Elementare Zahlentheorie mit Maple (01202) **SS 2017**

Klausur am 02.09.2017:

Musterlösungen

Aufgabe 1

(a) Die Behauptung ist falsch. Ein Gegenbeispiel ist $a = 2$, $b = 2$ und $c = 4$, denn $2^2 + 1 = 5$, $2^4 + 1 = 17$, und 5 ist kein Teiler von 17.

(b) Mit der 3. binomischen Formel gilt für alle $m > 1$:

$$g_m - 2 = a^{2^m} - 1 = (a^{2^{m-1}} + 1)(a^{2^{m-1}} - 1) = g_{m-1} \cdot (g_{m-1} - 2),$$

also $g_{m-1} \mid g_m - 2$ und $g_{m-1} - 2 \mid g_m - 2$.

Für $n < m$ folgt nun $g_n \mid g_{n+1} - 2$. Außerdem gilt $g_{n+1} - 2 \mid g_{n+2} - 2$, $g_{n+2} - 2 \mid g_{n+3} - 2$, $\ldots, g_{m-1} - 2 \mid g_m - 2$, so dass $g_{n+1} - 2 \mid g_m - 2$ und insgesamt $g_n \mid g_m - 2$ folgt.

Sei $\mathrm{ggT}(g_n, g_m) = d$, d.h. $d \mid g_n$ und $d \mid g_m$ für alle $m, n \in \mathbb{N}, m > n$. Wegen $g_n \mid g_m - 2$ gibt es ein $k \in \mathbb{Z}$, sodass gilt $g_m = k \cdot g_n + 2$. Da $d \mid g_n$ und $d \mid g_m$ gilt, folgt $d \mid 2$, also ist $d = 1$ oder $d = 2$.
Wir unterscheiden zwei Fälle:

- Sei a gerade. Dann ist a^{2^n} gerade und somit $g_n = a^{2^n} + 1$ ungerade.
- Sei a ungerade. Dann ist a^{2^n} ungerade und somit $g_n = a^{2^n} + 1$ gerade.

Es folgt

$$\mathrm{ggT}(g_n, g_m) = \begin{cases} 1, & \text{falls a gerade ist,} \\ 2, & \text{falls a ungerade ist.} \end{cases}$$

Aufgabe 2

Sei (a, b) eine Lösung für $2x^2 + (x + 3)^2 = y^2$, d.h. es gilt

$$2a^2 + (a + 3)^2 = b^2 \Leftrightarrow 2a^2 + a^2 + 6a + 9 = 3a^2 + 6a + 9 = b^2.$$

Betrachten wir die Gleichung modulo 3, so erhalten wir

$$b^2 = 3a^2 + 6a + 9 \equiv 3a^2 \equiv 0 (\mathrm{mod}\, 3),$$

also $b^2 \equiv 0 (\mathrm{mod}\, 3)$ und, da 3 eine Primzahl ist, folgt $b \equiv 0 (\mathrm{mod}\, 3) \Leftrightarrow 3 \mid b$.
Betrachten wir die Gleichung modulo 9, so erhalten wir

$$3a^2 + 6a + 9 \equiv 3a^2 + 6a \equiv b^2 (\mathrm{mod}\, 9).$$

Da $3 \mid b$ ist, folgt $9 \mid b^2$, also $b^2 \equiv 0 (\mathrm{mod}\, 9)$ und somit

$$3a^2 + 6a \equiv 0 (\mathrm{mod}\, 9).$$

Wegen $3a^2 + 6a = 3(a^2 + 2a)$ und $9 \mid 3(a^2 + 2a)$ muss $3 \mid a^2 + 2a$ sein.
Um a näher zu bestimmen, betrachten wir die drei möglichen Fälle:

- Sei $a \equiv 0 (\mathrm{mod}\, 3)$. Dann ist
$$a^2 + 2a \equiv 0^2 + 2 \cdot 0 \equiv 0 (\mathrm{mod}\, 3),$$
also $3 \mid a^2 + 2a$.
- Sei $a \equiv 1 (\mathrm{mod}\, 3)$. Dann ist
$$a^2 + 2a \equiv 1^2 + 2 \cdot 1 \equiv 3 \equiv 0 (\mathrm{mod}\, 3),$$
also $3 \mid a^2 + 2a$.
- Sei $a \equiv 2 (\mathrm{mod}\, 3)$. Dann ist
$$a^2 + 2a \equiv 2^2 + 2 \cdot 2 \equiv 8 \equiv 2 (\mathrm{mod}\, 3),$$
also $3 \nmid a^2 + 2a$, ein Widerspruch.

Es folgt, $a \equiv 0 (\mathrm{mod}\, 3)$ oder $a \equiv 1 (\mathrm{mod}\, 3)$.

(Alternativ zur Fallunterscheidung: Da $3 \mid a^2 + 2a$, folgt $3 \mid a(a+2)$, also gilt entweder $3 \mid a \Leftrightarrow a \equiv 0 (\mathrm{mod}\, 3)$ oder $3 \mid (a+2) \Leftrightarrow a \equiv 1 (\mathrm{mod}\, 3)$.)

Aufgabe 3

(a) Sei $n \in \mathbb{N}$ eine Primzahl mit $n > 3$, also gilt $\sigma(n) = n + 1$. Da dann $n - 1$ keine Primzahl ist, gibt es mindestens einen echten Teiler $d \in \mathbb{Z}$ mit $1 < d < n - 1$. $d = 2$ ist so ein Teiler, da $n - 1$ gerade ist. Es folgt
$$\sigma(n-1) \geq 1 + 2 + (n-1) = n + 2 > n + 1 = \sigma(n),$$
die Behauptung.

(b) Sei $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$ mit $k \in \mathbb{N}$ die kanonische Primfaktorzerlegung von $n \in \mathbb{N}$. Dann gilt
$$\sigma(n) = \sigma(p_1^{e_1}) \cdot \dots \cdot \sigma(p_k^{e_k}).$$
$\sigma(n)$ ist genau dann ungerade, wenn jeder einzelne Faktor ungerade ist.
Wir betrachten den Spezialfall $n = p^k$ für eine Primzahl p und schauen, wann $\sigma(p^k) = 1 + p + p^2 + \ldots + p^k$ ungerade ist:

- $p = 2$: Es gilt $\sigma(2^k) = 1 + 2 + 2^2 + \ldots + 2^k \equiv 1 (\mathrm{mod}\, 2)$, d.h. dieser Term ist immer ungerade.
- $p \neq 2$, also $p > 2$: Wegen $p^j \equiv 1 (\mathrm{mod}\, 2)$ für alle $j \in \mathbb{N}$ folgt
$$\sigma(p^k) \equiv \sum_{i=0}^{k} 1 (\mathrm{mod}\, 2),$$
also $\sigma(p^k) \equiv k + 1 (\mathrm{mod}\, 2)$ und $\sigma(p^k)$ ist genau dann ungerade, wenn k gerade ist.

Zusammengefasst ist $\sigma(n)$ genau dann ungerade, wenn in der Primfaktorzerlegung von n für ein beliebiges $n \in \mathbb{N}$ bei allen ungeraden Primzahlen nur gerade Exponenten vorkommen, d.h. n ist von der Form $n = 2^k \cdot m^2$, wobei m ungerade und $k \geq 0$ beliebig ist.

Aufgabe 4

Zu lösen ist das System linearer Kongruenzen

$$\begin{aligned} x_0 &\equiv 2(\mathrm{mod}7) \\ x_0 &\equiv 3(\mathrm{mod}6) \\ x_0 &\equiv 0(\mathrm{mod}5). \end{aligned}$$

Es ist $m_1 = 7, m_2 = 6, m_3 = 5, M = 7 \cdot 6 \cdot 5 = 210, M_1 = 30, M_2 = 35, M_3 = 42$.
Wir berechnen die Lösungen der $M_i X \equiv 1(\mathrm{mod}\, m_i), i = 1, 2, 3$, mit dem erweiterten Euklidischen Algorithmus:

- $i = 1 : 30X \equiv 1(\mathrm{mod}\, 7)$
  Es ist $\mathrm{ggT}(30, 7) = 1 = (-3) \cdot 30 + 13 \cdot 7$, also $s = -3$ und $t = 13$. Wir erhalten $x_1 = -3 \mod 7 = 4$.
- $i = 2 : 35X \equiv 1(\mathrm{mod}\, 6)$
  Es ist $\mathrm{ggT}(35, 6) = 1 = (-1) \cdot 35 + 6 \cdot 6$, also $s = -1$ und $t = 6$. Wir erhalten $x_2 = -1 \mod 6 = 5$.
- $i = 3 : 42X \equiv 1(\mathrm{mod}\, 5)$
  Es ist $\mathrm{ggT}(42, 5) = 1 = (-2) \cdot 42 + 17 \cdot 5$, also $s = -2$ und $t = 17$. Wir erhalten $x_3 = -2 \mod 5 = 3$.

Wir erhalten

$$\begin{aligned} x_0 &= (2 \cdot 30 \cdot 4 + 3 \cdot 35 \cdot 5 + 0 \cdot 42 \cdot 3) \mod 210 \\ &= (240 + 525) \mod 210 \\ &= (30 + 105) \mod 210 \\ &= 135 \mod 210 \\ &= 135. \end{aligned}$$

Peters Mutter hat demnach mindestens 135 Schokoladenbonbons gekauft.

Aufgabe 5

(a) Da 17 eine Primzahl ist und $17 \nmid 3$ folgt $\mathrm{ggT}(3, 17) = 1$. Mit dem Kleinen Satz von Fermat folgt $3^{16} \equiv 1 (\mathrm{mod}\, 17)$.
Mit dem Hinweis in der Aufgabenstellung erhalten wir

$$3^{2640} \equiv (3^{48})^{55} \equiv ((3^{16})^3)^{55} \equiv (1^3)^{55} \equiv 1^{55} \equiv 1 (\mathrm{mod}\, 17).$$

Daraus folgt mit $2643 = 48 \cdot 55 + 3$

$$3^{2643} \equiv 3^{48 \cdot 55 + 3} \equiv (3^{48})^{55} \cdot 3^3 \equiv 3^3 \equiv 27 \equiv 10 (\mathrm{mod}\, 17).$$

(b) Die Primfaktorzerlegung von 1515 ist $1515 = 3 \cdot 5 \cdot 101$. Es gilt also

$$\varphi(1515) = \varphi(3) \cdot \varphi(5) \cdot \varphi(101) = 2 \cdot 4 \cdot 100 = 800.$$

Da $\mathrm{ggT}(7, 1515) = 1$ gilt, lässt sich der Satz von Euler anwenden. Es ist somit $7^{800} \equiv 1 (\mathrm{mod}\, 1515)$.
Daraus folgt

$$7^{2402} \equiv 7^{3 \cdot 800 + 2} \equiv (7^{800})^3 \cdot 7^2 \equiv 1^3 \cdot 7^2 \equiv 7^2 \equiv 49 (\mathrm{mod}\, 1515).$$

Aufgabe 6

Nach Definition ist $N(z) = N(a+bi) = a^2+b^2$. Mit $(a^2+b^2)\cdot(c^2+d^2) = (ac+bd)^2\cdot(ad-bc)^2$ (Lemma 6.2.9) folgt

$$\begin{aligned}
N(z) &= 1073 \\
&= 29 \cdot 37, && \text{da } 1073 = 29 \cdot 37 \\
&= (25 + 4) \cdot (36 + 1) \\
&= (5^2 + 2^2) \cdot (6^2 + 1^2) \\
&= (5 \cdot 6 + 2 \cdot 1)^2 \cdot (5 \cdot 1 - 2 \cdot 6)^2, && \text{mit Lemma 6.2.9} \\
&= 32^2 + (-7)^2 \\
&= 32^2 + 7^2,
\end{aligned}$$

also ist z=32+7i ist eine der gesuchten Gauß'schen Zahlen.

Sei $N(v) = 29$ und $N(w) = 37$, und somit $N(vw) = 29 \cdot 37 = 1073$. Wir setzen $z := vw$, denn dann ist

$$29 = N(z) = N(a + bi) = a^2 + b^2, \text{ also z.B. } a = 5 \text{ und } b = 2, \text{ d.h. } v = 5 + 2i \text{ und}$$

$$37 = N(z) = N(a + bi) = a^2 + b^2, \text{ also z.B. } a = 6 \text{ und } b = 1, \text{ d.h. } v = 6 + i.$$

Es folgt

$$z = vw = (5 + 2i)(6 + i) = 30 + 5i + 12i - 2 = 28 + 17i,$$

eine zweite Gauß'sche Zahl, für die $N(z) = 1073$ gilt.

Aufgabe 7

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

```
1  LinKong:=proc(m::posint)
2  local i,J,N,a;
3  J:={}; #Menge für Lösungen
4  N:={}; #Menge für keine Lösungen
5  a:=1;
6  while a < m do
7       for i from 1 to m-1 do
8            if a*i mod m=3 mod m then
9                 J:=J union {[a,i]};
10                else
11                N:=N union {[a,i]};
12           fi;
13      od;
14      a:=a+1;
15 od;
16 print(J);
17 print(N);
18 end:
```

```
> LinKong(4);
                          {[1, 3], [3, 1]}
        {[1, 1], [1, 2], [2, 1], [2, 2], [2, 3], [3, 2], [3, 3]}
```

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

(b) Die Prozedur berechnet die Lösungen von $aX \equiv 3 (\mathrm{mod}\, m)$ für alle $a < m$ und ein gegebenes $m \in \mathbb{N}$. Die X, die eine Lösung sind, werden zusammen mit a in J ausgegeben, und die X, die keine Lösung sind, sind in N. (Die Rollen von J und N können

Für $m = 4$ erhalten wir als Ausgabe:

$$J := \{[1,3],[3,1]\} \text{ und } N := \{[1,1],[1,2],[2,1],[2,2],[2,3],[3,2],[3,3]\}.$$

Aufgabe 8

Eine mögliche Lösung der Aufgabe wäre die folgende Prozedur:

```
primlist:=proc(m::posint) (*berechnet g und ordnet es, abhängig
     ob Primzahl oder nicht, einer passenden Liste zu
     (ggf. inkl. Primfaktorzerlegung)*)
     local n,g,f,L,N;
     L:=[];
     N:=[];
     for n from 1 to m do
          g:=2*n^2+3*n-1;
          if isprime(g) then
               L:=[op(L),[n,g]]
          else
               f:=ifactor(g);
               N:=[op(N),[n,g,f]];
          fi;
     od;
     print(L);
     print(N);
end:

> primlist(5);
```

$$[[2, 13], [4, 43]]$$

$$[[1, 4, (2)^2], [3, 26, (2)\ (13)], [5, 64, (2)^6]] \quad \textbf{(1)}$$