

Matematiska Institutionen  
KTH

**Lösning till lappskrivning nr 5, variant B, på kursen Diskret matematik, 5B1118, för media1, fredagen den 13 maj, 2005.**

1. Låt  $G$  beteckna gruppen  $G = \langle Z_{17} \setminus \{0\}, \cdot \rangle$ , dvs gruppen bestående av elementen skilda från noll i ringen  $Z_{17}$  med operationen multiplikation modulo 17. Bestäm en delgrupp  $H$  till  $G$  med två element och ange tre olika sidoklasser till  $H$  i  $G$ . Hur många olika sidoklasser till  $H$  finns det totalt i  $G$ . (Två sidoklasser räknas som lika om de består av precis samma element.)

**Lösning** Mängden  $H = \{1, -1\} = \{1, 16\}$  bildar en delgrupp med två element. Den är själv en sidoklass,  $H = H1$ . Två andra sidoklasser är  $H2 = \{2, -2\} = \{2, 15\}$  och  $H3 = \{3, -3\} = \{3, 14\}$

2. De inverterbara elementen i ringen  $Z_{18}$  bildar en grupp  $G$  med sex element. Visa att  $G$  är cyklisk. (Påminnelse: Ett element  $a$  i en ring  $Z_n$  är inverterbart precis då  $\text{sgd}(a, n) = 1$ .)

**Lösning** De inverterbara elementen är 1, 5, 7, 11, 13, 17 eftersom det är precis de elementen som är relativt prima till 18. Vi undersöker nu vilka delgrupper som dessa element genererar:

$$\langle 5 \rangle = \{5, 5^2 = 7, 5^3 = 17, 5^4 = 13, 5^5 = 11, 5^6 = 1\}.$$

Detta var ju alla element i den givna gruppen som alltså är cyklisk. Uppgiften är löst och vi behöver inte studera något av de resterande elementen.

**Alternativ lösning** Elementet 5 ligger i givna gruppen eftersom  $\text{sgd}(5, 18) = 1$ . Den givna gruppen har sex element så ordningen av 5 delar 6. Men eftersom  $5^2 = 7 \neq 1$  och  $5^3 = 17 \neq 1$  så är enda möjligheten att 5:s ordning är 6. Detta element är då en generator för hela gruppen som då är cyklisk.

3. Låt  $G$  vara en cyklisk grupp med 27 element och antag att  $G$  genereras av elementet  $g$ . Ange på lämpligt sätt de element i denna grupp som har ordning tre. Visa också, t ex med hjälp av känd sats, att gruppen saknar element av ordning sex.

**Lösning** Vi vet att ordningen av ett element måste dela antalet element i gruppen. Eftersom 6 inte delar 27 så finns inget element av ordning 6 i gruppen.

Elementen  $H = \{g^9, g^{18}, g^{27} = e\}$  bildar en grupp med 3 element och alla dessa element utom  $e$  har ordning 3. Om  $g^i$  skulle ha ordning 9 så skulle  $g^{3i} = g^{k \cdot 27}$  dvs  $3i = 27k$ . Detta ger att 9 delar talet  $i$ . De enda möjliga elementen är de i gruppen  $H$ .