Projekt 8.1 Modulo-regning, restklassegrupperne og Fermats lille sætning

Vi anvender moduloregning og restklasser mange gange om dagen, nemlig når vi taler om tid, om hvad klokken er, om hvor lang tid der er til et eller andet, vi har aftalt, dvs. når vi udmåler tid med et ur. Når tiden udmåles i timer, regner vi modulo 24 (eller 12), og når tiden udmåles i minutter regner vi modulo 60. Vi siger ikke, at klokken er 80 minutter over 10, men at den er 20 minmutter over 11. Når klokken passerer midnat, tæller vi ikke videre på tallinjen med 25, 26 osv., men forfra – om natten er klokken 1, 2 osv. Siger vi, at vi går i seng KL 23, regner vi modulo 24, mens de som siger, at de går i seng KL 11, regner modulo 12. Regner man modulo 12, "identificerer" man altså 23 og 11.

Går man i seng KL 23 og sætter uret, så man kan sove i 8 timer, så står man ikke op kl. $23+8=31$, men kl. 7. Tallet 7 får vi matematisk, ved at trække 24 fra 31. I praksis tæller de fleste nok op til 24 (det var én time) og resten af de 8 timer, altså tallet 7 angiver så klokkeslettet, hvor vi står op. Også her "identificerer" vi altså 31 og 7. Men vi kan naturligvis ikke skrive: $31=7$. Derfor har man i matematik indført en særlig betegnelse for denne måde at identificerer tal på, nemlig ved at skrive:

$$31\,(\mathrm{mod}\,24)=7\,(\mathrm{mod}\,24)$$

"mod 24" læses *modulo 24*, og angiver, at vi trækker 24 fra tallet lige så mange gange vi kan, indtil vi har et tal mellem 0 og 24. Således gælder altså:

$$48\,(\mathrm{mod}\,24)=0\,(\mathrm{mod}\,24) \qquad \text{og} \qquad 245\,(\mathrm{mod}\,24)=5\,(\mathrm{mod}\,24)$$

Det sidste udtryk kan vi tolke således: Hvis klokken nu fx er 9, så er den om 245 timer $9+5=14$.
5 kan opfattes som *resten* vi får ved division af 245 med 24. Divisionen går jo ikke op, men giver 10 og altså 5 til rest.
Vi kunne også regne tilbage i tiden:

$$-20\,(\mathrm{mod}\,24)=4\,(\mathrm{mod}\,24)$$

Dette kan vi tolke således. Hvis klokken nu fx er 9, så var den for 20 timer siden $9+4=13$.

Tilsvarende gælder der:

$$80\,(\mathrm{mod}\,60)=20\,(\mathrm{mod}\,60) \qquad \text{og} \qquad 380\,(\mathrm{mod}\,365)=15\,(\mathrm{mod}\,365)$$

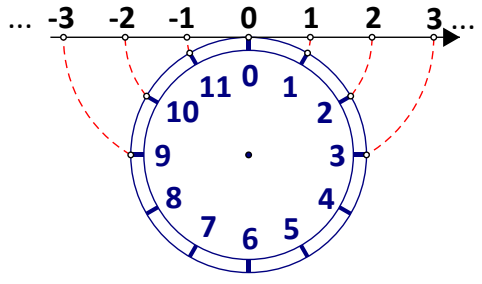
Prøv at give en fortolkning af disse to udtryk.

Regner vi modulo 24, så identificerer vi altså alle tallene:

$$\{\ldots,-44,-20,4,28,52,\ldots\}$$

Tilføj selv yderligere to negative og to positive tal.
En sådan mængde af tal kalder vi for en *restklasse modulo 24*. Vi siger også, at tallene i en sådan restklasse er *kongruente modulo 24*, og anvender symbolet $\equiv$ til at udtrykke dette. Vi skriver fx: $4\equiv 52\,(\mathrm{mod}\,24)$.

Øvelse 1.
a) Opskriv restklasen hørende til tallet 0, og restklassen hørende til tallet 10.
b) Hvor mange forskellige restklasser modulo 24 findes der?



I almindelighed kan man ved *restklasser modulo n*, hvor *n* er et naturligt tal, forestille sig, at man vikler en tallinje rundt om en cirkel, der har omkredsen *n*. Hver gang vi går *n* positioner frem på den omviklede tallinje rammer vi altså det samme punkt på cirklen.
Restklasserne repræsenteres af tallene {0, 1, 2, …, *n*-1}, der kaldes for *de principale rester* ved division med *n*.
På illustrationen ser man fx, at tallene -3 og 9 er i samme restklasse og altså er kongruente modulo 12.

Bemærkning. Vi regner kun med hele tal. Men princippet med restklasser kan udstrækkes til alle reelle tal. Et vigtigt eksempel er enhedscirklen, hvor vi regner modulo 2π, når vi løser trigonometriske ligninger.

Eksempel

$7 \equiv 12 \pmod 5$ $\quad$ $7 \equiv 122 \pmod 5$

$-3 \equiv 1 \pmod 4$ $\quad$ $-3 \equiv 17 \pmod 4$

Vi skriver ikke altid (mod *n*) efter tallet, hvis dette tal er den principale rest. I stedet tillader vi os for nemheds skyld at skrive eksempelvis $12 \pmod 5 = 2$. Her står, at den principale rest ved division af 12 med 5 er 2.

Øvelse 2

Bestem følgende:

a) $21 \pmod 3$ b) $558 \pmod{17}$ c) $5306509 \pmod{10}$ d) $-20 \pmod 3$ e) $123123123 \pmod 9$

Regning med restklasser

Vi vil nu gå over til en mere systematisk indføring i regning med restklasser, der er et centralt element i moderne talteori og dermed i kryptologi.

Definitioner: Begreber hørende til divisionsligningen

Mængden af hele tal (positive, negative og nul) betegnes $\mathbb{Z}$. At et tal *a* er et helt tal angives således:

$a \in \mathbb{Z}$, der læses "*a* tilhører mængden af hele tal, $\mathbb{Z}$".

Når vi har to vilkårlige hele tal, $a, b \in \mathbb{Z}$, kan vi dividere *a* op i *b* ved den metode, vi lærte i folkeskolen. Det giver et helt talt *q* som resultat og dertil en rest r. Resultatet skrives således:

$b = q \cdot a + r$, hvor $q \in \mathbb{Z}$, og $0 \le r < a$ (*)

Vi vil altid skrive resultatet således at resten r ligger i dette interval. Denne rest kaldes *den principale rest*. Opskrivningen af (*) kaldes *divisionsligningen*.

Hvis *a går op i b*, dvs. hvis resten er 0, siger vi at *a er divisor i b*, og vi skriver: $a \mid b$

Hvis *a ikke går op i b* skriver vi: $a \nmid b$

Tallene 1 og *b* går altid op i *b*, og de regnes sjældent med, når vi taler om divisorer. Hvis vi vil understrege dette taler vi om *ægte divisorer*.

Eksempel: Opskrivning af divisionsligninger

1) a = 5, b = 32: $32 = 6 \cdot 5 + 2$

2) a = 3, b = 16: $16 = 5 \cdot 3 + 1$

3) a = 3, b = -16: $-16 = -6 \cdot 3 + 2$

Bemærk, at kravet om $0 \le r < a$ giver en lidt anden divisionsligning for negative tal.

Eksempel: Divisorer I et tal

a) $6 \mid 216$ $\quad$ $37 \mid 2.954.524$ $\quad$ $113 \nmid 965.356\,113$

b) Du kan finde samtlige divisorer i et tal ved hjælp af dit værktøjsprogram. Det kan eksempelvis se således ud:

$\text{factor}(30) = 2 \cdot 3 \cdot 5$ og $\text{factor}(216) = 2^3 \cdot 3^3$

Opskrivninger af typen:

$30 = 2 \cdot 3 \cdot 5$ og $216 = 2^3 \cdot 3^3$

kaldes for en *faktorisering i primfaktorer*. På grund af primtallenes natur kan vi ikke faktorisere videre. Omvendt kan vi ud af faktoriseringen se, hvilke tal der er divisorer. Eksempelvis kan vi se, at tallene:

$2, 3, 5, 6 (= 2 \cdot 3), 10 (= 2 \cdot 5)$ og $15 (= 3 \cdot 5)$

er divisorer i 30.

Øvelse 3
Faktoriser tallene 2310 og 2 954 524 og opskriv samtlige ægte divisorer.

Sætning 1
For vilkårlige tal $a, b \in \square$ er divisionsligningen éntydig.

Bevis
Antag at vi har to opskrivninger af divisionsligningen:

$$b = q_1 \cdot a + r_1$$
$$b = q_2 \cdot a + r_2$$

og lad os sige $r_2 \geq r_1$
Træk fra og få:

$$(q_1 - q_2) \cdot a = r_2 - r_1$$

Da $0 \leq r_1 < a$, $0 \leq r_2 < a$ og $r_2 \geq r_1$, vil_

$$0 \leq r_2 - r_1 < a$$

Derfor må der gælde:

$(q_1 - q_2) = 0$, dvs. at $q_1 = q_2$

Indsæt nu dette i de to første ligninger:

$$b = q_1 \cdot a + r_1$$
$$b = q_1 \cdot a + r_2$$

hvoraf vi let ser, at også $r_1 = r_2$
Hermed er sætningen vist.

Undersøgelsen af, om to tal er kongruente modulo et tal *n* kan udføres på en lidt anden måde, end ved at opskrive divisionsligningen, nemlig ved at undersøge, om forskellen på de to tal er delelig med *n*. Dette er indholdet i næste sætning. Man kan ofte se denne egenskab anvendt som definition på kongruens.

Sætning 2
1) Hvis $a \pmod n = b \pmod n$, så gælder: $n \mid (a - b)$
2) Hvis $n \mid (a - b)$, så gælder: $a \pmod n = b \pmod n$

Bevis for punkt 1
Opskriv divisionsligningerne for *a* og *b*:

$$a = q_1 \cdot n + r$$
$$b = q_2 \cdot n + r$$

Vi trækker fra og får:

$$a - b = (q_1 - q_2) \cdot n$$

Men her står jo, at *n* går op i tallet $(a - b)$: $n \mid (a - b)$

Bevis for punkt 2
Antag $n \mid (a - b)$. Dvs. der findes et tal *k*, så:

$$a - b = k \cdot n \qquad (*)$$

Opskriv divisionsligningen for *b*:

$$b = h \cdot n + r \qquad (**)$$

Læg nu de to ligninger (*) og (**) sammen:

$$a = (k + h) \cdot n + r \qquad (***)$$

Men her står jo i (***) og, at tallene *a* og *b* har samme rest ved division med *n*.
Hermed er sætning 2 bevist.

I øvelse 1 så vi, at der er 24 restklasser modulo 24, hvilket svarer til at sige, at der kan forekomme 24 forskellige (principale) rester, når vi dividerer tal, med 24. Restklasserne repræsenteres af de principale rester, så mængden af alle restklasser modulo 24 er:

$$\mathbb{Z}_{24} = \{0,1,2,3,4,\ldots,22,23\}$$

Tilsvarende har vi_

$$\mathbb{Z}_3 = \{0,1,2\} \qquad \mathbb{Z}_3 = \{0,1,2,3,4\} \qquad \mathbb{Z}_6 = \{0,1,2,3,4,5\}$$

og generelt:

Definitioner: Mængden $\mathbb{Z}_n$

Lad *n* være et positivt helt tal. Mængden af principale rester ved division med *n* betegnes:

$$\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$$

Et tal i $\mathbb{Z}_n$ opfattes som repræsentant for sin tilsvarende restklasse.

Hvis $a,b \in \mathbb{Z}_n$ definerer vi addition af restklasser således:

$$a+b = (a+b)(\mathrm{mod}\, n)$$

Sætning 3 Regning med restklasser

1) $(a+b)(\mathrm{mod}\, n) = (a(\mathrm{mod}\, n) + b(\mathrm{mod}\, n))(\mathrm{mod}\, n)$

2) $(a-b)(\mathrm{mod}\, n) = (a(\mathrm{mod}\, n) - b(\mathrm{mod}\, n))(\mathrm{mod}\, n)$

3) $(a\cdot b)(\mathrm{mod}\, n) = (a(\mathrm{mod}\, n) \cdot b(\mathrm{mod}\, n))(\mathrm{mod}\, n)$

Bevis

Alle beviser bygger blot på definitionen og anvendelsen af divisionsligningerne:

$a = q_1 \cdot n + r_1$, hvoraf specielt: $a(\mathrm{mod}\, n) = r_1$

$b = q_2 \cdot n + r_2$, hvoraf specielt: $b(\mathrm{mod}\, n) = r_2$

Når vi regner modulo *n* kan vi smide alle led, der indeholder faktoren *n* væk.

Punkt 1)

$$a+b = q_1 \cdot n + r_1 + q_2 \cdot n + r_2 = (q_1+q_2)\cdot n + (r_1+r_2)$$

Heraf får vi:

$(a+b)(\mathrm{mod}\, n) = (r_1+r_2)(\mathrm{mod}\, n)$ Udnyt definitionen på modulo

$(a+b)(\mathrm{mod}\, n) = (a(\mathrm{mod}\, n) + b(\mathrm{mod}\, n))(\mathrm{mod}\, n)$ Indsæt udtrykkene for r_1 og r_2

Punkt 2)

Overlades til læseren som en øvelse.

Punkt 3)

$$\begin{aligned} a\cdot b &= (q_1 \cdot n + r_1)\cdot(q_2 \cdot n + r_2) \\ &= q_1 \cdot q_2 \cdot n^2 + q_1 \cdot r_2 \cdot n + q_2 \cdot r_1 \cdot n + r_1 \cdot r_2 \\ &= (q_1 \cdot q_2 \cdot n + q_1 \cdot r_2 + q_2 \cdot r_1)\cdot n + r_1 \cdot r_2 \end{aligned}$$

Heraf får vi:

$(a\cdot b)(\mathrm{mod}\, n) = (r_1 \cdot r_2)(\mathrm{mod}\, n)$ Udnyt definitionen på modulo

$(a\cdot b)(\mathrm{mod}\, n) = (a(\mathrm{mod}\, n) \cdot b(\mathrm{mod}\, n))(\mathrm{mod}\, n)$ Indsæt udtrykkene for r_1 og r_2

Hermed er formlerne bevist.

Bemærkning. Når vi er nødt til at udføre en ekstra omgang modulo på højre side skyldes det, at summen eller produktet af de principale rester ofte vil falde udenfor $\square_n$.

Eksempel: Moduloregning med og uden matematisk værktøj
Kan man sin lille tabel, er det forholdsvis let at gennemføre simple modulo-udregninger som:

$$3457 \pmod 7 = 6 \pmod 7$$

Man foretager divisionen i hovedet og når frem til, at den sidste division er 7 op i 27. Det giver 3 med 6 som rest.
Man kan også regne lidt mere avanceret ved at inddrage de negative tal og udnytte moduloregnereglerne samt vores kendskab til den lille tabel (7 går op i 3500 og 7 går op i 49):

$$3457 \pmod 7 = \left(3457 - 3500\right) \pmod 7 = -43 \pmod 7 = \left(-43 + 49\right) \pmod 7 = 6 \pmod 7$$

Med en lommeregner uden modulofaciliteter kunne man udregne:

$$\frac{3457}{7} = 493.857$$

Det største hele tal i 7-tabellen, der er mindre end 3457 er derfor 493. Lommeregneren kan så give resten:

$$3497 - 493 \cdot 7 = 6$$

Øvelse 4
a) Bestem $\left(1! + 2! + 3! + 4! + \ldots + 100!\right) \left(\mathrm{mod}\, 12\right)$
b) Bestem $2^{50} \left(\mathrm{mod}\, 7\right)$

Øvelse 5
Vis ved at give et modeksempel, at vi *ikke* kan slutte:

$$a^2 \equiv b^2 \pmod n \Rightarrow a \equiv b \pmod n$$

Eksempel: Regler for, hvornår et helt tal går op i et andet helt tal
Før lommeregnernes tid lærte man en række regler, der skulle hjælpe til hurtige udregninger. Det var fx regler om, hvornår et tal går op i et andet tal. Det er let at indse, at
- 2 går op, hvis det går op i sidste ciffer (lige tal)
- 4 går op, hvis det går op i tallet bestemt af de sidste to cifre
- 5 går op, hvis tallet ender på 0 eller 5
- 10 går op, hvis tallet ender på 10.

Det er også let acceptere, at et tal som 6 går op, hvis tallets primfaktorer, henh. 2 og 3 begge går op.
Der er ingen let anvendelig regel for hvornår 7 går op.
Men der er simple regler for hvornår 3, 9 og 11 går op. Det kan man indse ved modulo-regning:
Det tal vi vil dividere op i skrives ud i titalsystemet således:

$$N = a_n \cdot 10^n + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

hvor N er tallet $N = a_n a_{n-1} \ldots a_2 a_1 a_0$
Eksempelvis kan vi skrive $3457 = 3 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10 + 7$
Når vi undersøger om et tal k går op, så reducerer vi modulo k.

Går 3 op i tallet *N*?
Vi anvender de tre regneregler:

$$N \left(\mathrm{mod}\, 3\right) = \left(a_n \cdot 10^n + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0\right) \left(\mathrm{mod}\, 3\right)$$

$$= \left(\left(a_n \cdot 10^n\right) \left(\mathrm{mod}\, 3\right) + \ldots + \left(a_2 \cdot 10^2\right) \left(\mathrm{mod}\, 3\right) + \left(a_1 \cdot 10\right) \left(\mathrm{mod}\, 3\right) + a_0 \left(\mathrm{mod}\, 3\right)\right) \left(\mathrm{mod}\, 3\right)$$

$$= \left(a_n \left(\mathrm{mod}\, 3\right) \cdot \left(10 \left(\mathrm{mod}\, 3\right)\right)^n + \ldots + a_2 \left(\mathrm{mod}\, 3\right) \cdot \left(10 \left(\mathrm{mod}\, 3\right)\right)^2 + a_1 \left(\mathrm{mod}\, 3\right) \cdot 10 \left(\mathrm{mod}\, 3\right) + a_0 \left(\mathrm{mod}\, 3\right)\right) \left(\mathrm{mod}\, 3\right)$$

Og nu kommer det smarte med tallet tre: $10 \pmod 3 = 1$. Dvs ovenstående bliver lig med:

$$\left(a_n \pmod 3 \cdot 1^n + \ldots + a_2 \pmod 3 \cdot 1^2 + a_1 \pmod 3 \cdot 1 + a_0 \pmod 3\right) \pmod 3$$
$$= \left(a_n \pmod 3 + \ldots + a_2 \pmod 3 + a_1 \pmod 3 + a_0 \pmod 3\right) \pmod 3$$
$$= \left(a_n \ldots + a_2 + a_1 + a_0\right) \pmod 3$$

Konklusion: Tallet 3 går op i et tal, hvis tallet 3 går op i tværsummen af taklets cifre.
3 går ikke op i 3497, fordi 3 ikke går op i $3+4+9+7=23$
3 går op i tallet 5378205123, fordi 3 går op i tværsummen, der er 36

Øvelse 6: Hvornår går 9 og 11 op i et tal?
Anvend samme metode som ovenfor til at vise:
a) 9 går op i et tal, hvis 9 går op i tallets tværsum
b) 11 går op i et tal, hvis 11 går op i den alternerende tværsum: $(-1)^n \cdot a_n + (-1)^{n-1} \cdot a_{n-1} + \ldots - a_1 + a_0$
(*Hint*: Udnyt, at $10 \pmod{11} = -1 \pmod{11}$)

Betragter vi $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ og lader vi tallene *a* og *b* være 3 og 4, så er:

$$a+b = 3+4 = 7 \equiv 1 \pmod 6$$
$$a \cdot b = 3 \cdot 4 = 12 \equiv 0 \pmod 6$$

Dvs., at indenfor $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ gælder der:

$$3+4=1$$
$$3 \cdot 4 = 0$$

Allerede her kan vi se, at regning inden for disse mængder er en del anderledes end indenfor almindelige tal, hvor nulreglen altid gælder: Er et produkt 0, er en af faktorerne 0.

Eksempel: Tabeller i $\mathbb{Z}_n$
Vi kan få et godt overblik over regnereglerne i disse mængder ved at opstille tabeller af samme type, som vi lærte at kende i folkeskolen, da vi i de første klasser lærte at addere og multiplicere. For multiplikation udelader vi normalt tallet 0. For $\mathbb{Z}_3$ og $\mathbb{Z}_4$ ser det således ud:

$\mathbb{Z}_3$:

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

·	1	2
1	1	2
2	2	1

$\mathbb{Z}_4$:

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

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Øvelse 7: Tabeller og ligninger med addition i $\mathbb{Z}_5$ og $\mathbb{Z}_6$
a) Opstil tilsvarende tabeller i henholdsvis $\mathbb{Z}_5$ og $\mathbb{Z}_6$.
b) For additionstabellerne lægger vi mærke til, at hver kolonne og hver række indeholder alle tallene i pågældende $\mathbb{Z}_n$ præcis én gang. Specielt indeholder de 0. Det betyder at ethvert tal har et omvendt (*inverst*) tal, der ved addition

ophæver det, så vi får 0. I $\mathbb{Z}_4$ er det omvendte tal til 3 tallet 1, og det omvendte til 2 er 2 selv. Hvad er i $\mathbb{Z}_5$ det omvendte til 3? Hvad er i $\mathbb{Z}_6$ det omvendte til 3?

c) Den egenskab vi har set i b) betyder, at vi kan løse ligninger (med addition) i $\mathbb{Z}_n$. Løs følgende ligninger:

- i $\mathbb{Z}_4$: $2+x=1$
- i $\mathbb{Z}_5$: $4+x=3$
- i $\mathbb{Z}_6$: $3+x=0$

d) Den egenskab vi har set, at $\mathbb{Z}_n$ har, når vi fokuserer på addition, er den samme egenskab som mængden af alle hele tal $\mathbb{Z}$ har. Hvad kalder vi her de omvendte (*inverse*) tal til de naturlige tal? Hvad er løsningerne til ligningerne indenfor $\mathbb{Z}$?

Øvelse 8: Ligninger med multiplikation i $\mathbb{Z}_n$

a) For multiplikationstabellerne lægger vi mærke til et andet system:

- i $\mathbb{Z}_3$ og $\mathbb{Z}_5$ indeholder hver kolonne og hver række alle tallene i pågældende $\mathbb{Z}_n$ (fraregnet 0) præcis én gang. Specielt indeholder de 1. Det betyder at ethvert tal har et reciprokt (*inverst*) tal, der ved multiplikation ophæver det, så vi får 1. I $\mathbb{Z}_5$ er det reciprokke tal til 2 lig med tallet 3. Hvad er det reciprokke tal til 4?
- $\mathbb{Z}_4$ og $\mathbb{Z}_6$ har ikke denne egenskab. Vi ser fx, at i $\mathbb{Z}_4$ indeholder kolonnen og rækken ud for tallet 2 ikke alle tal i $\mathbb{Z}_4$, specielt ikke tallet 1. Hvilke tal har ikke et reciprokt element, og hvilke har?

c) Undersøgelserne i b) fortæller os, at vi kan løse ligninger (med multiplikation) i $\mathbb{Z}_3$ og $\mathbb{Z}_5$, men kun i specielle situationer i $\mathbb{Z}_4$ og $\mathbb{Z}_6$. Undersøg om følgende ligninger har en løsning, og bestem i givet fald løsningen:

- i $\mathbb{Z}_3$: $2\cdot x=1$
- i $\mathbb{Z}_4$: $2\cdot x=1$
- i $\mathbb{Z}_5$: $4\cdot x=3$
- i $\mathbb{Z}_6$: $3\cdot x=2$

d) Den egenskab, vi har set, at $\mathbb{Z}_3$ og $\mathbb{Z}_5$ har, når vi fokuserer på multiplikation, har mængden af alle hele tal $\mathbb{Z}$ ikke. Man kan betragte udvidelsen af talmængderne fra de hele tal $\mathbb{Z}$ til de rationale tal $\mathbb{Q}$ (alle brøkerne) som svaret på et ønske om at kunne løse den slags ligninger. Hvad er løsningerne til ligningerne indenfor $\mathbb{Q}$?

Et kig ind i den moderne algebra

Når vi som ovenfor undersøger, om man kan løse ligninger indenfor en mængde som $\mathbb{Z}_n$ udstyret med regningsarten addition, eller udstyret med regningsarten multiplikation, så bevæger vi os ind i den del af matematikken, vi kalder for moderne algebra.

I moderne algebra studerer man *mængder*, der er udstyret med en *komposition*. Eksempler kan være:

- Mængden af hele tal $\mathbb{Z}$ udstyret med kompositionen +. Dette skriver vi kort således: $(\mathbb{Z},+)$.
- Mængden af positive rationale tal $\mathbb{Q}_+$ udstyret med kompositionen $\cdot$. Dette skriver vi kort således: $(\mathbb{Q}_+,\cdot)$
- Mængden af restklasser $\mathbb{Z}_5$ udstyret med kompositionen $\cdot$. Dette skriver vi kort således: $(\mathbb{Z}_5,\cdot)$.
- Mængden af vektorer i 2D, udstyret med vektoraddition +. Dette kan vi skrive kort således: $(V_2,+)$.
- Mængden af vektorer i 3D, udstyret med vektorprodukt $\times$. Dette kan vi skrive kort således: $(V_3,\times)$.
- Mængden af lineære funktioner udstyret med kompositionen $\circ$ (sammensætning af funktioner). Dette kunne vi kort skrive således: $(\mathrm{L},\circ)$.
- Mængden af positive hele tal $\mathbb{Z}_+$ udstyret med kompositionen x^y (potensopløftning). Dette kunne vi kort skrive således: $(\mathbb{Z}_+,x^y)$.

En *komposition* $\otimes$ i en mængde *M* er en regningsart, der kombinerer to elementer i mængden, så vi får et nyt element i mængden:

Hvis $x, y \in M$, så vil også $x \otimes y \in M$

Derfor er fx *plus* (+), men ikke *gange* ($\cdot$) en komposition i mængden af negative hele tal $\mathbb{Z}_-$.

Og derfor er *skalarproduktet* ikke en komposition i mængden af vektorer. Skalarproduktet kombinerer to vektorer så resultatet bliver et *tal* og ikke en vektor.

Årsagen til, at moderne algebra er en succeshistorie, er bl.a. at man her har fundet redskaber til at studere fælles træk ved vidt forskellige strukturer, hvilket kan give dybere indsigt i hvorfor bestemte matematiske sammenhænge er gældende.

Den grundlæggende konstruktion i moderne algebra er begrebet en *gruppe*:

Definitioner: Grupper

Lad *M* være en mængde udstyret med en komposition $\otimes$. Vi kalder $(M, \otimes)$ for en *gruppe*, hvis der gælder følgende:

1) $\otimes$ opfylder den *associative lov*: $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ for alle elementer *a*, *b* og *c* i *M*.
2) Der findes et *neutralt element*, *e* i *M*: $a \otimes e = e \otimes a = a$ for alle elementer *a* i *M*.
3) Ethvert element *a* i *M* har et *inverst element* $\bar{a}$: $a \otimes \bar{a} = \bar{a} \otimes a = e$

Eksempel: $(\mathbb{Z}, +)$ er en gruppe

1) Den associative lov siger, at man kan hæve og sætte plus-parenteser:
$a + (b + c) = (a + b) + c = a + b + c$
2) Tallet 0 er neutralt element, da $a + 0 = 0 + a = a$, for ethvert tal *a*.
3) Det hele tal *a* har et inverst element, nemlig $-a$: $a + (-a) = (-a) + a = 0$

Øvelse 9

a) Vis, at $(\mathbb{Z}_+, \cdot)$ er en gruppe.

b) Vis, at $(\mathbb{Z}_n, +)$ er en gruppe for ethvert tal *n*.

c) Vis, at $(\mathbb{Z}_5, \{0\}, \cdot)$ er en gruppe, hvor $\mathbb{Z}_5$, $\{0\}$ angiver, at vi ser bort fra tallet 0.

d) Hvad kan du sige om de øvrige mængder med komposition i eksemplet ovenfor?

Øvelse 10: I en gruppe kan man løse simple ligninger

Vis, at hvis $(M, \otimes)$ er en gruppe, så kan man indenfor denne mængde løse ligninger af typen:

1) $a \otimes x = b$ b) $x \otimes a = b$

Øvelse 11: Der er kun ét neutralt element

Antag at både *e* og *f* er neutrale elementer. Udnyt definitionen herpå til at vise $e = f$.

Det har altså god mening at tale om *det* neutrale element.

Øvelse 12: Inverse elementer er entydigt bestemt.

Antag, at *a* har to inverse elementer: $\bar{a}$ og $\tilde{a}$. Vis ved a regne på udtrykket $\bar{a} \otimes a \otimes \tilde{a}$, at $\bar{a} = \tilde{a}$.

Det har altså god mening at tale om *det* inverse element til *a*.

Øvelse 13: Kommutative grupper
Hvis der om en komposition $\otimes$ gælder:

$a \otimes b = b \otimes a$, for alle $a, b \in M$

siger vi, at $\otimes$ er *kommutativ*.
Hvis *M* er en gruppe, kaldes den en *kommutativ gruppe*.
Hvilke af kompositionerne i eksemplet i starten af afsnittet er kommutative?

Restklassegrupperne $(\mathbb{Z}_p, \{0\}, \cdot)$

Vi kan ikke løse ligninger af typen: $a \cdot x = b$ indenfor $(\mathbb{Z}, +)$. Søger vi at løse ligningen vil vi dividere *a* over på h (dvs. gange med det inverse element til *a*). Men så er vi ude i de rationale tals verden. Det er derfor heller ikke så overraskende, at vi heller ikke kan løse sådanne ligninger generelt indenfor $\mathbb{Z}_4$ og $\mathbb{Z}_6$. Det så vi ovenfor. Derimod er det overraskende, at vi kan løse *multiplikative* ligninger både inden for $\mathbb{Z}_3$ og $\mathbb{Z}_5$. I øvelse 6c) så vi, at $(\mathbb{Z}_5, \{0\}, \cdot)$ er en gruppe, hvor $\mathbb{Z}_5, \{0\}$ angiver, at vi ser bort fra tallet 0.

Vi ville have fået et tilsvarende resultat, hvis vi havde opstillet tabeller over $\mathbb{Z}_7$ og $\mathbb{Z}_8$. Man kan løse simple multiplikative ligninger indenfor $(\mathbb{Z}_7, \{0\}, \cdot)$, men ikke indenfor $(\mathbb{Z}_8, \{0\}, \cdot)$. De ser ud til at der gælder følgende generelle resultat:

Sætning: Restklassegrupperne
1) Hvis *p* er et primtal, så er $(\mathbb{Z}_p, \{0\}, \cdot)$ en gruppe
2) Hvis *n* ikke er et primtal, så er $(\mathbb{Z}_n, \{0\}, \cdot)$ ikke en gruppe

Bevis for 1)
Vi får brug for en sætning om primtal, som vi her gengiver uden bevis:

Antag p er et primtal. Så gælder, at hvis $p \mid a \cdot b$ *så vil p gå op i enten a eller b*.

Beviset findes i projekt 0.5 om *Euklids algoritme*.

Antag nu *p* er et primtal. Mængden $\mathbb{Z}_p, \{0\}$ består af:

$$\{1, 2, 3, \ldots, p-1\}$$

Den *associative lov* gælder klart, idet den nedarves fra $(\mathbb{Z}, \cdot)$.

Restklassen 1 er ifølge definitionen på multiplikation af restklasser et *neutralt element* i $\mathbb{Z}_p, \{0\}$.
Det eneste vanskelige punkt er at vise, at et vilkårligt element *a* har et inverst element. Vi lader os lede af det mere simple argument, vi i øvelse 5 gennemførte for at ethvert element i $\mathbb{Z}_5, \{0\}$ har et inverst element: Vi opstillede multiplikationstabellen, og her fandt vi, at hver kolonne og hver række indeholdt alle tallene i $\mathbb{Z}_5, \{0\}$ præcis én gang. Specielt indeholder de det neutrale element 1. Det betyder at ethvert tal har et reciprokt (*inverst*) tal, der ved multiplikation ophæver det, så vi får 1.
a-rækken i multiplikationstabellen for $\mathbb{Z}_p, \{0\}$ indeholder følgende:

$$\{a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)\} \qquad (*)$$

Hvis *p* er et primtal er alle disse forskellige. For antag, at to af dem var ens, dvs. de repræsenterede samme restklasse:

$$a \cdot r \,(\mathrm{mod}\, p) = a \cdot s \,(\mathrm{mod}\, p)$$

Hvis *r* og *s* er forskellige er ét af dem størst, lad os sige det er *r*. Ifølge sætning 2 gælder så:

$$p \mid (a \cdot r - a \cdot s)$$
$$p \mid a \cdot (r - s)$$

Men ifølge sætningen vi citerede i starten af beviset gælder så:

Enten: $p|a$ eller: $p|(r-s)$

Da $a<p$ kan det første ikke være tilfældet. Derfor må det andet gælde, dvs.:

$p|(r-s)$

Vi antog, at *r* og *s* er forskellige, og at $r>s$. Så er $0<r-s<p$

Men så kan *p* jo ikke gå op i $(r-s)$, hvilket giver en modstrid. Altså er $r=s$ og antagelsen om at der findes to restklasser i (*) der er ens er forkert: De er alle forskellige.

Når de alle er forskellige, betyder det, at *a*-rækken indeholder alle tallene i $\square_5$, $\{0\}$ præcis én gang. Specielt indeholder den det neutrale element 1.

Konklusion: Et af tallene i (*) er kongruent med 1. Lad os sige det er $a\cdot b$. Så er *b* det det reciprokke (*inverse*) element til *a*.

Bemærkning 1. Da multiplikation er kommutativ er det lige meget, om vi ser på *a*-rækken eller *a*-kolonnen.
Bemærkning 2. Beviset ovenfor er et eksistensbevis, dvs. vi viser, at der må findes et reciprokt element, men vi angiver ikke en metode til at finde det. Det gør vi i projektet 0.4 om Euklids algoritme.

Øvelse 14: Bevis for 2).

Antag *n* ikke er et primtal, dvs. *n* er et sammensat tal: $n=r\cdot s$

Vis ved at give et modeksempel, at ikke alle elementer i $(\square_n, \{0\},\cdot)$ har et inverst element.

Øvelse 15

De $p-1$ tal i gruppen $(\square_p, \{0\},\cdot)$, hvor *p* er et primtal, kan fremkomme ud fra et vilkårligt af tallene, fx *a* ved at udregne a^t mod p, for alle tal *t* mellem 1 og $p-1$. I et værktøjsprogram som Maple kan det for $p=17$ og $a=3$ se således ud:

$seq(3^t \bmod 17, t=1..16) = 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1$.

hvor vi ser, at alle 16 elementer er med én gang.

a) Vælg et andet tal end 3, og gennemfør det samme.

b) Gennemfør samme øvelse med primtallet 23 og et vilkårligt tal som frembringer.

Vi får i øvrigt forholdsvis let et "spin-off" af ovenstående i form af en berømt sætning fra matematikhistorien. Sætningen er opkaldt efter Pierre Fermat, der første gang formulerede den i et brev fra 1640. Fermat beviste aldrig sine mange påstande, i dette tilfælde fordi "beviset var alt for langt", så det blev først bevist i 1736 af Euler. Sætningen fik sit navn, *Fermats lille sætning* i en artikel fra 1914. Sætningen er bl.a. interessant, fordi en generalisering heraf, som Euler gennemførte, og som indgår i projekt 0.5, er helt central i argumentationen for, at krypteringssystemet RSA virker.

Fermats lille sætning

1) Hvis *p* er et primtal, og *a* er et tal, som *p* ikke går op i, så gælder der: $a^{p-1}\equiv 1(\bmod p)$

2) Hvis *p* er et primtal, og *a* er vilkårligt tal, så gælder der: $a^p\equiv a(\bmod p)$

Bevis for punkt 1)

Antag *p* er et primtal, og at *a* er et tal, som *p* ikke går op i. I beviset for sætningen ovenfor om restklassegrupperne så vi på situationen $a<p$. Men ser vi beviset igennem, ser vi, at det centrale var, om *p* gik op i *a* eller ej. Så vi behøver ikke begrænsningen $a<p$.

I beviset indgik, at de to mængder:

$\{1,2,3,\ldots,p-1\}$ og $\{a\cdot 1, a\cdot 2, a\cdot 3,\ldots, a\cdot(p-1)\}$

repræsenterer de samme restklasser. Ifølge regnereglerne for modulo-regning og sætning 2 gælder derfor:

$$1\cdot 2\cdot 3\cdot \ldots \cdot (p-1) = a\cdot 1\cdot a\cdot 2\cdot a\cdot 3\cdot \ldots \cdot a\cdot (p-1) \pmod p$$

$$1\cdot 2\cdot 3\cdot \ldots \cdot (p-1) = 1\cdot 2\cdot 3\cdot \ldots \cdot (p-1)\cdot a^{p-1} \pmod p$$

$$p \mid 1\cdot 2\cdot 3\cdot \ldots \cdot (p-1)\cdot a^{p-1} - 1\cdot 2\cdot 3\cdot \ldots \cdot (p-1)$$

$$p \mid \left(1\cdot 2\cdot 3\cdot \ldots \cdot (p-1)\right)\cdot \left(a^{p-1}-1\right)$$

Nu har vi igen situationen beskrevet i sætningen først i beviset ovenfor: primtallet *p* går op i et produkt, derfor går det op i mindst én af faktorerne:

$$p \mid \left(1\cdot 2\cdot 3\cdot \ldots \cdot (p-1)\right) \quad \text{eller} \quad p \mid \left(a^{p-1}-1\right)$$

Det første er umuligt, da *p* er et primtal. Derfor gælder det andet. Men ifølge sætning 2, så betyder det, at:

$$a^{p-1} \pmod p = 1 \pmod p$$

eller: $a^{p-1} \equiv 1 \pmod p$

Dette var første version af sætningen.

Bevis for punkt 2)

Lad *a* være et vilkårligt tal. Der er nu to muligheder:

1) *a* er et tal, som *p* ikke går op i 2) at *a* er et tal, som *p* går op i

I første tilfælde har vi situationen fra før, så:

$$a^{p-1} \equiv 1 \pmod p$$

Samtidig er:

$$a \equiv a \pmod p$$

så regnereglerne for modulo-regning giver:

$$a\cdot a^{p-1} \equiv a\cdot 1 \pmod p$$

$$a^p \equiv a \pmod p$$

I andet tilfælde har vi, at *p* går op i *a*. Dermed går *p* også op i ethvert tal, som indeholder *a* som en faktor, eksempelvis i $a\cdot \left(a^{p-1}-1\right)$. Men dette tal er lig med $a^p - a$, så:

$$p \mid \left(a^p - a\right),$$

$a^p \pmod p = a \pmod p$ Anvend sætning 2

$a^p \equiv a \pmod p$ Samme udtryk skrevet med kongruens symbolet.

Hermed er sætningen bevist.

Øvelse 16

Hvis $p=3$ og $a=5$, så siger Fermats lille sætning, at $a^{p-1} = 5^{3-1} = 5^2 = 25$ er kongruent med 1 modulo 3.
Kontroller at det er tilfældet.
Kontroller yderligere Fermats lille sætning med følgende eksempler:

a) $p=5$ og $a=3$

b) $p=7$ og $a=2$

c) $p=11$ og $a=2$

d) $p=13$ og $a=10$

De matematiske værktøjsprogrammer kan gennemføre modulo-regning. Hvis vi ville tjekke Fermats lille sætning på $p=17$ kunne det i maple se sådan ud:

$$seq\left(a^{16} \bmod 17,\ a = 1\ ..16\right) \xrightarrow{\text{to list}} [\,1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1\,]$$

Øvelse 17. Fermats lille sætning undersøgt med værktøjsprogram
Anvend dit værktøjsprogram til at undersøge Fermats lille sætning med primtallet 23 og det sammensatte tal 27.

Eksempel: Perspektivering til kryptering
I den moderne kryptologi, der kaldes RSA-systemet, anvendes meget store primtal i krypteringen af en besked. Udgangspunktet er to primtal *p* og *q* med fx 100 cifre hver. De to tal er hemmelige. Så udregnes deres produkt $n = p \cdot q$, samt yderligere tallet $\varphi(n) = (p-1)\cdot(q-1)$. Herefter smides populært sagt de to primtal *p*, og *q* væk. Derved bliver systemet ubrydeligt. Ved hjælp af tallet $\varphi(n)$ bestemmes så de to nøgler, den ene til kryptering, den anden til dekryptering. De to nøgler bestemmes ved hjælp af *Euklids algoritme*, som behandles i projekt 0.4. Alle beregninger foretages modulo *n*, så dette tal er offentlig kendt, men det er ikke noget problem, for der findes ingen enkle måder til at faktorisere store tal i primfaktorer. Så man kan ikke bestemme primtallene ud fra kendskab til tallet *n*. Man kan derfor heller ikke bestemme tallet $\varphi(n)$, uden kendskab til de to oprindelige primtal. Det betyder, at selv om man kender nøglen til kryptering, kan man ikke bestemme nøglen til dekryptering.
Der er naturligvis mange tekniske problemer i et sådant system. Der er uendeligt mange primtal, og faktisk ikke så få endda af dem. Men der findes ingen formler, der kan generere primtal, så hvordan får vi fat i et primtal på 100 cifre? Eller sagt på en anden måde – hvis vi har et godt bud på et stort primtal, hvordan afgør vi så med sikkerhed, at det faktisk er et primtal? Et stort område indenfor moderne kryptografi drejer sig netop om primtalstest. Der findes ikke et primtalstest, der med 100% sikkerhed giver svaret, det er netop et test. Men der findes meget avancerede og meget stærke sådanne test.
Det første primtalstest man udsætter et tal for er faktisk Fermats lille sætning! Sætningen siger, at *hvis* et tal *p* er et primtal så gælder det, at for *ethvert* mindre tal *a* har a^{p-1} resten 1 ved division med *p*. Den siger ikke det omvendte, at *hvis* det om et tal *q* gælder, at for *ethvert* mindre tal *a* har a^{q-1} resten 1 ved division med *q*, så er tallet *q* et primtal. Men hvis et tal *q* opfylder dette, så er der meget god sandsynlighed for, at det er et primtal, hvorfor det giver mening at gå videre med stærkere og mere krævende test.
Der findes tal *q*, der opfylder betingelserne i Fermats lille sætning, og som ikek er primtal. Disse kaldes *Carmichael tal*. Det mindste Carmichael tal er tallet 561. Det er altså det første sammensatte tal, som består Fermats test. 561 er et sammensat tal: $561 = 3\cdot 11\cdot 17$.