Extra uppgifter kapitel 3

November 24, 2023

Övning 1

Skriv ned additionstabellen och multiplikationstabellen för $\mathbb{Z}/(3)$ och $\mathbb{Z}/(4)$. Tänka själva och jämför sedan era svar med exempel 3.4.3 och 3.4.4. Se Övning 3.3 i kompendiet om du vill träna mer på detta.

Övning 2

I $\mathbb{Z}/(n)$ finns det alltid additiva inverser eftersom det är en ring. Hitta den additiva inversen till 4 modulo 8, dvs ett heltal k mellan 0 och 10 sådan att

$$4 +_8 k = 0.$$

Vi kallar ibland talet k för '-4 modulo 10' eller '$-_{10}4$'. Avgör också om 4 har någon multiplikativ invers modulo 8.

Övning 3

Para ihop alla element i $\mathbb{Z}/(7)$ med sin additiva invers och skriv ner dom.

Övning 4

Låt $-_n a$ betecka den additiva inversen till a modulo n. Att subtrahera a från b modulo n är att addera $-_n a$ till b, alltså

$$b -_n a = b + (-_n a).$$

Förenkla följande algebraiska uttryck för $n = 7$ och $n = 12$:

i) $4 \cdot_n 4 +_n 5$

ii) $4 \cdot_n 3 +_n 5$

iii) $4 \cdot_n 1 +_n 5$

iv) $5 \cdot_n 0 -_n 3$

v) $5 \cdot_n 1 -_n 3$

vi) $5 \cdot_n 6 -_n 3$

Se Övning 3.1 i kompendiet om du vill träna mer på detta.

Övning 5

Vad är

$$32589 \cdot_{8743587} 0 \quad \text{(skrivs alternativt som: } 32589 \cdot 0 \bmod 8743587\text{)}$$

och

$$98647 \cdot_{2347698245} 1 \quad \text{(skrivs alternativt som: } 98647 \cdot 1 \bmod 2347698245\text{)}$$

Övning 6

Är $(\mathbb{N}, +, \cdot)$ en ring? Här är $+$ och $\cdot$ vanliga plus och gånger. *Ledtråd: Ni måste kolla ifall alla räkneregler i Definition 3.3.1 är uppfyllda.*

Övning 7

Hitta den multiplikativa inversen till 4 modulo 7. Dvs hitta ett heltal k mellan 0 och 7 sådan att

$$4 \cdot_7 k = 1.$$

Vi kallar ibland talet k för '1/4 modulo 7' eller '4^{-1} modulo 7' trots att det inte är en fjärdedel i den vanliga bemeningen. Se övning 3.2 om du vill träna mer på detta (där ska du räkna ut alla par av multiplikativa inverser modulo 3, modulo 5 och modulo 7).

Övning 8

Se till att ha gjort uppgift 2 före denna. Läs delkapitel 3.4 och lista ut för vilka n som det gäller att alla nollskiljda tal har en multiplikativ invers.

Övning 9

När det är tydligt att vi jobbar med modulär aritmetik skriver vi potenser såsom med vanlig aritmetik

$$x^2 = x \cdot_n x, \qquad x^3 = x \cdot_n x \cdot_n x \qquad o.s.v.$$

När det är tydligt ifall vi jobbar på den vanliga tallinjen eller den modulära tallinjen så struntar vi i att skriva $+_n$ och $\cdot_n$ och skriver bara $+, \cdot$ som vanligt.

Beräkna möjliga värden av funktionen/polynomet

$$f\colon \mathbb{Z}/(4) \to \mathbb{Z}/(4) \tag{1}$$
$$x \mapsto x^2 + x + 1. \tag{2}$$

Detta är alltså funktionen som tar in ett tal x på tallinjen modulo 5 (0,1,2 eller 3) och spottar ut det tal du får om du adderar 1 med x och x^2 modulo 4.

Facit

Svar 1

Jämför sedan era svar med exempel 3.4.3 och 3.4.4.

Svar 2

När man räknar modulo 8 så är 4 sin egen additiva invers, alltså $4 = -_8 4$. Vi ser att 4 inte har någon multiplikativ invers modulo 8 eftersom det finns inget tal mellan 0 och 8 sådan att man får resultatet 1 efter multiplikation med 4 modulo 8, vilket kan ses i denna tabell:

- $1 \cdot_8 4 = 4$
- $2 \cdot_8 4 = 0$
- $3 \cdot_8 4 = 4$
- $4 \cdot_8 4 = 0$
- $5 \cdot_8 4 = 4$
- $6 \cdot_8 4 = 0$
- $7 \cdot_8 4 = 4$

Övning 3

- 0 är sin egen additiva invers.
- 1 och 6 är varandras additiva inverser modulo 7.
- 2 och 5 är varandras additiva inverser modulo 7.
- 3 och 4 är varandras additiva inverser modulo 7.

Svar 4

i) $4 \cdot_7 4 +_7 5 = (4 \cdot 4 + 5)\%7 = 21\%7 = 0$

ii) $4 \cdot_7 3 +_7 5 = (4 \cdot 3 + 5)\%7 = 17\%7 = 3$

iii) $4 \cdot_7 1 +_7 5 = (4 \cdot 1 + 5)\%7 = 9\%7 = 2$

iv) $5 \cdot_7 0 -_7 3 = (5 \cdot 0 - 3)\%7 = -3\%7 = 4$

v) $5 \cdot_7 1 -_7 3 = (5 \cdot 1 - 3)\%7 = 2\%7 = 2$

vi) $5 \cdot_7 6 -_7 3 = (5 \cdot 6 - 3)\%7 = 27\%7 = 6$

i) $4 \cdot_{12} 4 +_{12} 5 = (4 \cdot 4 + 5)\%12 = 21\%12 = 9$

ii) $4 \cdot_{12} 3 +_{12} 5 = (4 \cdot 3 + 5)\%12 = 17\%12 = 5$

iii) $4 \cdot_{12} 1 +_{12} 5 = (4 \cdot 1 + 5)\%12 = 9\%12 = 9$

iv) $5 \cdot_{12} 0 -_{12} 3 = (5 \cdot 0 - 3)\%12 = -3\%12 = 9$

v) $5 \cdot_{12} 1 -_{12} 3 = (5 \cdot 1 - 3)\%12 = 2\%12 = 2$

vi) $5 \cdot_{12} 6 -_{12} 3 = (5 \cdot 6 - 3)\%12 = 27\%12 = 3$

Svar 5

$$32589 \cdot_{8743587} 0 = 0 \text{ och } 98647 \cdot_{2347698245} 1 = 98647$$

Svar 6

Det är inte en ring eftersom det saknas additiva inverser (inga negativa tal är tillåtna). Det betyder att $(\mathbb{N}, +)$ inte är en grupp vilket är ett av villkoren för att trippletten $(\mathbb{N}, +, \cdot)$ skulle ha varit en ring.

Svar 7

Det är 2 som är den multiplikativa inversen till 4 modulo 7 per definition därför att

$$2 \cdot_7 4 = 1.$$

Svar 8

Det är om och endast om n är ett primtal som $\mathbb{Z}/(n)$ är en kropp enligt sats 3.4.6. Att vara en kropp betyder att mängden av nollskiljda element är en grupp med avseende på multiplikation (se definition 3.3.4). I en grupp har alla element inverser, alltså är sats 3.4.6. svaret på vår fråga.

Svar 9

Vi skriver nu $+$ och $\cdot$ istället för $+_4$ och $\cdot_4$ eftersom vi vet att vi jobbar modulo 4.

- $f(0) = 0^2 + 0 + 1 = 1$
- $f(1) = 1^2 + 1 + 1 = 3$
- $f(2) = 2^2 + 2 + 1 = 0 + 2 + 1 = 3$
- $f(3) = 3^2 + 3 + 1 = 1 + 3 + 1 = 1$