Lösungen der Klausur in Elementarer Zahlentheorie, SoSe 2007

Aufgabe 1

Zeige, dass für alle $n > 1$ gilt: Falls $n^2 + 2$ prim ist, so ist n durch 3 teilbar.

Lösung:

Angenommen n sei nicht durch 3 teilbar. $\Rightarrow n \equiv 1(3)$ oder $n \equiv 2(3)$
$\Rightarrow n^2 \equiv 1(3) \Rightarrow n^2 + 2 \equiv 0(3) \Rightarrow n = 1$ oder $n^2 + 2$ zusammengesetzt. $\square$

Aufgabe 2

Bestimme alle Lösungen der Kongruenz

$$7x^2 + x + 22 \equiv 0 \ (60).$$

Lösung:

Sei $f(x) := 7x^2 + x + 22$. $\quad 60 = 2^2 \cdot 3 \cdot 5$.

- Bestimmen der Lösungen mod 2 durch Ausprobieren:

  $f(x) \equiv x^2 + x \ (2)$. Lösungen mod 2 sind $x \equiv 0 \ (2)$ und $x \equiv 1 \ (2)$.

- Bestimmen der Lösungen mod 4 durch den Aufsteigesatz:

  $f'(x) = 14x + 1 \equiv 1 \not\equiv 0 \ (2) \Rightarrow$ Jede Lösung modulo 2 liefert genau eine Lösung modulo 4.

  $f(x) \equiv 3x^2 + x + 2 \ (4)$.
  $0 + 2b, b \in \{0, 1\}$ ist Lösung für $b = 1$.
  $1 + 2b, b \in \{0, 1\}$ ist Lösung für $b = 1$.

  $\Rightarrow x \equiv 2 \ (4)$ und $x \equiv 3 \ (4)$ sind alle Lösungen modulo 4.

  (Alternativ können die Lösungen mod 4 auch durch Ausprobieren gefunden werden.)

- Bestimmen der Lösungen mod 3 durch Ausprobieren:

  $f(x) \equiv x^2 + x + 1 \ (3)$. Einzige Lösung modulo 3 ist $x \equiv 1 \ (3)$.

- Bestimmen der Lösungen mod 5 durch Ausprobieren:

  $f(x) \equiv 2x^2 + x + 2 \ (5)$. Einzige Lösung modulo 5 ist $x \equiv 1 \ (5)$.

- Bestimmen der Lösungen mod 60 durch den chinesischen Restsatz:

  Es müssen die beiden folgenden Kongruenzensysteme gelöst werden:

  $$x \equiv 1 \ (3), \quad x \equiv 2 \ (4), \quad x \equiv 1 \ (5) \tag{1}$$

  und

  $$x \equiv 1 \ (3), \quad x \equiv 3 \ (4), \quad x \equiv 1 \ (5) \tag{2}$$

$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 4 \cdot 5$.
$M_1 = 20, \quad M_2 = 15, \quad M_3 = 12. \quad M_i M_i^* \equiv 1 \ (m_i)$
$\Rightarrow 20 \ M_1^* \equiv -M_1^* \equiv 1 \ (3) \Rightarrow M_1^* = -1,$
$15 \ M_2^* \equiv -M_2^* \equiv 1 \ (4) \Rightarrow M_2^* = -1,$
$12 \ M_3^* \equiv 2 \ M_3^* \equiv 1 \ (5) \Rightarrow M_3^* = 3.$
$\Rightarrow x \equiv -20x_1 - 15x_2 + 36x_3 \ (60).$

Zu (1):$x_1 = 1, \quad x_2 = 2, \quad x_3 = 1$
$\Rightarrow x \equiv -20 - 30 + 36 = -14 \equiv 46 \ (60).$

Zu (2):$x_1 = 1, \quad x_2 = 3, \quad x_3 = 1$
$\Rightarrow x \equiv -20 - 45 + 36 = -29 \equiv 31 \ (60).$

$\Rightarrow x \equiv 31 \ (60)$ und $x \equiv 46 \ (60)$ sind alle Lösungen modulo 60.

□

Aufgabe 3

Zeige: Ist $(m_1, m_2) = 1$ und $na \equiv nb \ (m_i)$ für $i = 1, 2$, so folgt

$$a \equiv b \ \left(\frac{m_1 m_2}{(m_1, n)(m_2, n)} \right).$$

Lösung:

$na \equiv nb \ (m_i) \overset{2.1.(5)}{\Longrightarrow} a \equiv b \left(\frac{m_i}{(n, m_i)} \right), \quad i = 1, 2.$ Also gilt nach 2.1.(6)
$a \equiv b \left(\left[\frac{m_1}{(n,m_1)}, \frac{m_2}{(n,m_2)} \right] \right)$, d.h. $a \equiv b \left(\frac{m_1 \cdot m_2}{(n,m_1)(n,m_2)} \right)$, da $(m_1, m_2) = 1$ und damit auch $\left(\frac{m_1}{(n,m_1)}, \frac{m_2}{(n,m_2)} \right) = 1.$ □

Aufgabe 4

Sei $(m, n) = 1$. Zeige: Für jedes $z \in \mathbb{Z}, \ (z, mn) = 1$, existieren $x, y \in \mathbb{Z}, \ (x, n) = (y, m) = 1$, mit $z = xm + yn$.

Lösung:

Nach dem Euklidischen Algorithmus gibt es eine Darstellung $1 = am + bn$ mit $a, b \in \mathbb{Z}$. Also ist $z = zam + zbn = xm + yn$ mit $x = za, \ y = zb$. Sei nun $d := (x, n) \Rightarrow d | xm + yn = z$ und wegen $d | n$ folgt $d | (z, n) = 1 \Rightarrow d = 1$. Ebenso sieht man: $(y, m) = 1$. □

Aufgabe 5

Für ungerade natürliche Zahlen x und m zeige: $\mathrm{ord}_{2m}(x) = \mathrm{ord}_m(x)$.

Lösung:

Sei $d := \mathrm{ord}_{2m}(x)$, dann ist $x^d \equiv 1\ (2m)$, also auch $x^d \equiv 1\ (m) \Rightarrow \mathrm{ord}_m(x) \leq \mathrm{ord}_{2m}(x)$.

Sei $t := \mathrm{ord}_m(x)$, dann ist $x^t \equiv 1\ (m)$. Da $x \equiv 1\ (2)$ ist auch $x^t \equiv 1\ (2)$, also folgt $x^t \equiv 1\ ([2,m])$, wobei $[2,m] = 2m$, da m ungerade. Also $\mathrm{ord}_{2m}(x) \leq \mathrm{ord}_m(x)$.

Alternativ:

Sei $t := \mathrm{ord}_m(x)$, dann ist $x^t \equiv 1\ (m) \Rightarrow x^t = 1 + gm,\ g \in \mathbb{Z}$. Zu zeigen: g ist gerade, denn dann gilt $x^t = 1 + gm = 1 + g' \cdot 2m$ mit $g' = g/2 \in \mathbb{Z}$ und damit $x^t \equiv 1\ (2m)$, also $\mathrm{ord}_{2m}(x) \leq \mathrm{ord}_m(x)$.

$x^t = 1 + gm \Rightarrow x^t - 1 = gm$. Die linke Seite ist gerade, da x und damit x^t ungerade ist. Da m ungerade ist, muss also g gerade sein. Damit ist alles gezeigt. □

Aufgabe 6

Gilt $\omega(n) \cdot \mu^2(n) = 2$, so ist $n + 1 - \varphi(n)$ die Summe zweier Primzahlen.

Lösung:

$\omega(n) \cdot \mu^2(n) = 2 \Rightarrow \omega(n) = 2$ und $\mu(n) = 1 \Rightarrow n = p \cdot q,\quad p, q$ prim, und $n + 1 - \varphi(n) = p\,q + 1 - \varphi(p\,q) = p\,q + 1 - (p-1)(q-1) = p + q$. □

Aufgabe 7

Sei $\lambda(n) := (-1)^{\Omega(n)}$. Zeige, dass gilt:

$$\sum_{d|n} \mu(d)\lambda(d) = 2^{\,\omega(n)}.$$

Lösung:

Wir zeigen, dass $L(n) := \sum_{d|n} \mu(d)\lambda(d)$ multiplikativ ist und rechnen die Identität auf Primzahlpotenzen nach.

Für n_1, n_2 mit $(n_1, n_2) = 1$ gilt:

$$L(n) := \sum_{d|n} \mu(d)\lambda(d) = \sum_{\substack{d_1|n_1 \\ d_2|n_2}} \mu(d_1 d_2)\lambda(d_1 d_2) \underset{\mu,\lambda \text{ mult.}}{=} \sum_{\substack{d_1|n_1 \\ d_2|n_2}} \mu(d_1)\mu(d_2)\lambda(d_1)\lambda(d_2)$$

$$= \sum_{d_1|n_1} \mu(d_1)\lambda(d_1) \sum_{d_2|n_2} \mu(d_2)\lambda(d_2) = L(n_1)L(n_2).$$

Es reicht also $L(p^k)$ zu betrachten:

$$L(p^k) := \sum_{d|p^k} \mu(d)\lambda(d) = 1 + (-1)(-1) + 0 = 2 = 2^{w(p^k)} \qquad \text{für } k \geq 1.$$

Daraus folgt die Behauptung. □

Alternative Lösung: Sei $n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$. (Kanonische Zerlegung)

$\Rightarrow$ rechte Seite $= 2^{\omega(n)} = 2^k$.

Linke Seite $= \sum_{d|n} \mu(d)(-1)^{\Omega(d)} = \sum_{d|p_1 \cdot \dots \cdot p_k} \mu(d)(-1)^{\Omega(d)}$

$= \sum_{d|p_1 \cdot \dots \cdot p_k} (-1)^{\Omega(d)}(-1)^{\Omega(d)} = \sum_{d|p_1 \cdot \dots \cdot p_k} 1 = \binom{k}{1} + \binom{k}{2} + \dots + \binom{k}{k}$

$= \sum_{i=1}^{k} \binom{k}{i} 1^i \cdot 1^{k-i} = (1+1)^k = 2^k =$ rechte Seite. $\square$

Aufgabe 8

Für $n > 1$ sei $A_n := 3^n - 2$. Zeige mit dem quadratischen Reziprozitätsgesetz für das Jacobi-Symbol:

$$\left(\frac{3}{A_n}\right) = 1 \Leftrightarrow n \text{ ungerade.}$$

Lösung:

Nach 3.14.(7) gilt:

$\left(\frac{3}{A_n}\right)\left(\frac{A_n}{3}\right) = (-1)^{\frac{A_n-1}{2}\cdot\frac{3-1}{2}} = (-1)^{\frac{3^n-3}{2}}$.

$\left(\frac{A_n}{3}\right) = \left(\frac{-2}{3}\right) = \left(\frac{1}{3}\right) = 1 \Rightarrow \left(\frac{3}{A_n}\right) = (-1)^{\frac{3^n-3}{2}} = \begin{cases} 1, & \text{falls } 4 \mid 3^n - 3 \\ -1, & \text{falls } 4 \nmid 3^n - 3 \end{cases}$

n gerade $\Rightarrow 3^n \equiv 1\ (4)$ (denn Potenzen von ungeraden Zahlen sind ungerade und $(2n+1)^2 \equiv 1\ (4)$)

$\Rightarrow 3^n - 3 \equiv 2\ (4) \Rightarrow \left(\frac{3}{A_n}\right) = -1$.

n ungerade $\Rightarrow 3^{n-1} \cdot 3 \equiv 3\ (4) \Rightarrow 3^n - 3 \equiv 0\ (4) \Rightarrow \left(\frac{3}{A_n}\right) = 1$. $\square$

Alternative Lösung:

Es gilt $\left(\frac{3}{A_n}\right) = \left(\frac{A_n}{3}\right)(-1)^{\frac{A_n-1}{2}\cdot\frac{3-1}{2}} = (-1)^{\frac{3^n-3}{2}}$, da $\left(\frac{A_n}{3}\right) = \left(\frac{-2}{3}\right) = \left(\frac{1}{3}\right) = 1$.

Also gilt: $\left(\frac{3}{A_n}\right) = 1 \Leftrightarrow (-1)^{\frac{3^n-3}{2}} = 1 \Leftrightarrow 3^n \equiv 3\ (4) \Leftrightarrow n$ ungerade, da

$3^{2k} \equiv 9^k \equiv 1\ (4)$ und $3^{2k+1} \equiv 9^k \cdot 3 \equiv 3\ (4)$. $\square$