Diskrete Strukturen Nachbereitungsaufgabe 7

Khmelyk Oleh

2023

(a) Geben Sie alle Elemente der Gruppe $(\mathbb{Z}_{10}^*;\cdot)$ an. Geben Sie eine andere Gruppe mit 4 Elementen an zu der $(\mathbb{Z}_{10}^*;\cdot)$ isomorph ist und geben Sie alle Isomorphismen zwischen den beiden Gruppen (ohne Begründung) an. Hinweis: Ü4

$(\mathbb{Z}_{10}^*;\cdot) = \{1,3,7,9\}$
Verknuepfungstafel:

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Z.B. $(\mathbb{Z}_4;+)$ ist isomorph zu $(\mathbb{Z}_{10}^*;\cdot)$,
Verknuepfungstafel:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

wir koenen diese Isomorphismen dazwishen geben:
$f : (\mathbb{Z}_{10}^*;\cdot) \to (\mathbb{Z}_4;+) : f(1) = 0; f(3) = 1; f(7) = 3; f(9) = 2$
$g : (\mathbb{Z}_4;+) \to (\mathbb{Z}_{10}^*;\cdot) : g(0) = 1; f(1) = 3; f(2) = 9; f(3) = 7$

(b) Hat die Gruppe $(\mathbb{Z}_{19}^*;\cdot)$ Erzeuger? Begründen Sie Ihre Antwort! Wenn ja, so bestimmen Sie die Anzahl der Erzeuger dieser Gruppe. Zeigen Sie, dass 3 eine Primitivwurzel in $(\mathbb{Z}_{19}^*;\cdot)$ ist. Nutzen Sie dies, um alle $x \in \mathbb{Z}_{19}$ zu finden, die $5^{42} \cdot x \equiv 10^3 \cdot 7^{-2} (\text{mod} 19)$ erfüllen.

19 - Primzahl $\Rightarrow$ hat $(\mathbb{Z}_{19}^*;\cdot) : \varphi(\varphi(19)) = \varphi(18) = 1 \cdot 3 \cdot 2 = 6$
Zu zeigen: 3 eine Primitivwurzel in $(\mathbb{Z}_{19}^*;\cdot)$:
Mod 19:
$3^0 = 1; 3 = 3; 3^2 = 9; 3^3 = 8; 3^4 = 5; 3^5 = 15; 3^6 = 7; 3^7 = 2; 3^8 = 6; 3^9 = 18; 3^{10} = 16; 3^{11} = 10; 3^{12} = 11; 3^{13} = 14; 3^{14} = 4; 3^{15} = 12; 3^{16} = 17; 3^{17} = 13; 3^{18} = 1;$
Wir haben alle elemente aus $(\mathbb{Z}_{19}^*;\cdot)$ getrofen $\Rightarrow < 3 >= (\mathbb{Z}_{19}^*;\cdot)$

$5^{43} \cdot x \equiv 10^3 \cdot 7^{-2} \bmod 19$
$10^3 \cdot 7^{-2} \equiv 3^{33} \cdot 3^{-6} = 3^{27} = 3^{18+9} \equiv 3^9 \equiv 18 \bmod 19$
$5^43 \equiv 3^{4 \cdot 43} = 3^{172} \equiv 3^{-8} \equiv 3^{10} \equiv 16 \equiv -3$

$-3x \equiv 18 \bmod 19 \Rightarrow x \equiv -6 \equiv 13 \bmod 19$