Diskrete Strukturen Nachbereitungsaufgabe 5

Khmelyk Oleh

2023

(a) Berechnen Sie $2^{41}(mod 43)$.

Alle alle Vergleiche sind modulo 43.
$2^{41} \mod 43 \equiv 2 \cdot 2^{40} \equiv 2 \cdot 32^8 \equiv 2 \cdot (-11)^8 \equiv 2 \cdot 11^8 \equiv 2 \cdot 121^4 \equiv 2 \cdot (-8)^4 \equiv 2 \cdot 8^4 \equiv 2 \cdot 64^2 \equiv 2 \cdot 21^2 = 2 \cdot 441 \equiv 2 \cdot (430 + 11) \equiv 2 \cdot 11 \equiv 22 \equiv -21$

(b) Berechnen Sie mit dem erweiterten euklidischen Algorithmus $ggT(m, n)$ fuer r die Zahlenpaare

$$(i) n = 51, m = 187 \ (ii) n = 115, m = 42$$

und geben Sie jeweils $a, b \in \mathbb{Z}$ mit $ggT(m, n) = a \cdot n + b \cdot m$ an.

(i)$187 = 51 \cdot 3 + 34$
$51 = 34 \cdot 1 + 17$
$34 = 17 \cdot 2 + 0 \Rightarrow ggT(187, 51) = 17$

$17 = 34 - 17 = 34 - (51 - 34) = -51 + 2 \cdot 34 = -51 + 2(187 - 51 \cdot 3) = 2 \cdot 187 - 7 \cdot 51$

(ii)$115 = 42 \cdot 2 + 31$
$42 = 31 + 11$
$31 = 11 \cdot 2 + 9$
$11 = 9 + 2$
$9 = 2 \cdot 4 + 1$
$2 = 2 \cdot 1 + 0 \Rightarrow ggT(115, 42) = 1$

$1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (11 - 9) = -4 \cdot 11 + 5 \cdot 9 = -4 \cdot 11 + 5(31 - 11 \cdot 2) = 5 \cdot 31 - 14 \cdot 11 = 5 \cdot 31 - 14 \cdot (42 - 31) = -14 \cdot 42 + 19 \cdot 31 = -14 \cdot 42 + 19(115 - 42 \cdot 2) = 19 \cdot 115 - 52 \cdot 42$