

Lösning till DM 3.43

Uppgift

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Figur 1: Multiplikationstabeller för $\mathbb{Z}_6$ och $\mathbb{Z}_7$

I "normal" räkning finns den viktiga räkneregeln nollfaktorlagen. Den säger att om en produkt är noll så måste någon av faktorerna vara noll; det går inte att multiplicera fram noll på annat sätt. Tittar man i multiplikationstabellerna i Figur 1 ser man att detta inte är givet i modulär aritmetik.

- (a) I tabellen för $\mathbb{Z}_6$ finns ett antal nolldelare, det vill säga tal andra än noll som kan vara faktorer i noll. Förklara varför det alltid finns nolldelare om man räknar modulo ett sammansatt tal.
- (b) I tabellen för $\mathbb{Z}_7$ finns däremot bara nollor i nollans rad och kolumn. Förklara varför det inte kan finnas nolldelare då man räknar modulo ett primtal.

Lösning

- (a) Antag att $n \in \mathbb{N}$ är ett sammansatt tal, så att $n = ab$ för några $a, b \in \mathbb{N}$ som uppfyller $a, b > 1$. Vi hävdar att a och b är nolldelare i $\mathbb{Z}_n$.

Eftersom $n = ab$ och $a, b > 1$, följer det att $n > a$, och eftersom $a \neq 0$ kan därför inte a vara delbart med n . Med andra ord innebär detta att $a \not\equiv 0 \pmod{n}$, det vill säga att $a \neq 0$ i $\mathbb{Z}_n$. På samma sätt fås att $b \neq 0$ i $\mathbb{Z}_n$. Men n är förstås en multipel av sig själv, så $n = 0$ i $\mathbb{Z}_n$. Det innebär att det i $\mathbb{Z}_n$ gäller att $ab = 0$, även om $a \neq 0$ och $b \neq 0$, alltså att a och b är nolldelare i $\mathbb{Z}_n$.

- (b) Låt $p \in \mathbb{N}$ vara ett primtal. Vi hävdar att det inte finns några nolldelare i $\mathbb{Z}_p$, och kommer att visa detta med ett motsägelsebevis.

Antag därför att a är en nolldelare i $\mathbb{Z}_p$. Detta betyder att det finns ett heltal b sådant att $ab = 0$ gäller i $\mathbb{Z}_p$, men $a \neq 0$ och $b \neq 0$ gäller i $\mathbb{Z}_p$.

Att $ab = 0$ i $\mathbb{Z}_p$ betyder per definition att ab är en multipel av p , alltså att $p \mid ab$. Eftersom p är ett primtal betyder detta att antingen $p \mid a$ eller $p \mid b$. Men detta skulle betyda att antingen $a = 0$ eller $b = 0$ gäller i $\mathbb{Z}_p$, vilket är en motsägelse.