

ÖVNING 10 - DISKRET MATEMATIK 030507

HANNES REIJNER

22.3.2 Visa att den multiplikativa gruppen till $\mathbf{Z}_{23}$ är cyklisk genom att hitta en generator.

lösning. Vi börjar med att notera att antalet inverterbara element i $\mathbf{Z}_{23}$ är $\phi(23) = 22$ eftersom 23 är ett primtal. Vi har således att den multiplikativa gruppen $U(\mathbf{Z}_{23})$ innehåller alla element utom 0 vilket kan skrivas som $U(\mathbf{Z}_{23}) = \{\mathbf{Z}_{23} \setminus 0\}$. Vi räknar modulo 23 och testar med 2 eftersom det då blir lätt att räkna. Vi ser att $\langle 2 \rangle = \{2, 4, 8, 16, 32 = 9, 18, 36 = 13, 26 = 3, 6, 12, 24 = 1\}$. Vi testar nu med elementet som inte tillhör $\langle 2 \rangle$ och väljer återigen ett litet tal för att underlätta räknandet. Det minsta talet som inte tillhör $\langle 2 \rangle$ är 5 (åtminstone minst betraktat som ett element i $\mathbf{Z}$): $\langle 5 \rangle = \{5, 25 = 2, 10, 50 = 4, 20 = -3, -15 = 8, 40 = -6, -30 = -7, -35 = 11, 55 = 9, 45 = -1, -5, -25 = -2 = 21, -10 = 13, -50 = -4 = 19, -20 = 3, 15 = -8, -40 = 6, 30 = 7, 35 = 12 = -11, -55 = -9, -45 = 1\} = U(\mathbf{Z}_{23})$. Vi har därmed att $U(\mathbf{Z}_{23})$ är en cyklisk grupp och att 5 är en generator. Detta kan också lösas m.h.a sats 20.8.3 i boken såsom vi gjorde på övningen.

E-mail address: hannes@math.kth.se

URL: www.math.kth.se/~hannes