 1 \pmod{11}$ und es folgt

$$5^{72} \equiv (5^{10})^7 \cdot 5^2 \equiv 1^7 \cdot 5^2 \equiv 25 \equiv 3 \pmod{11}.$$

Aus $5^{72} \equiv 3 \pmod{11}$ folgt, dass 11 ein Teiler von $5^{72} - 3$ ist.

Aufgabe 4

Behauptung: Die Funktion ist multiplikativ.

Beweis: Seien $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$ und p eine Primzahl. Dann betrachten wir 4 Fälle:

1. $p \mid m, p \mid n$:
   Es folgt zunächst $p \mid mn$. Damit gilt $f(mn) = 0 = 0 \cdot 0 = f(m)f(n)$.
2. $p \mid m, p \nmid n$:
   Es folgt $p \mid mn$. Also gilt $f(mn) = 0 = 0 \cdot 1 = f(m)f(n)$.

3. $p \nmid m, p \mid n$:
   Dieser Fall verläuft analog zu Fall 2.
4. $p \nmid m, p \nmid n$:
   Es gilt also $p \nmid mn$, und damit folgt $f(mn) = 1 = 1 \cdot 1 = f(m)f(n)$.

Aufgabe 5

(a) Wir betrachten zunächst die Pell'sche Gleichung $X^2 - dY^2 = 1$. Diese hat unter der Voraussetzung, dass $d > 0$ keine Quadratzahl ist, immer eine (nicht-triviale) Lösung (x, y). Wir multiplizieren beide Seiten der Gleichung $x^2 - dy^2 = 1$ mit 4 und erhalten $4 = 4(x^2 - dy^2) = 4x^2 - 4dy^2 = (2x)^2 - (2y)^2 d$. Damit ist $(2x, 2y)$ eine Lösung der Gleichung.

(b) Bei gegebener Fundamentallösung zu einer Pell'schen Gleichung haben alle positiven Lösungen die Form (a_n, b_n) mit $a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n$ für alle $n \in \mathbb{N}$. Die Pell'sche Gleichung $X^2 - 6Y^2 = 1$ hat die Fundamentallösung $(5, 2)$. Damit gilt $a_2 + b_2\sqrt{6} = (a_1 + b_1\sqrt{6})^2 = (5 + 2 \cdot \sqrt{6})^2 = 49 + 20\sqrt{6}$, also $(a_2, b_2) = (49, 20)$.

Aufgabe 6

1. Lösungsvorschlag:

Wenn wir Gauß'sche Zahlen v und w finden können mit $N(v) = 17$ und $N(w) = 29$, dann gilt wegen der Multiplikativität der Norm

$$N(vw) = N(v)N(w) = 17 \cdot 29 = 493 = N(z).$$

Setzen wir dann $z = vw$, so haben wir eine Gauß'sche Zahl mit der gewünschten Norm gefunden. Sei $a+bi \in \mathbb{Z}[i]$. Dann gilt $N(a+bi) = a^2+b^2$. Wir können also $a = 4$ und $b = 1$ setzen und erhalten $v = 4+i$ und $N(v) = 4^2 + 1^2 = 17$. Analog folgt für $w = 5+2i \in \mathbb{Z}[i]$, dass $N(w) = 5^2 + 2^2 = 25 + 4 = 29$. Nun können wir z wie folgt berechnen:

$$z = vw = (4 + i)(5 + 2i) = 18 + 13i.$$

a und b bzw. c und d sind aber nicht eindeutig, da z. B. $a^2 + b^2 = b^2 + a^2$ gilt. Wir können also auch $v = b + ai = 1 + 4i$ setzen, analog bei w. Dadurch ergeben sich dann möglicherweise andere Zahlen z.

2. Lösungsvorschlag:

Fr $z = a + bi \in \mathbb{Z}[i]$ gilt $N(z) = N(a + bi) = a^2 + b^2$. Mit Lemma 6.2.9 folgt

$$\begin{aligned} N(z) &= 493 = 17 \cdot 29 \\ &= (16 + 1)(25 + 4) \\ &= (4^2 + 1^2)(5^2 + 2^2) \\ &= (4 \cdot 5 + 1 \cdot 2)^2 + (4 \cdot 2 - 1 \cdot 5)^2 && \text{(Lemma 6.2.9)} \\ &= 22^2 + 3^2. \end{aligned}$$

Wir erhalten hier also die Gauß'sche Zahl $z = 22 + 3i$.

An dieser Lösung sehen wir auch, dass z nicht eindeutig ist, da hier für die Zerlegungen von 17 und 29 dasselbe gilt wie in Lösungsvorschlag 1.

Aufgabe 7

Eine mögliche Prozedur könnte folgendermaßen aussehen:

```
> Lagrange:=proc() # gibt eine Darstellung aller ungeraden n
                     von 7 bis 75 durch p+2*q an
  local n, p, q;
  for n from 7 by 2 to 75 do
    p:=2;
    while p < n do
      q:=2;
      while q < n do
        if n=p+2*q then
          print([n,p,q]);
          p:=n;
          q:=n;
        fi;
        q:=nextprime(q);
      od;
      p:=nextprime(p);
    od;
  od;
  end:
```

Wir lassen n von 7 bis 75 laufen, berücksichtigen aber nur die ungeraden Zahlen, was wir durch die Anweisung „`by 2`“ in der `for`-Schleife erreichen. Im Anschluss daran verwenden wir zwei `while`-Schleifen, um die Primzahlen p und q von 2 bis n durchlaufen zu lassen. Dabei wir die obere Schranke auf n gesetzt (p und q sind zwangsläufig kleiner als n), um die Laufzeit nicht unnötig zu erhöhen. In der inneren `while`-Schleife wird die Bedingung abgefragt, ob n die Form $p + 2q$ für ein p und ein q hat. Ist dies der Fall, so wird $[n, p, q]$ ausgegeben und es werden p und q auf n gesetzt, um die beiden `while`-Schleifen zu beenden und zum nächsten n überzugehen (eine Darstellung für n genügt uns nach Aufgabenstellung). Ist die Bedingung nicht erfüllt, so wird q auf die nächsthöhere Primzahl gesetzt und die innere `while`-Schleife wird erneut durchlaufen. Wird zum aktuellen p kein passendes $q < n$ gefunden, so wird die innere `while`-Schleife beendet und zur nächstgrößeren Primzahl p gesprungen und die innere `while`-Schleife erneut durchlaufen. Diese Vorgänge wiederholen sich, bis wir bei $n = 75$ angelangt sind.

Aufgabe 8

(a) Die Prozedur wird mit dem Befehl `zusgesetzt(3,4,2,6);` aufgerufen. Da alle übergebenen Parameter natürliche Zahlen sind, ist die Bedingung `posint` erfüllt. Die lokale Variable `n` wird deklariert und im Anschluss auf $3^2+4^2+2^2+6^2 = 9+16+4+36 =$

65 gesetzt. In der nachfolgenden `if`-Abfrage wird geprüft, ob $3 \cdot 4 = 2 \cdot 6$ gilt. Wegen $3 \cdot 4 = 12 = 2 \cdot 6$ wird der `then`-Zweig ausgeführt. Hier wird 65 am Bildschirm ausgegeben, ebenso wie die Primfaktorzerlegung von 65, nämlich `(5)(13)`. Der `else`-Zweig wird nicht ausgeführt. Die `if`-Anweisung wird mit `fi;` beendet und die Prozedur endet ebenfalls.

(b) Die Ausgabe auf den Befehl `zusgesetzt(3,4,2,5);` lautet `false`. In der `if`-Abfrage gilt $3 \cdot 4 = 12 \neq 10 = 2 \cdot 5$. Daher wird der `else`-Zweig ausgeführt. Hier wird das Ergebnis von `isprime(54)` ausgegeben.

(c) Die Eingabe `zusgesetzt(3,-4,2,6);` löst eine Fehlermeldung aus. Der Prozedur dürfen nur natürliche Zahlen übergeben werden (`posint`). -4 ist keine natürliche Zahl.