Lösungen der Nachklausur in Elementarer Zahlentheorie, SoSe 2007

Aufgabe 1

Sei $n > 1$ und für alle Primzahlen $p \leq \sqrt[3]{n}$ gelte $p \nmid n$. Zeige durch Widerspruch, dass dann n entweder eine Primzahl oder das Produkt zweier Primzahlen ist.

Lösung:

Wir nehmen an n, enthalte mindestens drei Primfaktoren $p_1 < p_2 < p_3$. Dann gilt $p_1 | n$ und $p_1 = \sqrt[3]{p_1^3} \leq \sqrt[3]{n}$. Dies steht im Widerspruch dazu, dass $p_1 \nmid n$ für $p_1 \leq \sqrt[3]{n}$ gelten sollte. Folglich ist n eine Primzahl oder das Produkt zweier (nicht notwendigerweise verschiedener) Primzahlen

□

Aufgabe 2

Bestimme alle Lösungen der Kongruenz

$$x^3 + 15x + 9 \equiv 0 \ (63).$$

Lösung:

Sei $f(x) := x^3 + 15x + 9$. $\quad 63 = 7 \cdot 9$.

- Bestimmen der Lösungen mod 7 durch Ausprobieren:

  $f(x) \equiv x^3 + x + 2 \ (7)$. Lösungen mod 7 sind $x \equiv 4 \ (7)$ und $x \equiv 6 \ (7)$.

- Bestimmen der Lösungen mod 9 durch Ausprobieren:

  $f(x) \equiv x^3 + 6x \ (9)$. Lösungen mod 9 sind $x \equiv 0 \ (9)$, $x \equiv 3 \ (9)$ und $x \equiv 6 \ (9)$.

- Bestimmen der Lösungen mod 63 durch den chinesischen Restsatz:

  Es müssen die folgenden Kongruenzensysteme gelöst werden:

$$x \equiv 4 \ (7) \ \wedge \ x \equiv 0 \ (9) \tag{1}$$

$$x \equiv 4 \ (7) \ \wedge \ x \equiv 3 \ (9) \tag{2}$$

$$x \equiv 4 \ (7) \ \wedge \ x \equiv 6 \ (9) \tag{3}$$

$$x \equiv 6 \ (7) \ \wedge \ x \equiv 0 \ (9) \tag{4}$$

$$x \equiv 6 \ (7) \ \wedge \ x \equiv 3 \ (9) \tag{5}$$

$$x \equiv 6 \ (7) \ \wedge \ x \equiv 6 \ (9) \tag{6}$$

  Es ist $m = m_1 \cdot m_2 = 7 \cdot 9$ und $M_1 = \frac{m}{m_1} = 9, \quad M_2 = \frac{m}{m_2} = 7$.
  $M_i M_i^* \equiv 1 \ (m_i) \Rightarrow 9 \ M_1^* \equiv 1 \ (7) \ \Leftrightarrow \ 2 \ M_1^* \equiv 1 \ (7) \ \Rightarrow \ M_1^* = 4.$
  $7 \ M_2^* \equiv 1 \ (9) \ \Rightarrow \ M_2^* = 4.$

$$\Rightarrow x \equiv M_1 \ M_1^* x_1 + M_2 \ M_2^* x_2 \ (63) \ \Leftrightarrow \ x \equiv 36x_1 + 28x_2 \ (63)$$

Zu (1): $x_1 = 4, \quad x_2 = 0$
$\Rightarrow x \equiv 36 \cdot 4 + 28 \cdot 0 \equiv 18 \ (63)$.

Zu (2): $x_1 = 4, \quad x_2 = 3$
$\Rightarrow x \equiv 36 \cdot 4 + 28 \cdot 3 \equiv 39 \ (63)$.

Zu (3): $x_1 = 4, \quad x_2 = 6$
$\Rightarrow x \equiv 36 \cdot 4 + 28 \cdot 6 \equiv 60 \ (63)$.

Zu (4): $x_1 = 6, \quad x_2 = 0$
$\Rightarrow x \equiv 36 \cdot 6 + 28 \cdot 0 \equiv 27 \ (63)$.

Zu (5): $x_1 = 6, \quad x_2 = 3$
$\Rightarrow x \equiv 36 \cdot 6 + 28 \cdot 3 \equiv 48 \ (63)$.

Zu (6): $x_1 = 6, \quad x_2 = 6$
$\Rightarrow x \equiv 6 \ (63)$.

$\Rightarrow x \equiv 18, \ 39, \ 60, \ 27, \ 48, \ 6 \ (63)$ sind alle Lösungen modulo 63.

□

Aufgabe 3

Zeige: Falls $na \equiv nb \ (m_i)$ für $i = 1, 2$, gilt:

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

Lösung:

Aus $na \equiv nb \ (m_i)$ für $i = 1, 2$ folgt nach 2.1.(6):
$na \equiv nb \ ([m_1, m_2]) \overset{2.1.(5)}{\Longrightarrow} a \equiv b \left(\frac{[m_1, m_2]}{(n, [m_1, m_2])} \right)$ □

Aufgabe 4

Zeige:
Ist $2^k - 3$ prim, so genügt $n = 2^{k-1}(2^k - 3)$ der Gleichung $\sigma(n) = 2n + 2$.

Lösung:

Für $k \geq 2$ und $2^k - 3$ prim, ist $(2^{k-1}, 2^k - 3) = 1$ und wir können mit der Multiplikativität von σ und der geometrischen Summenformel schließen:

$$\sigma((2^{k-1}) \cdot (2^k - 3)) = \sigma(2^{k-1}) \cdot \sigma(2^k - 3) = (2^0 + 2^1 + 2^2 + ... + 2^{k-1}) \cdot ((2^k - 3) + 1)$$

$$= (2^k - 1) \cdot (2^k - 2) = 2^{2k} - 3 \cdot 2^k + 2 = 2((2^{k-1}) \cdot (2^k - 3)) + 2 = 2n + 2$$

□

Aufgabe 5

Für $m \in \mathbb{N}$ und $x, y \in \mathbb{Z}$ gelte $xy \equiv 1(m)$. Zeige:

$$\mathrm{ord}_m(x) = \mathrm{ord}_m(y).$$

Lösung:

$\mathrm{ord}_m(x)$ und $\mathrm{ord}_m(y)$ sind definiert, da x und y bezüglich der Multiplikation invers zueinander sind. Es sind genau die Elemente mod m invertierbar, die zu m teilerfremd sind. Also gilt $(x, m) = (y, m) = 1$.

Aus $xy \equiv 1(m)$ folgt $(xy)^i \equiv x^i y^i \equiv 1^i \equiv 1(m)$ für alle $i \in \mathbb{N}$.

Sei $\mathrm{ord}_m(x) =: k$ und $\mathrm{ord}_m(y) =: l$. Dann gilt $x^k y^k \equiv y^k \equiv 1(m)$, also $l \leq k$, und $x^l y^l \equiv x^l \equiv 1(m)$, also $k \leq l$. □

Aufgabe 6

Zeige:
Falls $\omega(n) \cdot \mu^2(n) = 3$, so ist $\dfrac{\sigma(n) + \varphi(n)}{2} - n$ die Summe dreier Primzahlen.

Lösung:

$\omega(n)\mu^2(n) = 3 \Longrightarrow \mu^2(n) = 1$ und $\omega(n) = 3$

n ist also quadratfrei und hat drei Primteiler, d.h. $n = p_1 p_2 p_3$. Dann ist

$\sigma(n) = 1 + p_1 + p_2 + p_3 + p_1p_2 + p_1p_3 + p_2p_3 + p_1p_2p_3$

$\varphi(n) = (p_1 - 1)(p_2 - 1)(p_3 - 1) = p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3 + p_1 + p_2 + p_3 - 1$

Damit ergibt sich: $\frac{\sigma(n)+\varphi(n)}{2} - n = p_1 + p_2 + p_3$

□

Aufgabe 7

Zeige, dass für alle $n \in \mathbb{N}$ gilt:

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

Lösung:

Die zahlentheoretischen Funktionen 2^ω und 1 sind multiplikativ und damit auch ihr Faltprodukt $2^\omega * 1$.

Für $(n, m)) = 1$ gilt: $d((nm)^2) = d(n^2m^2) = d(n^2)d(m^2)$ wegen der Multiplikativität von d. Also genügt es, die Identität auf Primpotezen zu überprüfen:

$(2^\omega * 1)(p^a) = 2^{\omega(1)} + 2^{\omega(p^1)} + ... + 2^{\omega(p^a)} = 1 + \sum_{j=1}^{a} 2 = 2a + 1 = d(p^{2a})$

□

Aufgabe 8

Sei $n > 1$ ungerade und $A_n := 6^n - 1$. Zeige mithilfe des quadratischen Reziprozitätsgesetzes für das Jacobi-Symbol, dass stets gilt:

$$\left(\frac{7}{A_n}\right) = 1.$$

Lösung:

Nach 3.14.(7) gilt:

$\left(\frac{7}{A_n}\right)\left(\frac{A_n}{7}\right) = (-1)^{\frac{A_n-1}{2}\cdot\frac{7-1}{2}} = (-1)^{\frac{6^n-2}{2}}$.

$\left(\frac{A_n}{7}\right) = \left(\frac{6^n-1}{7}\right) = \left(\frac{(-1)^n-1}{7}\right) = \left(\frac{-2}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{2}{7}\right) = -1$

$\Rightarrow \left(\frac{7}{A_n}\right) = (-1)(-1)^{\frac{6^n-2}{2}} = \begin{cases} 1, & \text{falls } 6^n - 2 \equiv 2 \ (4) \\ -1, & \text{falls } 6^n - 2 \equiv 0 \ (4) \end{cases}$

Für $n \geq 2$ ist $6^n - 2$ immer $\equiv 2$ (4). Also $\left(\frac{7}{A_n}\right) = 1$. □