Albert–Ludwigs–Universität Freiburg
Institut für Mathematik
Abteilung für Reine Mathematik
PD Dr. K. Halupczok
Dipl.–Math. S. Feiler

Klausur zur Vorlesung

Elementare Zahlentheorie

Sommersemester 2009

Musterlösung

15. Juli 2009 — 4 Seiten

Klausuraufgabe 1
Bestimmen Sie alle durch 7 teilbaren $n \in \mathbb{N}$, für die $n \equiv 1 \bmod 4$, $n \equiv 1 \bmod 5$ und $n \equiv 1 \bmod 6$ gilt.

Lösung:
In der Aufgabenstellung sind sämtliche $n \in \mathbb{N}$ mit

$$n \equiv 1 \bmod 4,\ n \equiv 1 \bmod 5,\ n \equiv 1 \bmod 6 \text{ und } n \equiv 0 \bmod 7$$

gesucht. Für alle $n \in \mathbb{N}$ mit $n \equiv 1 \bmod 12$ gilt $n \equiv 1 \bmod 4$ und $n \equiv 1 \bmod 6$.
Für alle $n \in \mathbb{N}$ mit $n \equiv 1 \bmod 4$ und $n \equiv 1 \bmod 6$ gilt $n \equiv 1 \bmod [4,6]$ mit $[4,6] = 12$.
Also gilt für alle $n \in \mathbb{N}$

$$(n \equiv 1 \bmod 4 \quad \text{und} \quad n \equiv 1 \bmod 6) \qquad \Longleftrightarrow \qquad n \equiv 1 \bmod 12.$$

Gesucht werden also alle $n \in \mathbb{N}$ mit

$$n \equiv 1 \bmod 5, \qquad n \equiv 0 \bmod 7 \qquad \text{und} \qquad n \equiv 1 \bmod 12.$$

Seien $m_1 := 5$, $m_2 := 7$, $m_3 := 12$, $M_1 := m_2 \cdot m_3 = 84$, $M_2 := m_3 \cdot m_1 = 60$ und $M_3 := m_1 \cdot m_2 = 35$.
Gesucht werden $M_1^* \in \mathbb{Z}$, $M_2^* \in \mathbb{Z}$ und $M_3^* \in \mathbb{Z}$ mit $M_1 \cdot M_1^* \equiv 1 \bmod m_1$, $M_2 \cdot M_2^* \equiv 1 \bmod m_2$ und $M_3 \cdot M_3^* \equiv 1 \bmod m_3$. Für alle $M_1^* \in \mathbb{Z}$, alle $M_2^* \in \mathbb{Z}$ und alle $M_3^* \in \mathbb{Z}$ gilt

$$\begin{aligned}
M_1 \cdot M_1^* \equiv 1 \bmod m_1 &\iff 84 \cdot M_1^* \equiv 1 \bmod 5 \iff (-1) \cdot M_1^* \equiv 1 \bmod 5 \\
&\iff M_1^* \equiv -1 \bmod 5, \\
M_2 \cdot M_2^* \equiv 1 \bmod m_2 &\iff 60 \cdot M_2^* \equiv 1 \bmod 7 \iff 4 \cdot M_2^* \equiv 1 \bmod 7 \\
&\iff M_2^* \equiv 2 \bmod 7
\end{aligned}$$

und

$$\begin{aligned}
M_3 \cdot M_3^* \equiv 1 \bmod m_3 &\iff 35 \cdot M_3^* \equiv 1 \bmod 12 \iff (-1) \cdot M_3^* \equiv 1 \bmod 12 \\
&\iff M_3^* \equiv -1 \bmod 12.
\end{aligned}$$

Mit dem Chinesischen Restsatz ergibt sich für alle $n \in \mathbb{N}$

$$\begin{aligned}
&n \equiv 1 \bmod 4,\ n \equiv 1 \bmod 5,\ n \equiv 1 \bmod 6 \text{ und } 7|n \\
&\quad\iff n \equiv 1 \bmod 5, \qquad n \equiv 0 \bmod 7 \qquad \text{und} \qquad n \equiv 1 \bmod 12 \\
&\quad\iff n \equiv 1 \cdot 84 \cdot (-1) + 0 \cdot 60 \cdot 2 + 1 \cdot 35 \cdot (-1) \bmod (5 \cdot 7 \cdot 12) \\
&\quad\iff n \equiv (-84 - 35) \bmod (60 \cdot 7) \\
&\quad\iff n \equiv -119 \bmod 420 \\
&\quad\iff n \equiv 301 \bmod 420.
\end{aligned}$$

Klausuraufgabe 2
Zeigen Sie:
Sind $p_1, \ldots, p_{\omega(m)} \in \mathbb{P}$ die verschiedenen Primteiler von $m \in \mathbb{N}$ und gilt $\varphi\left(p_1 \cdots p_{\omega(m)}\right) | m$, so folgt $m = \varphi\left(\dfrac{m \cdot p_1 \cdots p_{\omega(m)}}{\varphi\left(p_1 \cdots p_{\omega(m)}\right)}\right)$.

Lösung:
Seien $m \in \mathbb{N}$ mit der Primfaktorzerlegung $\prod_{j=1}^{\omega(m)} p_j^{a_j}$ und $\ell := \prod_{j=1}^{\omega(m)} p_j$. Es gelte $\varphi(\ell) | m$.
Mit $\ell = \prod_{j=1}^{\omega(m)} p_j$ und $\varphi(\ell) | m$ folgt wegen Bemerkung 1.18

$$\varphi(\ell) = \varphi\left(\prod_{j=1}^{\omega(m)} p_j\right) = \prod_{j=1}^{\omega(m)} \varphi(p_j) = \prod_{j=1}^{\omega(m)} (p_j - 1) = \prod_{j=1}^{\omega(m)} p_j^{b_j}$$

mit $b_j \in \mathbb{N}_0$ und $b_j \leq a_j$ für alle $j \in \mathbb{N}$ mit $j \leq \omega(m)$.
Deshalb ist

$$\frac{m \cdot \ell}{\varphi(\ell)} = \frac{\prod_{j=1}^{\omega(m)} p_j^{a_j} \cdot \prod_{j=1}^{\omega(m)} p_j}{\prod_{j=1}^{\omega(m)} p_j^{b_j}} = \prod_{j=1}^{\omega(m)} p_j^{a_j - b_j + 1}.$$

Wegen $a_j \geq b_j$ ist $a_j - b_j + 1 \geq 1$ für alle $j \in \mathbb{N}$ mit $j \leq \omega(m)$.
Damit ergibt sich

$$\varphi\left(\frac{m \cdot \ell}{\varphi(\ell)}\right) = \varphi\left(\prod_{j=1}^{\omega(m)} p_j^{a_j - b_j + 1}\right) = \prod_{j=1}^{\omega(m)} \varphi\left(p_j^{a_j - b_j + 1}\right) = \prod_{j=1}^{\omega(m)} (p_j - 1) \cdot p_j^{a_j - b_j}$$
$$= \prod_{j=1}^{\omega(m)} (p_j - 1) \cdot \prod_{j=1}^{\omega(m)} p_j^{a_j - b_j} = \prod_{j=1}^{\omega(m)} p_j^{b_j} \cdot \prod_{j=1}^{\omega(m)} p_j^{a_j - b_j} = \prod_{j=1}^{\omega(m)} p_j^{a_j} = m.$$

Klausuraufgabe 3
Seien $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $(a, p) = 1$ und $\operatorname{ord}_p(a) = 3$.
Zeigen Sie, dass $(a + 1, p) = 1$ gilt.

Lösung:
<u>1. Möglichkeit</u>
Wegen $\operatorname{ord}_p(a) = 3$ wird $a^3 - 1$ von p geteilt.
Es ist $(a - 1) \cdot (a^2 + a + 1) = a^3 + a^2 + a - a^2 - a - 1 = a^3 - 1$.
Wegen $\operatorname{ord}_p(a) = 3 > 1$ ist $a^1 \not\equiv 1 \bmod p$ und deshalb gilt $p \nmid (a - 1)$. Das zeigt $p | (a^2 + a + 1)$.
Die Annahme $p | (a + 1)$ führt wegen $a^2 = (a^2 + a + 1) - (a + 1)$ damit zu $p | a^2$.
Das bedeutet $(a, p) \geq p$ mit Widerspruch zu $(a, p) = 1$. Also gilt $(a + 1, p) = 1$.
<u>2. Möglichkeit</u>
Die Annahme $p | (a + 1)$ führt zu $a^2 = a^2 - 1 + 1 = (a - 1) \cdot (a + 1) + 1 \equiv 1 \bmod p$.
Daraus folgte $\operatorname{ord}_p(a) \leq 2$ mit Widerspruch zu $\operatorname{ord}_p(a) = 3$. Also gilt $(a + 1, p) = 1$.
<u>3. Möglichkeit</u>
Die Annahme $p | (a + 1)$ führt zu $a \equiv -1 \bmod p$.
Daraus folgte $a^3 \equiv -1 \bmod p$ im Widerspruch zu $a^3 \equiv 1 \bmod p$, was sich aus $\operatorname{ord}_p(a) = 3$ ergibt.

Klausuraufgabe 4
Bestimmen Sie alle Lösungen der Kongruenz $(x+2)^4 - 2x^2 - 8x - 7 \equiv 0 \bmod 163$.

Lösung:
Seien $f: \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & f(x) := (x+2)^4 - 2x^2 - 8x - 7 \end{array} \right\}$, $g: \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & g(x) := (x-1)^2 \end{array} \right\}$ und $h: \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & h(x) := (x+2)^2 \end{array} \right\}$.
Für alle $x \in \mathbb{R}$ gilt

$$\begin{aligned} f(x) &= (x+2)^4 - 2x^2 - 8x - 7 & &= (x+2)^4 - 2 \cdot \left(x^2 + 4 \cdot x + 4\right) + 1 \\ &= \left((x+2)^2\right)^2 - 2 \cdot (x+2)^2 + 1 & &= (h(x))^2 - 2 \cdot h(x) + 1 \\ &= (h(x) - 1)^2 & &= g(h(x)). \end{aligned}$$

Für alle $x \in \mathbb{Z}$ ist also $f(x) \equiv 0 \bmod 163 \iff g(h(x)) \equiv 0 \bmod 163$.
Suche zunächst alle $y \in \mathbb{Z}$ mit $g(y) \equiv 0 \bmod 163$.
Es ist $163 = 81 \cdot 2 + 1 = 54 \cdot 3 + 1 = 32 \cdot 5 + 3 = 23 \cdot 7 + 2 = 14 \cdot 11 + 9 < 13^2 = 169$.
Nach dem Sieb des Erathostenes ist $163 \in \mathbb{P}$ und für alle $y \in \mathbb{Z}$ gilt

$$g(y) \equiv 0 \bmod 163 \iff 163 | (y-1)^2 \overset{163 \in \mathbb{P}}{\iff} 163 | (y-1) \iff y \equiv 1 \bmod 163.$$

Damit folgt für alle $x \in \mathbb{Z}$

$$\begin{aligned} & f(x) \equiv 0 \bmod 163 \\ \iff\ & g(h(x)) \equiv 0 \bmod 163 \iff h(x) \equiv 1 \bmod 163 \\ \iff\ & (x+2)^2 \equiv 1 \bmod 163 \iff x + 2 \equiv 1 \bmod 163 \text{ oder } x + 2 \equiv -1 \bmod 163 \\ \iff\ & x \equiv 160 \bmod 163 \text{ oder } x \equiv 162 \bmod 163, \end{aligned}$$

da es nach dem Satz von Lagrange höchstens zwei $z \in \mathbb{Z}$ mit $-81 < z \leq 81$ und $z^2 \equiv 1 \bmod 163$ gibt und $1^2 = (-1)^2 = 1 \equiv 1 \bmod 163$ gilt.

Klausuraufgabe 5
Zeigen Sie: Für alle $a \in \{99, 999, 9999, 99999, \ldots\}$ gilt $11 | a$ oder $\left(\frac{11}{a}\right) = -1$.

Lösung:
Es gibt ein $n \in \mathbb{N}$ mit $a = \sum_{j=0}^{n} 9 \cdot 10^j = 9 \cdot \sum_{j=0}^{n} 10^j = 9 \cdot \frac{10^{n+1} - 1}{10 - 1} = 10^{n+1} - 1$.
Damit folgt

$$a = 10^{n+1} - 1 = 10^2 \cdot 10^{n-1} - 1 \equiv -1 \bmod 4 \equiv 3 \bmod 4$$

und

$$a = 10^{n+1} - 1 \equiv (-1)^{n+1} - 1 \bmod 11 \equiv \begin{cases} 0 \bmod 11, & \text{falls } n \text{ ungerade} \\ 9 \bmod 11, & \text{falls } n \text{ gerade} \end{cases}.$$

Ist n ungerade, so wird a also von 11 geteilt.
Ist n gerade, so folgt mit den Rechenregeln für das Jacobi–Symbol

$$\left(\frac{11}{a}\right) \underset{a \equiv 3(4) \equiv 11(4)}{\overset{\text{QRG}}{=}} (-1) \cdot \left(\frac{a}{11}\right) \overset{a \equiv 9(11)}{=} (-1) \cdot \left(\frac{9}{11}\right) = (-1) \cdot \left(\frac{3^2}{11}\right) = (-1) \cdot 1 = -1.$$

Klausuraufgabe 6
Beweisen Sie die Identität $\Lambda \cdot \ln + \Lambda * \Lambda = \mu * \ln^2$.

Lösung:
Nach Folgerung 5.7 (3) ist $\mathbb{1} * \Lambda = \ln$. Damit folgt für alle $n \in \mathbb{N}$

$$\begin{aligned}
&(\mathbb{1} * ((\Lambda \cdot \ln) + (\Lambda * \Lambda)))(n) = (\mathbb{1} * (\Lambda \cdot \ln) + \mathbb{1} * (\Lambda * \Lambda))(n) \\
&\quad = (\mathbb{1} * (\Lambda \cdot \ln))(n) + ((\mathbb{1} * \Lambda) * \Lambda)(n) = \sum_{d|n} \mathbb{1}(d) \cdot (\Lambda \cdot \ln)\left(\frac{n}{d}\right) + (\ln * \Lambda)(n) \\
&\quad = \sum_{d|n} \Lambda\left(\frac{n}{d}\right) \cdot \ln\left(\frac{n}{d}\right) + \sum_{d|n} \ln(d) \cdot \Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \Lambda\left(\frac{n}{d}\right) \cdot \left(\ln\left(\frac{n}{d}\right) + \ln(d)\right) \\
&\quad = \ln(n) \cdot \sum_{d|n} \mathbb{1}(d) \cdot \Lambda\left(\frac{n}{d}\right) = \ln(n) \cdot (1 * \Lambda)(n) \\
&\quad = \ln^2(n).
\end{aligned}$$

Mit der MÖBIUSschen Umkehrformel 5.11 folgt die Behauptung.

Klausuraufgabe 7
Begründen Sie, warum die Zahlen der Form $(M_p + 1) \cdot k - 1$ mit $M_p := 2^p - 1$, $p \in \mathbb{P} \setminus \{2\}$ und $k \in \mathbb{N}$ nicht als Summe dreier Quadratzahlen geschrieben werden können.

Lösung:
Für alle $p \in \mathbb{P} \setminus \{2\}$ ist $M_p = 2^p - 1$. Seien nun $p \in \mathbb{P} \setminus \{2\}$ und $k \in \mathbb{N}$.
Es ist $(M_p + 1) \cdot k - 1 = 2^p \cdot k - 1 = 2^{p-3} \cdot 8k - 1 = 8 \cdot (2^{p-3} \cdot k - 1) + 7$.
Seien also $a := 0 \in \mathbb{N}_0$ und $b := 2^{p-3} \cdot k - 1 \in \mathbb{N}_0$. Dann gilt $(M_p + 1) \cdot k - 1 = 4^a \cdot (8b + 7)$ und mit dem Satz von LEGENDRE ist also $(M_p + 1) \cdot k - 1$ nicht als Summe dreier Quadrate darstellbar.

Klausuraufgabe 8
Sei $n \in \mathbb{N}$ mit $\mu^2(n) \cdot \omega(n) = 2$ gegeben.
Wie lässt sich ein nicht–trivialer Teiler von n bestimmen, wenn die Werte n und $\varphi(n)$ bekannt sind?

Lösung:
Sei $n \in \mathbb{N}$ mit $\mu(n) \cdot \omega(n) = 2$. Wegen $\omega(m) \geq 0$ für alle $m \in \mathbb{N}$ und $2 > 0$ gilt $\mu(n) > 0$.
Das führt wegen $\mu(m) \in \{-1, 0, 1\}$ aber zu $\mu(n) = 1$ und damit ergibt sich $\omega(n) = 2$.
Es gibt also ein $p \in \mathbb{P}$ und ein $q \in \mathbb{P} \setminus \{p\}$ mit $n = pq$.
Damit folgt $\varphi(n) = \varphi(pq) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1) = pq - p - q + 1 = n - p - q + 1$.
Multipliziert man die letzte Gleichung mit p, so erhält man $p \cdot \varphi(n) = pn - p^2 - pq + p$ bzw.

$$p^2 - (n - \varphi(n) + 1) \cdot p + n = 0 \qquad \text{und} \qquad q^2 - (n - \varphi(n) + 1) \cdot q + n = 0$$

folgt analog nach Multiplikation der Gleichung mit q.
Da p und $q \neq p$ also Nullstellen des (durch n und $\varphi(n)$ eindeutig bestimmten) Polynoms

$$f: \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & f(x) := x^2 - (n - \varphi(n) + 1) \cdot x + n \end{array} \right\}$$

sind und das Polynom (als Polynom zweiten Grades) maximal zwei Nullstellen hat, erhält man p und q durch Ermitteln der Nullstellen von f.