Diskrete Mathematik - Übungen SW09

David Jäggli

22. April 2023

Inhaltsverzeichnis

1 Einführung in die Zahlentheorie

I.)
$n \geq 2$ und $n \in \mathbb{N}$

a) $n \mod n = 0$ dann muss $(n+1) \mod n = 1$
b) n^2 ist immer ein Vielfaches von n, heisst $n^2 \mod n = 0$
c) $(3n+6) \mod n = 3n \mod n + 6 \mod n = 6 \mod n$
d) $4n-1 \mod n = (4n \mod n) + (-1 \mod n) = -1 \mod n = n-1 \mod n = n-1$
e) $(n^2+n) \mod n = 0$
f) $(n^3+2n^2+4) \mod n = 4 \mod n$
g) $((2n+2)(n+1)) \mod n = (2n^2+4n+2) \mod n = 2 \mod n$
h) $n! \mod n = n \cdot (n-1)! \mod n = 0$

Korrektur:
g) $2 \mod n = \begin{cases} 0 & \text{für } n = 2 \\ 2 & \text{für } n > 2 \end{cases}$

II.)
$ggT(587, 392) =$

$$\begin{aligned} 587 &= 1 \cdot 392 + 195 \\ 392 &= 2 \cdot 195 + 2 \\ 195 &= 97 \cdot 2 + 1 \\ 97 &= 97 \cdot 1 + 0 \end{aligned}$$

$ggT(587, 392) = 1$

erweiterter euklidischer Algorithmus

$$\begin{aligned} 1 &= 195 - 97 \cdot 2 \\ &= 195 - 97 \cdot (392 - 2 \cdot 195) = 195 \cdot 195 - 97 \cdot 392 \\ &= 195 \cdot (587 - 392) - 97 \cdot 392 \\ &= 195 \cdot 587 - 195 \cdot 392 - 97 \cdot 392 \\ &= 195 \cdot 587 - 212 \cdot 392 \end{aligned}$$

Daraus folgt

$$\begin{aligned} 1 &\equiv 195 \cdot 587 - 292 \cdot 392 \pmod{587} \\ &\equiv (587 - 292) \cdot 392 \pmod{587} \\ &\equiv 295 \cdot 392 \pmod{587} \end{aligned}$$

III.)
Bestimme alle Lösungen von den Kongruenzen:

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 4 \mod 11 \end{aligned}$$

Obvious:

$$\begin{aligned} m = m_1 \cdot m_2 \cdot m_3 \cdot m_4 &= 330 \\ M_1 = \frac{m}{m_1} &= 165 \\ M_2 = \frac{m}{m_2} &= 110 \\ M_3 = \frac{m}{m_3} &= 66 \\ M_4 = \frac{m}{m_4} &= 30 \end{aligned}$$

Für alle $i (1 \leq i \leq 4)$ muss $M_i \cdot y_i$ berechnet werden.

i_1:

$$165 = 2 \cdot 82 + 1$$

$$y_1 = 1$$

i_2:

$$110 = 3 \cdot 36 + 2$$

$$y_2 = 2$$

i_3:

$$66 = 2 \cdot 82 + 1$$

$$y_3 = 1$$

i_4:

$$
\begin{aligned}
30 &= 11 \cdot 2 + 8 \\
11 &= 1 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
\\
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (8 - 2 \cdot 3) \\
&= 3 \cdot 3 - 8 \\
&= 3 \cdot (11 - 8) - 8 \\
&= 3 \cdot 11 - 4(30 - 2 \cdot 11) \\
&= 11 \cdot 11 - 4 \cdot 30 \\
\\
y_4 &= -4 = 7
\end{aligned}
$$

Nach x auflösen:

$$
\begin{aligned}
x &\equiv \sum_{i=1}^{4} r_i \cdot M_i \cdot y_1 \pmod{m} \\
&\equiv 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 + 4 \cdot 30 \cdot 7 \pmod{330)} \\
&\equiv 1643 \pmod{330} \\
&\equiv 323
\end{aligned}
$$

IV.)
$12! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$
$12! = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2^3 \cdot 3^2 \cdot 2 \cdot 5 \cdot 11 \cdot 2^2 \cdot 3$
$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$

$\phi(12!) = 2^9(2-1) \cdot 3^4(3-1) \cdot 5(5-1) \cdot (7-1) \cdot (11-1)$
$\phi(12!) = 2^9 \cdot 3^4 \cdot 2 \cdot 6 \cdot 4 \cdot 5 \cdot 10$
$\phi(12!) = 2^9 \cdot 3^4 \cdot 2 \cdot 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 5$
$\phi(12!) = 2^{14} \cdot 3^5 \cdot 5^2$
$\phi(12!) = 99532800$