Ausgewählte Kapitel der elementaren Zahlentheorie: 5. Übungsblatt

Sophiane Yahiatène – syahiate@math.uni-bielefeld.de

May 18, 2018

Aufgabe 1

(a) Seien $a, b \in \mathbb{Z}$ mit Primfaktorzerlegung $a = u_1 \cdot \prod_{p \text{ Primzahl}} p^{n_p}$ und $b = u_2 \cdot \prod_{p \text{ Primzahl}} p^{m_p}$, wobei fast alle $n_p, m_p \in \mathbb{Z}$ Null und u_1, u_2 Einheiten in $\mathbb{Z}$ sind. Es ist leicht einzusehen, dass

$$\mathrm{ggT}(a, b) = u \cdot \prod_{p \text{ Primzahl}} p^{\min(n_p, m_p)}$$

gilt, wobei u eine Einheit in $\mathbb{Z}$ ist. Also erhählt man für $a = 5, b = 5^2$ und $m = 2^2 \cdot 5$

$$\mathrm{ggT}(a, m) = u \cdot 2^{\min(0,2)} \cdot 5^{\min(1,1)} = 5$$
$$\mathrm{ggT}(b, m) = u \cdot 2^{\min(0,2)} \cdot 5^{\min(1,2)} = 5.$$

(b) Seien $a, b, m \in \mathbb{Z}$ mit $a \equiv b \mod m$, d.h. es existiert ein $n \in \mathbb{Z}$ mit $a = n \cdot m + b$. Wir zeigen nun, dass $d := \mathrm{ggT}(b, m)$ der ggT von a und m ist. Dazu stellen wir zunächst fest, dass d sowohl a als auch m teilt. Die Zahl d teilt bereits nach Definition m und wegen $a = n \cdot m + b$ auf a.
Als nächstes zeigen wir, dass jeder Teiler u von a und m auch d teilt. Da u die Zahlen a und m teilt, teilt u wegen $b = a - n \cdot m$ auch b. Also gilt nach Definition von d, dass $u \mid d$.

Aufgabe 2

Seien $m \in \mathbb{N}$, $z \in \mathbb{Z}$ und $r_1, r_2 \in \{0, 1, \ldots, m-1\}$ mit $r_1 \equiv z \equiv r_2 \mod m$, so gilt nach Definition $m \mid r_1 - r_2$ und insbesondere $m \mid |r_1 - r_2|$. Aus $0 \leq r_1, r_2 \leq m - 1$ folgt $0 \leq |r_1 - r_2| \leq m - 1$ und somit insgesamt $|r_1 - r_2| = 0$. Aus letzterem folgt $r_1 = r_2$.

Aufgabe 3

Zunächst stellt man fest, dass für $n, x \in \mathbb{Z}$ mit $x \equiv n \mod 9$ folgendes gilt: $3 \mid x$ genau dann, wenn $3 \mid n$. Dies sieht man ein, indem man bemerkt, dass aufgrund der Voraussetzung $9 \mid (x - n)$ gilt und somit insbesondere $3 \mid (x - n)$, d.h. $x \equiv n \mod 3$. Aus letzterem folgt die Eigenschaft.
Man kann leicht verifizieren, dass die einzigen Kubikzahlen $\mod 9$ gerade $0, 1$ und 8 sind. Es gilt nämlich

$$\begin{aligned}
0^3 &\equiv 0 \mod 9,\\
1^3 &\equiv 1 \mod 9,\\
2^3 &\equiv 8 \mod 9,\\
3^3 &\equiv 0 \mod 9,\\
4^3 &\equiv 1 \mod 9,\\
5^3 &\equiv 8 \mod 9,\\
6^3 &\equiv 0 \mod 9,\\
7^3 &\equiv 1 \mod 9 \text{ und}\\
8^3 &\equiv 8 \mod 9.
\end{aligned}$$

Da nur Zahlen teilerfremd zu 3 betrachtet werden sollen und wegen der anfänglichen Feststellung, sind die einzigen relevanten Reste $\mod 9$ gerade nur 1 und 8. Eine mögliche Lösung der Gleichung $(x, y, z) \in \mathbb{Z}^3$ hat die Eigenschaft: $(x^3 \mod 9, y^3 \mod 9, z^3 \mod 9) \in \{\overline{1}, \overline{8}\}^3$. Da aber die Zahlen 1 und 8 die Gleichung $\mod 9$ nicht lösen, existiert ein solches Triple nicht, d.h. die anfängliche Gleichung hat unter den gegebenen Eigenschaft keine Lösung in $\mathbb{Z}$.

Aufgabe 4

Sei $a \in \mathbb{Z}$ mit Primfaktorzerlegung $a = u \cdot \prod_{p \text{ Primzahl}} p^{n_p}$, so ist a genau dann Summe zweier Quadrate, wenn für jede Primzahl p aus der Faktorisierung mit $p \equiv 3 \mod 4$ mit geradem Exponenten auftritt.

(a) Die Zahl $16120 = 2^3 \cdot 5 \cdot 13 \cdot 31$ ist keine Summe zweier Quadrate, denn es gilt $13 \equiv 3 \mod 4$ und 13 tritt mit ungeradem Exponenten in der Faktorisierung auf.

(b) Die Zahl $278650175 = 3^2 \cdot 5^2 \cdot 7^3 \cdot 19^2$ ist keine Summe zweier Quadrate, denn es gilt $7 \equiv 3 \mod 4$ und 7 tritt mit ungeradem Exponenten in der Faktorisierung auf.

(c) Die Zahl $153632709 = 3^2 \cdot 23^4 \cdot 61$ ist Summe zweier Quadrate. Es gilt

$$\begin{aligned}
3^2 &= 3^2 + 0,\\
23^4 &= (23^2)^2 + 0 \text{ und}\\
61 &= 5^2 + 6^2
\end{aligned}$$

und somit

$$\begin{aligned}
153632709 &= N(3) \cdot N(23^2) \cdot N(5+6i) \\
&= N(3 \cdot 23^2 \cdot (5+6i)) \\
&= N(3 \cdot 23^2 \cdot 5 + 3 \cdot 23^2 \cdot 6i) \\
&= (3 \cdot 23^2 \cdot 5)^2 + (3 \cdot 23^2 \cdot 6)^2.
\end{aligned}$$