UNDERVISNINGS
MINISTERIET
STYRELSEN FOR
UNDERVISNING OG KVALITET

# Matematik A

Studentereksamen

*Gammel ordning*

Forberedelsesmateriale

Digitale eksamensopgaver med adgang til internettet

gl-stx181-MATn/A-08052018

Tirsdag den 8. maj 2018

# Forberedelsesmateriale til stx-A-net MATEMATIK

Der skal afsættes 6 timer af holdets sædvanlige uddannelsestid til, at eleverne kan arbejde med forberedelsesmaterialet forud for den skriftlige prøve.

3-5 spørgsmål i delprøve 2 af den skriftlige prøve tager udgangspunkt i det materiale, der findes i dette oplæg. De øvrige spørgsmål omhandler emner fra kernestoffet.

Oplægget indeholder teori, eksempler og øvelser i tilknytning til et emne, der ligger umiddelbart i forlængelse af et kernestofemne.

Resultaterne af arbejdet med dette forberedelsesmateriale bør medbringes til den skriftlige prøve.

Alle hjælpemidler er tilladt, og det er tilladt at modtage vejledning.

# Talteori

## Indhold

# Forord

Dette forberedelsesmateriale handler om talteori samt anvendelser heraf.

I forberedelsesmaterialet er der både øvelser og opgaver. Øvelserne er tænkt som hjælp til forståelse af teorien, herunder beviser for nogle af sætningerne. Opgaverne er tænkt som forberedelse til de opgaver, der kommer til den skriftlige eksamen.

I forberedelsesmaterialet anvendes fem typer af farvede bokse. De grønne indeholder definitioner, de grå indeholder eksempler, de orange indeholder sætninger, de blå indeholder øvelser og de lilla indeholder opgaver. Se eksempler på farvekoderne her:

**Definition**

**Eksempel**

**Sætning**

| | |
|---|---|
| **Øvelse** | Øvelserne er tænkt som hjælp til forståelse af teorien, herunder også beviser for nogle af sætningerne. |
| **Opgave** | Opgaverne er tænkt som forberedelse til de opgaver, der kommer til den skriftlige eksamen. |

# Indledning

Dette forberedelsesmateriale omhandler regning med de *naturlige tal* og de *hele tal*. Vi skal se på, hvordan tallene er bygget op og på deres egenskaber, og vi skal regne med de hele tal ved hjælp af *modulo-regning*, når de indgår i en ny type ligninger, kaldet *kongruensligninger*, og en ny type sammenhænge, der kaldes *diskrete sammenhænge*.

Moduloregning bruger vi (måske ubevidst) allerede mange gange om dagen. Når vi fx taler om tid, om hvad klokken er, eller om hvor lang tid, der er til et eller andet, så er det moduloregning, som ligger bag vores angivelser. Når tiden udmåles i timer, regner vi modulo 24 (eller 12), og når tiden udmåles i minutter regner vi modulo 60. Vi siger fx ikke, at klokken er 70 minutter over 8, men at den er 10 minutter over 9. Når klokken passerer midnat, tæller vi ikke videre på tallinjen med 25, 26 osv., men forfra – om natten er klokken 1, 2 osv. Hvis vi siger, 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. Hvis man regner modulo 12, "identificerer" man altså 23 og 11 som værende ens.

Forberedelsesmaterialet lægger både op til, at man regner i hånden med blyant og papir, men også til, at man anvender sit matematiske værktøjsprogram. Det er vigtigt for forståelsen af emnet, at man er bevidst om, hvornår man kan regne øvelser/opgaver i hånden, og hvornår man har brug for sit matematiske værktøjsprogram til at understøtte teorien.

# Tal, mængder og divisibilitet

Vi vil nu kigge nærmere på de hele tal, og på hvornår et helt tal går op i et andet helt tal. Vi får brug for at skelne mellem naturlige tal og hele tal. De naturlige tal kan vi skrive som $\{1, 2, 3, 4, ...\}$, hvor de fire første tal fortæller mønstret, og de tre prikker fortæller, at mønstret fortsætter. De hele tal kan på tilsvarende måde skrives som $\{..., -2, -1, 0, 1, 2, ...\}$.

**Definition 1** Et helt tal *d* kaldes en *divisor* i et helt tal *a*, hvis der findes et helt tal *q*, så $q \cdot d = a$.
Vi skriver $d \mid a$, og siger, at *d* går op i *a*, eller at *a* er deleligt med *d*.
Hvis *d* ikke går op i *a*, skriver vi $d \nmid a$.

**Eksempel 1** 7 er divisor i 28, da $4 \cdot 7 = 28$. Dette skrives $7 \mid 28$.
7 er ikke divisor i 29, da der *ikke* findes et helt tal *q*, så $q \cdot 7 = 29$. Dette skrives $7 \nmid 29$.

**Øvelse 1** Undersøg, om 6 er divisor i henholdsvis 23, 36 eller 44.

Bemærk, at tallet 0 er et særligt tal, som har uendeligt mange divisorer. Dette skyldes, at ethvert tal *d* er divisor i 0, eftersom der findes et tal *q*, så $q \cdot d = 0$ (nemlig $q = 0: \ 0 \cdot d = 0$) jf. definition 1. Alle andre hele tal forskellige fra 0 har kun endeligt mange divisorer. Fx. er alle positive divisorer i 12 tallene 1, 2, 3, 4, 6 og 12.

Bemærk desuden, at tallet *d* går op i tallet *a*, netop når *a* ligger i *d*-tabellen. Fx går 3 op i 15, netop fordi 15 ligger i 3-tabellen.

Ved at bruge definition 1 kan man vise, at hvis $d \mid a$ og $d \mid b$, så vil $d \mid (a+b)$:
Antag, at $d \mid a$ og $d \mid b$. Så findes hele tal $q_1$ og $q_2$, så $a = q_1 \cdot d$ og $b = q_2 \cdot d$.
Heraf får vi, at $a + b = q_1 \cdot d + q_2 \cdot d = (q_1 + q_2) \cdot d$.
Altså kan $a+b$ skrives som et helt tal $(q_1 + q_2)$ gange *d*, hvilket betyder, at $d \mid (a+b)$.

**Øvelse 2** Vis følgende tre påstande for hele tal $a$, $b$, $c$ og $d$. (Vink: brug definition 1)

a) Hvis $d \mid a$ og $d \mid b$, så vil $d \mid (a-b)$.

b) Hvis $d \mid a$, så vil $d \mid (a \cdot c)$.

c) Hvis $a \mid b$ og $b \mid c$, så vil $a \mid c$.

**Definition 2** Et tal $d$, som er divisor i både $a$ og $b$, kaldes en *fælles divisor* for $a$ og $b$. Det største tal blandt alle fælles divisorer for $a$ og $b$ kaldes *den største fælles divisor* for $a$ og $b$ og betegnes $\text{sfd}(a,b)$.

**Øvelse 3**

a) Bestem divisorerne i hvert af tallene 110 og 132 ved at prøve dig frem.

b) Bestem $\text{sfd}(110,132)$ ud fra din viden fra a).

**Opgave 1** Undersøg, hvilken kommando dit matematiske værktøjsprogram anvender til at bestemme den største fælles divisor for to hele tal $a$ og $b$.

**Definition 3** To hele tal $a$ og $b$ siges at være *indbyrdes primiske*, hvis $\text{sfd}(a,b)=1$.
Vi siger også, at $a$ er *primisk* med $b$.

**Øvelse 4**

a) Undersøg uden brug af matematisk værktøjsprogram, om tallene 10 og 21 er indbyrdes primiske.

b) Undersøg med brug af matematisk værktøjsprogram, om tallene 5500 og 3591 er indbyrdes primiske.

**Eksempel 2** Hvis man dividerer et helt tal $a$ med et helt tal $b$ ($b \neq 0$), vil divisionen ikke altid gå op. Dividerer vi fx 13 med 4, får vi, at 4 går 3 gange op i 13, og så er der en rest på 1. Dvs. $13 = 3 \cdot 4 + 1$.

Eksempel 2 illustrerer følgende påstand:

**Sætning 1** **Divisionsligningen**
Lad $a$ være et helt tal og $b$ et naturligt tal. Da findes entydigt bestemte hele tal $q$ (*kvotienten*) og $r$ (*resten*), så man kan opskrive divisionsligningen

$$a = q \cdot b + r \text{ og } 0 \leq r < b.$$

Resten $r$ kaldes den *principale* rest ved division med $b$.

**Opgave 2** Bestem den principale rest ved division af 215 med 7.

**Eksempel 3** Som det fremgår af eksempel 2, er divisionsligningen for $a = 13$ delt med $b = 4$: $13 = 3 \cdot 4 + 1$. I dette tilfælde er den principale rest 1.
Hvis derimod $a = -13$ og $b = 4$, bliver divisionsligningen: $-13 = (-4) \cdot 4 + 3$. Her er $r = 3$ den principale rest, fordi resten $r$ skal opfylde, at $0 \leq r < 4$.

**Øvelse 5** Opskriv divisionsligningen for følgende tal:

a) $a = 30$ og $b = 7$.

b) $a = -68$ og $b = 6$.

## Euklids algoritme

Som vi har set i det foregående afsnit, så kan man bestemme den største fælles divisor for to tal $a$ og $b$ ved at sammenholde divisorerne i de to tal. En anden måde at bestemme den største fælles divisor på er at benytte en regnemetode kaldet *Euklids algoritme*. Algoritmen forløber således:

Lad $a$ og $b$ være naturlige tal, og antag, at $a > b$.
Opskriv divisionsligningen (sætning 1) for $a$ divideret med $b$:

$$a = q_1 \cdot b + r, \quad \text{hvor} \quad 0 \le r < b.$$

Sæt for nemheds skyld $r_0 = a$, $r_1 = b$ og $r_2 = r$. Divisionsligningen ovenover ser nu sådan ud:

$$r_0 = q_1 \cdot r_1 + r_2, \quad \text{hvor} \quad 0 \le r_2 < r_1.$$

Hvis $r_2 = 0$, stopper vi. Hvis $r_2 \neq 0$, divideres $r_1$ med resten $r_2$, og divisionsligningen giver nu:

$$r_1 = q_2 \cdot r_2 + r_3, \quad \text{hvor} \quad 0 \le r_3 < r_2.$$

Hvis $r_3 = 0$, stopper vi. Hvis $r_3 \neq 0$, divideres $r_2$ med resten $r_3$, og divisionsligningen giver:

$$r_2 = q_3 \cdot r_3 + r_4, \quad \text{hvor} \quad 0 \le r_4 < r_3.$$

Sådan fortsættes, indtil man får en rest, som er 0. Vi antager her, at dette sker ved rest nr. $n+1$, altså $r_{n+1} = 0$. På denne måde får vi følgende system af ligninger:

$$\begin{aligned}
r_0 &= q_1 \cdot r_1 + r_2 && 0 \le r_2 < r_1 \\
r_1 &= q_2 \cdot r_2 + r_3 && 0 \le r_3 < r_2 \\
r_2 &= q_3 \cdot r_3 + r_4 && 0 \le r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n && 0 \le r_n < r_{n-1} \\
r_{n-1} &= q_n \cdot r_n + r_{n+1} && 0 = r_{n+1} < r_n
\end{aligned}$$

Bemærk, at algoritmen nødvendigvis må stoppe efter et endeligt antal skridt, da resterne bliver mindre og mindre, for hver gang man anvender divisionsligningen ($r_0 > r_1 > \cdots > r_n > r_{n+1} = 0$).

**Sætning 2** Lad $a$ og $b$ være naturlige tal. Der gælder, at det tal $r_n$, som vi finder ved Euklids algoritme, er den største fælles divisor for tallene $a$ og $b$. Dvs. $\text{sfd}(a,b) = r_n$.

**Eksempel 4** Vi bestemmer den største fælles divisor for tallene 1176 og 518 ved brug af Euklids algoritme:

$$\begin{aligned}
1176 &= 2 \cdot 518 + 140 \\
518 &= 3 \cdot 140 + 98 \\
140 &= 1 \cdot 98 + 42 \\
98 &= 2 \cdot 42 + 14 \\
42 &= 3 \cdot 14 + 0
\end{aligned}$$

Algoritmen stopper her, fordi vi har fået resten 0. Ifølge sætning 2 kan vi aflæse den største fælles divisor i den næstsidste linje. Vi får $\text{sfd}(1176, 518) = 14$.

**Opgave 3**

a) Anvend Euklids algoritme til at bestemme $\text{sfd}(5880, 2088)$.
b) Anvend dit matematiske værktøjsprogram til at kontrollere resultatet i a).

## Primtal

Ethvert naturligt tal kan skrives som et produkt af primtal (og eventuelt tallet $-1$). Man kan derfor betragte primtallene som byggesten for de hele tal. Vi skal kigge lidt nærmere på disse byggesten.

**Definition 4** Et naturligt tal $a \geq 2$ kaldes et *primtal*, hvis det ikke kan deles med andre naturlige tal end 1 og tallet selv.
Et naturligt tal $a \geq 2$ kaldes et *sammensat tal*, hvis det ikke er et primtal, dvs. hvis det har en faktorisering $a = q \cdot d$, hvor $1 < d < a$, $1 < q < a$, og $d$ og $q$ er naturlige tal.

Bemærk: Tallet 1 er hverken et primtal eller et sammensat tal.

Hvis man ønsker at konstruere en liste af primtal mindre end eller lig med et givet tal $n$, kan man anvende en antik græsk metode, som hedder *Eratosthenes' si*. Metoden består i at opskrive de naturlige tal $2, 3, \ldots, n$ i en tabel. Det mindste tal (som er tallet 2) markeres, og alle multipla af 2 fjernes (dvs. alle tal i 2-tabellen). Dernæst markeres det mindste af de tilbageværende tal (det er nu tallet 3), hvorefter alle multipla af dette tal fjernes. Sådan fortsættes, indtil det mindste af de tilbageværende tal er større end $\sqrt{n}$. På denne måde får man siet alle sammensatte tal, der er mindre end eller lig med $n$, væk, og tilbage står primtallene mindre end eller lig med tallet $n$.

**Eksempel 5** Primtallene mindre end 49 kan bestemmes vha. Eratosthenes' si på følgende måde:

**Trin 0:**
Opskriv tallene fra 2 til 49.

| | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 |
| 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 43 | 44 | 45 | 46 | 47 | 48 | 49 |

**Trin 1:** Tallet 2 markeres, og multipla af 2 fjernes

| | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 |
| 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 43 | 44 | 45 | 46 | 47 | 48 | 49 |

**Trin 2:** Tallet 3 markeres, og multipla af 3 fjernes.

| | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 |
| 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 43 | 44 | 45 | 46 | 47 | 48 | 49 |

**Trin 3:** Tallet 5 markeres, og multipla af 5 fjernes.

| | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 |
| 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 43 | 44 | 45 | 46 | 47 | 48 | 49 |

**Trin 4:** Tallet 7 markeres, og multipla af 7 fjernes.

| | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 |
| 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 43 | 44 | 45 | 46 | 47 | 48 | 49 |

**Trin 5:** Primtallene mindre end 49 står nu tilbage i skemaet.

| | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 |
| 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 43 | 44 | 45 | 46 | 47 | 48 | 49 |

Da det mindste tilbageværende tal (som i dette tilfælde er tallet 11) er større end $\sqrt{49} = 7$, har vi nu fundet alle primtal mindre end 49, nemlig 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 og 47.

**Øvelse 6** Anvend Eratosthenes' si til at bestemme primtallene mindre end 225.

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 |
| 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 |
| 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 | 104 | 105 |
| 106 | 107 | 108 | 109 | 110 | 111 | 112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 | 120 |
| 121 | 122 | 123 | 124 | 125 | 126 | 127 | 128 | 129 | 130 | 131 | 132 | 133 | 134 | 135 |
| 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 | 144 | 145 | 146 | 147 | 148 | 149 | 150 |
| 151 | 152 | 153 | 154 | 155 | 156 | 157 | 158 | 159 | 160 | 161 | 162 | 163 | 164 | 165 |
| 166 | 167 | 168 | 169 | 170 | 171 | 172 | 173 | 174 | 175 | 176 | 177 | 178 | 179 | 180 |
| 181 | 182 | 183 | 184 | 185 | 186 | 187 | 188 | 189 | 190 | 191 | 192 | 193 | 194 | 195 |
| 196 | 197 | 198 | 199 | 200 | 201 | 202 | 203 | 204 | 205 | 206 | 207 | 208 | 209 | 210 |
| 211 | 212 | 213 | 214 | 215 | 216 | 217 | 218 | 219 | 220 | 221 | 222 | 223 | 224 | 225 |

**Øvelse 7** Argumentér for, hvorfor man ved brug af Eratosthenes' si finder alle primtal mindre end *n*, hvis man stopper, så snart det mindste af de tilbageværende tal er større end $\sqrt{n}$ .

**Sætning 3** **Aritmetikkens fundamentalsætning**
Ethvert naturligt tal *n* større end 1 er enten et primtal eller kan på én og kun én måde (pånær faktorernes rækkefølge) skrives som et produkt af primtal, dvs. $n = p_1 \cdots p_k$ , hvor $p_1, \ldots, p_k$ alle er primtal. Dette kaldes tallets *primfaktoropløsning*.

**Eksempel 6** Tallet 120 har primfaktoropløsningen $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$ .
Tallet 980 har primfaktoropløsningen $980 = 2 \cdot 2 \cdot 5 \cdot 7 \cdot 7$.
Vi kan bestemme $\text{sfd}(120,980)$ ud fra tallenes primfaktoropløsninger, eftersom største fælles divisor er produktet af de primfaktorer, som indgår i både 120 og 980. Vi ser at $\text{sfd}(120,980) = 2 \cdot 2 \cdot 5 = 20$.

**Øvelse 8** Bestem primfaktoropløsningen af tallet 308 og af tallet 1400.
Benyt de fundne primfaktoropløsninger til at bestemme $\text{sfd}(308,1400)$ .

**Øvelse 9** Undersøg, hvilken kommando dit matematiske værktøjsprogram anvender til at opløse et tal i dets primfaktorer.

**Sætning 4** **Euklids sætning**
Der findes uendeligt mange primtal.

**Bevis for sætning 4**
Antag omvendt, at der kun findes et endeligt antal primtal, dvs. at vi antager, at $p_1, p_2, \ldots, p_k$ er samtlige primtal. Betragt tallet $n = p_1 \cdot \cdots \cdot p_k + 1$ . Dette tal kan *ikke* være et primtal, da det er forskelligt fra alle $p_i$'erne . Altså må der ifølge sætning 3 findes et primtal *p*, så $n = d \cdot p$ , hvor $1 < d < n$ . Da $p_1, p_2, \ldots, p_k$ er samtlige primtal (ifølge antagelsen), så må *p* være ét af disse $p_i$ 'er, og dermed må $p \mid p_1 \cdot \cdots \cdot p_k$ . Nu har vi, at $p \mid n$ og $p \mid p_1 \cdot \cdots \cdot p_k$ , og derfor må *p* også være divisor i differensen $n - p_1 \cdot \cdots \cdot p_k$ (ifølge øvelse 2a).

Men $n - p_1 \cdot \cdots \cdot p_k = 1$, og tallet 1 har ingen primtalsdivisorer. Heraf slutter vi, at vores antagelse må være forkert, hvilket betyder, at $p_1, p_2, \ldots, p_k$ *ikke* kan være samtlige primtal.

Bemærk: Beviset er ikke i matematisk forstand *konstruktivt*. Dette betyder, at selvom der findes uendeligt mange primtal, så har vi ikke en algoritme til at producere primtal. Det er netop denne egenskab ved primtallene (at de ikke er konstruerbare), som man udnytter, når man vil lave en sikker kode inden for kryptering.

**Øvelse 10** Bevis, at et primtal $p$ er indbydes primisk med et helt tal $a$, hvis og kun hvis $p$ ikke går op i $a$.

## Restklasser og moduloregning

Vi skal i det følgende se, hvordan man kan inddele de hele tal i grupper kaldet *restklasser* og regne med disse ved hjælp af moduloregning.

Vi ser igen på eksemplet med klokken og på, hvordan man regner med timer, alt efter om man tænker på klokken som inddelt i 12 timer eller i 24 timer. Hvis man fx går i seng kl. 22 og sætter uret, så man kan sove i 9 timer, så siger vi ikke, at man står op kl. $22 + 9 = 31$, men derimod kl. 7. Tallet 7 får vi matematisk ved at trække 24 fra 31. I praksis tæller de fleste nok op til 24 (det var 2 timer), og så er der 7 timer tilbage af de 9 timer, hvilket vil sige, at vi står op kl. 7. Her "identificerer" vi altså 31 og 7 som værende ens. Men vi kan naturligvis ikke skrive $31 = 7$. Derfor har man i matematik indført en særlig betegnelse for denne måde at identificere tal på, nemlig ved at skrive $31 \equiv 7 \pmod{24}$.

Betegnelsen "mod 24" læses *modulo* 24 og angiver, at 24 går op i $31 - 7$. Eksempelvis ser vi, at der gælder:

$48 \equiv 0 \pmod{24}$ fordi $48 - 0 = 2 \cdot 24$, og

$245 \equiv 5 \pmod{24}$ fordi $245 - 5 = 10 \cdot 24$.

Det sidste udtryk, hvor vi regner modulo 24, kan vi tolke således: Hvis klokken nu fx er 9, så er den om 245 timer $9 + 5 = 14$.

**Øvelse 11**
a) Giv en praktisk fortolkning af udregningen $80 \equiv 20 \pmod{60}$ i relation til klokken.
b) Giv en praktisk fortolkning af udregningen $380 \equiv 15 \pmod{365}$ i relation til årskalenderen.

Vi vil nu indføre begrebet *modulo* lidt mere formelt, så vi kan indføre regneregler og senere løse ligninger, som gør brug af moduloregning.

**Definition 5** Lad $m$ være et naturligt tal. To hele tal $a$ og $b$ siges at være *kongruente modulo m*, hvis

$$m \mid (a - b).$$

Hvis $a$ og $b$ er kongruente modulo $m$, skriver vi

$$a \equiv b \pmod{m}.$$

**Eksempel 7**
a) $17 \equiv 2 \pmod{5}$, da 5 går op i $(17 - 2) = 15$.
b) $21 \equiv 0 \pmod{7}$, da 7 går op i $(21 - 0) = 21$.
c) $-4 \equiv 20 \pmod{12}$, da 12 går op i $(-4 - 20) = -24$.

En anden måde at udtrykke på, at to tal $a$ og $b$ er kongruente modulo $m$, er, at $a$ og $b$ har samme rest ved division med $m$. I eksempel 7 har tallene 17 og 2 begge rest 2 ved division med 5, tallene 21 og 0 har begge rest 0 ved division med 7, og tallene -4 og 20 har begge rest 8 ved division med 12 (jf. divisionsligningerne $-4 = -1 \cdot 12 + 8$ og $20 = 1 \cdot 12 + 8$).

**Øvelse 12** Undersøg, om

a) $1528 \equiv 10 \pmod{11}$.

b) $147 \equiv -2 \pmod{75}$.

**Øvelse 13** Benyt definition 5 til at bestemme de naturlige tal *m*, for hvilke der gælder, at

a) $28 \equiv 22 \pmod{m}$.

b) $33 \equiv -7 \pmod{m}$.

**Øvelse 14** Forklar, hvad det betyder, at et helt tal *a* opfylder, at $a \equiv 0 \pmod{m}$.

**Øvelse 15** Tag udgangspunkt i dagen i dag. Hvordan kan man bestemme, hvilken ugedag det er om 1000 dage?

I bogbranchen anvendes ISBN (The International Standard Book Number) som identifikationssystem. Enhver udgivet bog, pjece og lydbog har sit eget ISBN, som efter år 2007 består af et 13-cifret tal $x_1x_2x_3 \ldots x_{13}$, hvoraf de første tre cifre identificerer bogbranchen (pt. 978 eller 979), efterfulgt af et 9-cifret hovednummer (indeholdende information om land, forlag, titel) og til sidst et kontrolciffer, der viser, at hele nummeret er korrekt.
Fx er Danmarks landekode $x_4x_5 = 87$, Sveriges $x_4x_5 = 90$, mens bøger udgivet i USA, Storbritannien, Canada eller Australien har landekode $x_4 = 0$, og bøger udgivet i tysktalende lande har landekode $x_4 = 3$.
Et korrekt ISBN skal opfylde, at summen af de 13 cifre vægtet med skiftevis 1 og 3 er delelig med 10. Med andre ord opfylder et gyldigt ISBN at

$$x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + x_{13} \equiv 0 \pmod{10}.$$

**Eksempel 8** For at tjekke, om et ISBN er gyldigt, indsættes cifrene i ovenstående formel. Fx tjekkes ISBN 9788790996574 på følgende måde:
$9 + 3\cdot 7 + 8 + 3\cdot 8 + 7 + 3\cdot 9 + 0 + 3\cdot 9 + 9 + 3\cdot 6 + 5 + 3\cdot 7 + 4 = 180$.
Da $180 \equiv 0 \pmod{10}$, er dette et gyldigt ISBN.
Hvis et af cifrene er ulæseligt, fx cifferet $x_3$, så kan man reparere ISBN på følgende måde:
$9 + 3\cdot 7 + x_3 + 3\cdot 8 + 7 + 3\cdot 9 + 0 + 3\cdot 9 + 9 + 3\cdot 6 + 5 + 3\cdot 7 + 4 = 172 + x_3$.
Da dette tal skal være kongruent med 0 modulo 10, får vi, at $x_3 = 8$.
Tilsvarende; hvis det er et ciffer, der vægtes med 3, som er ulæseligt, fx cifferet $x_2$, så kan ISBN repareres på følgende måde:
$9 + 3\cdot x_2 + 8 + 3\cdot 8 + 7 + 3\cdot 9 + 0 + 3\cdot 9 + 9 + 3\cdot 6 + 5 + 3\cdot 7 + 4 = 3\cdot x_2 + 159$.
Tallet skal altså opfylde, at $3\cdot x_2 + 159 \equiv 0 \pmod{10}$, hvilket svarer til, at $3\cdot x_2 \equiv 1$.
Eneste ciffer, som opfylder dette, er $x_2 = 7$.
Laver man en simpel søgning på internettet, finder man titlen på udgivelsen.

**Opgave 4**

a) Undersøg, om tallene 9780385737951 og 9788711568197 er gyldige ISBN.

b) Bestem kontrolcifferet $x_{13}$ hørende til et gyldigt ISBN, som har nummeret $978043902352\,x_{13}$.

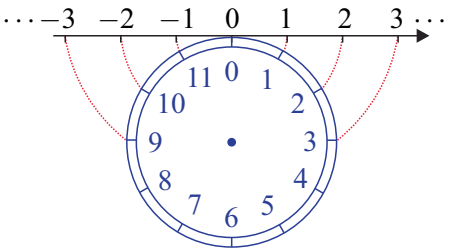
c) På en bog aflæses dets ISBN til $97887\,x_6\,2215694$. Det sjette ciffer $x_6$ er så utydeligt, at det ikke kan aflæses. Bestem det sjette ciffer, så bogen har et gyldigt ISBN, og overvej, om der er flere muligheder for cifret $x_6$.

Ved anvendelse af moduloregning kan vi inddele de hele tal i mængder, som har samme rest ved division med et givet tal $m$. Disse mængder kaldes for restklasser, og vi skal se, at det er muligt at regne med restklasser.

**Definition 6** *Restklassen* $[a]_m$ består af de hele tal $b$, som har samme rest som $a$ ved division med $m$. Tallet $a$ kaldes en *repræsentant* for restklassen $[a]_m$.

**Eksempel 9**
a) $[2]_5 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}$. Tallene i denne mængde har alle rest 2 ved division med 5.
b) $[0]_7 = \{\ldots, -14, -7, 0, 7, 14, 21, 28, \ldots\}$. Tallene i denne mængde har alle rest 0 ved division med 7.

Hvis vi vender tilbage til eksemplet med klokken, så ligger tallene 31 og 7 i samme restklasse, når vi regner modulo 24, fordi 31 timer svarer til 7 timer ($31 = 24 + 7$). Dette stemmer overens med definition 6, eftersom 31 og 7 har samme rest (nemlig 7) ved division med 24.




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

Restklasser og kongruenser svarer således til hinanden:

$$[a]_m = [b]_m \quad \Leftrightarrow \quad a \equiv b \pmod{m}.$$

En restklasse har derfor uendelig mange repræsentanter, fx er $[-3]_5 = [2]_5 = [7]_5$, eftersom $-3 \equiv 2 \equiv 7 \pmod 5$. Vi vil dog primært benytte den principale rest $a$, hvor $0 \le a < m$, som repræsentant for en restklasse modulo $m$. Bemærk forskellen i brugen af "$\equiv$" og "$=$".

Omkring antallet af restklasser gælder, at der er $m$ restklasser modulo $m$, svarende til de $m$ forskellige principale rester, som man kan få ved division med $m$.

**Definition 7** Mængden af restklasser modulo $m$ betegnes med $\mathbb{Z}_m$, dvs. $\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$.
(Indekset $m$ på restklasserne undlades, når der ikke er tvivl om, hvilken modulo vi arbejder med).

**Eksempel 10** Restklasserne modulo 5 kan repræsenteres ved tallene 0, 1, 2, 3 og 4:

$$[0] = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}.$$
$$[1] = \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\}.$$
$$[2] = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}.$$
$$[3] = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}.$$
$$[4] = \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}.$$

**Øvelse 16** Opskriv på tilsvarende måde som i eksempel 10 de mulige restklasser modulo 6.

**Opgave 5** Gør rede for, at $[18]=[44]$ i $\mathbb{Z}_{13}$.

## Addition og multiplikation af restklasser

Vi ønsker i det følgende at kunne regne med restklasser. Det viser sig, at det er muligt at definere addition og multiplikation på mængden $\mathbb{Z}_m$ uafhængigt af valg af restklassernes repræsentanter.

**Definition 8** For et naturligt tal $m$ er addition og multiplikation modulo $m$ givet ved:

$$[a]+[b]=[a+b].$$
$$[a]\cdot[b]=[a\cdot b].$$

**Eksempel 11** Tabellerne viser addition og multiplikation i $\mathbb{Z}_6$. Her angives restklassen $[x]$ ved den principale rest $x$ som repræsentant for restklassen.

| + | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 | 5 |
| **1** | 1 | 2 | 3 | 4 | 5 | 0 |
| **2** | 2 | 3 | 4 | 5 | 0 | 1 |
| **3** | 3 | 4 | 5 | 0 | 1 | 2 |
| **4** | 4 | 5 | 0 | 1 | 2 | 3 |
| **5** | 5 | 0 | 1 | **2** | 3 | 4 |

| • | **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 |

Additionstabellen fås ved eksempelvis at udregne $[5]+[3]=[5+3]=[8]=[2]$, svarende til $5+3\equiv 2 \pmod 6$.
Multiplikationstabellen fås ved eksempelvis at udregne $[5]\cdot[3]=[5\cdot 3]=[15]=[3]$, svarende til $5\cdot 3\equiv 3 \pmod 6$.

**Øvelse 17** Anvend tabellerne i eksempel 11 til at udregne og opskrive på moduloform i $\mathbb{Z}_6$:

a) $[5]+[1]$.
b) $[4]+[4]$.
c) $[4]\cdot[4]$.
d) $[2]\cdot[5]$.

**Øvelse 18** Opstil en additionstabel og en multiplikationstabel i $\mathbb{Z}_7$.

Additionstabellen for $\mathbb{Z}_6$ viser eksempelvis, at $[3]+[4]=[4]+[3]$, altså at rækkefølgen ved addition er ligegyldig. Tilsvarende viser multiplikationstabellen for $\mathbb{Z}_6$, at $[2]\cdot[5]=[5]\cdot[2]$, dvs. at rækkefølgen ved multiplikation er ligegyldig. Regning med restklasser svarer i nogle tilfælde til de regneregler, man bruger, når man regner med hele tal. Der gælder følgende regneregler:

**Sætning 5** For et naturligt tal $m$ og hele tal $a$, $b$, $c$ og $d$ gælder følgende regneregler i $\mathbb{Z}_m$:

i. Hvis $[a]=[b]$ og $[c]=[d]$, så er $[a]+[c]=[b]+[d]$.

ii. Hvis $[a]=[b]$ og $[c]=[d]$, så er $[a]-[c]=[b]-[d]$.

iii. Hvis $[a]=[b]$ og $[c]=[d]$, så er $[a]\cdot[c]=[b]\cdot[d]$.

iv. Hvis $k$ er et naturligt tal og $[a]=[b]$, så er $[a^k]=[b^k]$.

v. Hvis $[a]\cdot[b]=[a]\cdot[c]$ og $\text{sfd}(a,m)=1$, så er $[b]=[c]$.

**Øvelse 19** Overvej, hvorfor regneregel iv. i sætning 5 er indeholdt i regneregel iii.

**Eksempel 12** Vi vil bestemme den principale rest af $7^{20}$ ved division med 11.
Da tallet $7^{20}$ er et meget stort tal, omskriver vi det vha. potensregneregler til:
$7^{20}=7^{2\cdot2\cdot2\cdot2}\cdot7^{2\cdot2}$, så vi kan bestemme den principale rest ved at dele op i få trin.
I $\mathbb{Z}_{11}$ får vi (idet vi husker, at vi regner modulo 11), at

$$[7^2]=[7\cdot7]=[49]=[5] \quad\Rightarrow\quad [7^2]=[5]$$
$$[7^4]=[(7^2)^2]=[7^2\cdot7^2]=[7^2]\cdot[7^2]=[5]\cdot[5]=[5\cdot5]=[25]=[3] \quad\Rightarrow\quad [7^4]=[3]$$
$$[7^8]=[(7^4)^2]=[7^4\cdot7^4]=[7^4]\cdot[7^4]=[3]\cdot[3]=[3\cdot3]=[9] \quad\Rightarrow\quad [7^8]=[9]$$
$$[7^{16}]=[(7^8)^2]=[7^8\cdot7^8]=[7^8]\cdot[7^8]=[9]\cdot[9]=[9\cdot9]=[81]=[4] \quad\Rightarrow\quad [7^{16}]=[4]$$
$$[7^{20}]=[7^{16}\cdot7^4]=[7^{16}]\cdot[7^4]=[4]\cdot[3]=[4\cdot3]=[12]=[1] \quad\Rightarrow\quad [7^{20}]=[1]$$

Altså er $7^{20}\equiv1\,(\text{mod}\,11)$.

**Øvelse 20** Benyt metoden i eksempel 12 til at bestemme den principale rest af $4^{17}$ ved division med 7.

**Opgave 6** Bestem den principale rest af $5^{34}$ ved division med 9. (Vink: se eksempel 12).

## Lineære kongruensligninger

Ligninger med restklasser kan opstilles på samme måde som almindelige ligninger, hvor der indgår et ukendt $x$. De simpleste ligninger af denne type kaldes *lineære kongruensligninger*.

**Eksempel 13** Vi vil løse en lineær kongruensligning givet ved $[5]+[x]=[3]$ i $\mathbb{Z}_6$.
Hvis vi bruger additionstabellen for $\mathbb{Z}_6$

| + | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 | 5 |
| **1** | 1 | 2 | 3 | 4 | 5 | 0 |
| **2** | 2 | 3 | 4 | 5 | 0 | 1 |
| **3** | 3 | 4 | 5 | 0 | 1 | 2 |
| **4** | 4 | 5 | 0 | 1 | 2 | 3 |
| **5** | 5 | 0 | 1 | 2 | 3 | 4 |

så ser vi i rækken for $[5]$, at vi skal lægge $[4]$ til for at få $[3]$. Løsningen til

kongruensligningen er derfor $[x]=[4]$.
Alternativt kan vi skrive restklassen $[3]$ op som $\{\ldots,-3,3,9,15,21,\ldots\}$. Vi kan trække 5 fra hvert af disse tal, og vi får så $\{\ldots,-8,-2,4,10,16,\ldots\}$ svarende til restklassen $[4]$.
Vi får igen løsningen $[x]=[4]$ og siger, at vi i dette tilfælde har løst opgaven ved *inspektion*.

**Øvelse 21** Løs kongruensligningen $[3]+[x]=[1]$ i $\mathbb{Z}_7$.

**Eksempel 14** Vi vil løse en lineær kongruensligning givet ved $[4]\cdot[x]=[3]$ i $\mathbb{Z}_6$.
Hvis vi bruger multiplikationstabellen for $\mathbb{Z}_6$

| • | **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 |

så ser vi i rækken for $[4]$, at vi ikke kan finde en restklasse, så vi får $[3]$, når vi multiplicerer. Altså er der ingen løsning til denne kongruensligning.
Alternativt, hvis vi skriver restklassen $[3]$ som $\{\ldots,-3,3,9,15,21,\ldots\}$ og løser kongruensligningen ved inspektion, skal vi blandt disse tal lede efter et tal, hvor 4 går op. Vi ser, at der ikke findes et tal, hvor 4 går op, da alle tallene i listen er ulige. Konklusionen er igen, at der ikke findes en løsning til kongruensligningen.

Fremover vil vi skrive ligningerne på formen $[a\cdot x]=[b]$ og $[a+x]=[b]$, svarende til $[a]\cdot[x]=[b]$ og $[a]+[x]=[b]$.

**Øvelse 22** Løs følgende kongruensligninger i $\mathbb{Z}_6$ uden og med brug af matematisk værktøjsprogram:
a) $[2x]=[2]$ (to løsninger).
b) $[5x]=[3]$ (én løsning).

**Eksempel 15** Løsning af kongruensligningen $[5x]=[3]$ i $\mathbb{Z}_7$.
Vi vil forsøge at løse denne kongruensligning ved inspektion. Vi opskriver restklassen $[3]=\{\ldots,3,10,17,24,31,38,45,\ldots\}$ og leder blandt disse elementer efter et tal, hvor 5 er divisor. Tallet 10 opfylder dette, og da $10=5\cdot 2$, så kan $x$ være 2. Vi har således fundet ud af, at $[x]=[2]$ er en løsning til kongruensligningen, idet $[5\cdot 2]=[10]=[3]$ i $\mathbb{Z}_7$.

**Opgave 7** Find ud af, hvordan dit matematiske værktøjsprogram kan løse kongruensligninger, og løs kongruensligningen $[5x]=[3]$ i $\mathbb{Z}_7$ (se bilag).

**Opgave 8** Bestem mulige løsninger til følgende kongruensligninger:
a) $[3x]=[4]$ i $\mathbb{Z}_8$.
b) $[7x]=[5]$ i $\mathbb{Z}_9$.

**Opgave 9** Argumenter for, at restklassen $[3]$ ikke er løsning til kongruensligningen $[5x]=[1]$ i $\mathbb{Z}_9$.

Det er ikke alle kongruensligninger, der har løsninger, som vi allerede har set i eksempel 14, og der findes også kongruensligninger, der har flere forskellige restklasser som løsninger, som vi så i øvelse 22.

Det viser sig, at antallet af løsninger til en kongruensligning $[a \cdot x] = [b]$ i $\mathbb{Z}_m$ kan bestemmes ud fra konstanterne $a, b$ og $m$ på følgende måde:

**Sætning 6** Kongruensligningen $[a \cdot x] = [b]$ i $\mathbb{Z}_m$ har løsninger, hvis og kun hvis $\text{sfd}(a,m) \mid b$.
Hvis $\text{sfd}(a,m) \mid b$, så er antallet af løsninger lig med $\text{sfd}(a,m)$.

**Øvelse 23** Argumenter ved brug af sætning 6 for, at der er netop en løsning til kongruensligningen, hvis og kun hvis $\text{sfd}(a,m) = 1$.

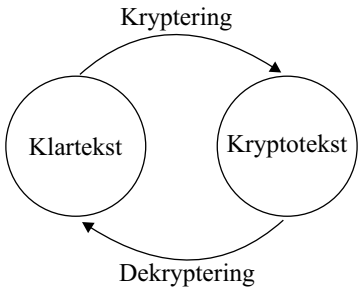
**Eksempel 16** Vi vil bestemme antallet af løsninger til kongruensligningen $[2x] = [3]$ i $\mathbb{Z}_4$.
Da $\text{sfd}(2,4) = 2$ og $2 \nmid 3$, følger det af sætning 6, at kongruensligningen ikke har nogen løsning.

**Eksempel 17** Vi vil bestemme antallet af løsninger til kongruensligningen $[2x] = [8]$ i $\mathbb{Z}_{10}$.
Da $\text{sfd}(2,10) = 2$ og $2 \mid 8$, følger det af sætning 6, at kongruensligningen har 2 løsninger.
Hvis vi ønsker at bestemme de to løsninger, kan vi opskrive restklassen $[8]$ i $\mathbb{Z}_{10}$:
$[8] = \{\ldots, 8, 18, 28, 38, \ldots\}$. Vi leder blandt disse elementer efter et tal, hvori 2 går op – det gør 2 i alle tallene. Fx er $8 = 2 \cdot 4$, hvilket betyder, at restklassen $[4]$ er en løsning, og $18 = 2 \cdot 9$, hvilket betyder, at $[9]$ er en løsning. Da vi nu har fundet to løsninger, og vi samtidigt har indset, at der netop er to løsninger, så har vi fundet alle løsninger til kongruensligningen.

**Opgave 10** Argumenter ved brug af sætning 6 for antallet af løsninger til kongruensligningerne
a) $[3x] = [8]$ i $\mathbb{Z}_{10}$.
b) $[3x] = [6]$ i $\mathbb{Z}_{15}$.

## Kryptering og dekryptering med diskrete sammenhænge

Kryptering af beskeder har lige siden Romerriget været en disciplin, som folk har ønsket at beherske, så en besked ikke gav mening, hvis en anden person, fx en fjende, opfangede beskeden.




Figuren til venstre illustrerer den grundlæggende opbygning af et kryptosystem bestående af kryptering og dekryptering.
Hvis udgangspunktet er en klartekst, så kan denne krypteres til en kryptotekst. Tilsvarende kan en kryptotekst dekrypteres, så man kommer tilbage til klarteksten.

Kejseren Julius Cæsar har givet navn til det simple kryptosystem, hvor hvert bogstav i klarteksten bliver erstattet af et nyt bogstav fx fem pladser længere til højre i alfabetet. Vi siger, at dette kryptosystem har et *skifte* på 5. Nøglen (kryptering/dekryptering) i dette kryptosystem kan beskrives ved nedenstående tabel, hvor vi vælger at arbejde med det engelske alfabet.

| **Klartekst** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Kryptotekst | F | G | H | I | J | K | L | M | N | O | P | Q | R |

| **Klartekst** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Kryptotekst | S | T | U | V | W | X | Y | Z | A | B | C | D | E |

**Øvelse 24** Krypter klarteksten "VI ER DISKRETE" ud fra ovenstående kryptosystem, idet mellemrummene bliver udeladt.

Vi kan også oversætte bogstaverne til tal, hvor tallet angiver bogstavets placering i alfabetet, og derved lave en talrepræsentation af nøglen:

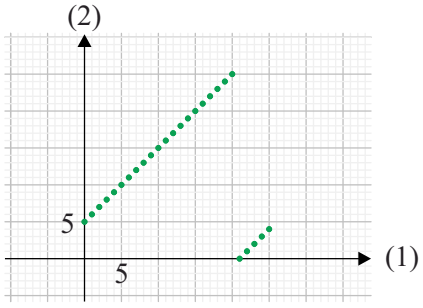
| **Klartekst** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Klartal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Kryptotal | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| Kryptotekst | F | G | H | I | J | K | L | M | N | O | P | Q | R |

| **Klartekst** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Klartal | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Kryptotal | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 | 3 | 4 |
| Kryptotekst | S | T | U | V | W | X | Y | Z | A | B | C | D | E |

Talrepræsentationen i tabellen viser, at vi skal lægge 5 til tallet i klarteksten for at få tallet i kryptoteksten, mens vi samtidigt regner modulo 26, så: $21+5\equiv 0$, $22+5\equiv 1$, $23+5\equiv 2$ osv. Dette betyder, at vi kan beskrive kryptosystemet ved hjælp af restklasser i $\mathbb{Z}_{26}$ og regning med disse restklasser.

Vi siger, at Julius Cæsar kryptosystemet kan beskrives ved den *diskrete sammenhæng* $[y]=[x+5]$ i $\mathbb{Z}_{26}$, hvor $x$ er talrepræsentationen af et bogstav i klarteksten, og $y$ er talrepræsentationen af bogstavet i kryptoteksten.

Grafen for den diskrete sammenhæng $[y]=[x+5]$ i $\mathbb{Z}_{26}$ ser ud på følgende måde:




Vi ser, at grafen består af en række punkter, som ligger på rette linjer. Bemærk, at $y$-værdierne til punkterne antager værdier mellem 0 og 25.

**Opgave 11** Find ud af, hvordan man tegner grafer for diskrete sammenhænge i dit matematiske værktøjsprogram, og tegn grafen for den diskrete sammenhæng $[y]=[x+5]$ i $\mathbb{Z}_{26}$ (se bilag).

**Eksempel 18** Når vi skal bestemme en diskret sammenhæng, der kan bruges til at dekryptere en kryptotekst, så skal vi bestemme en *omvendt* diskret sammenhæng.
Hvis vi som udgangspunkt krypterer med den diskrete sammenhæng $[y]=[x+9]$ i $\mathbb{Z}_{26}$, så har vi, at A i klarteksten bliver til 0 som klartal. 0 bliver med den diskrete sammenhæng til 9 som kryptotal, hvilket svarer til J som kryptotekst.
Når vi skal bestemme den omvendte diskrete sammenhæng, så skal vi bestemme en diskret sammenhæng, så vi fra 9 kommer tilbage til 0. Når vi regner med restklasser, så svarer dette til, at vi skal løse ligningen $[x+9]=[0]$ i $\mathbb{Z}_{26}$, fordi 0 er neutralt i forhold til addition. Vi løser ligningen ved inspektion, dvs. vi opskriver restklassen $[0]=\{\ldots,-26,0,26,52,78,\ldots\}$ i $\mathbb{Z}_{26}$. Subtraherer vi 9 fra alle elementer, så får vi $\{\ldots,-35,-9,17,43,69,\ldots\}$, hvilket svarer til restklasse $[17]$ i $\mathbb{Z}_{26}$. Den omvendte diskrete sammenhæng er derfor $[x]=[y+17]$ i $\mathbb{Z}_{26}$.
Vi kan nu prøve at dekryptere med denne omvendte diskrete sammenhæng. J som kryptotekst svarer til 9 som kryptotal. Adderer vi 9 med 17, så får vi 26, hvilket svarer til 0 i $\mathbb{Z}_{26}$. 0 som klartal svarer til A som klartekst, og vi er tilbage ved bogstavet, som vi startede med.

**Opgave 12**

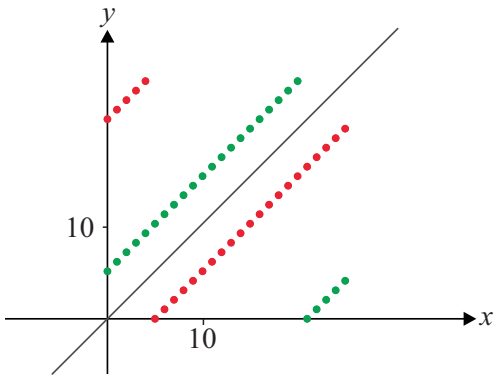
a) Løs kongruensligningen $[x+5]=[0]$ i $\mathbb{Z}_{26}$.

b) Betragt $[y]=[x+5]$ som en kongruensligning i $\mathbb{Z}_{26}$, og bestem en løsning $[x]$ udtrykt ved $[y]$ ved brug af regnereglerne for restklasser (sætning 5).

c) Opskriv en diskret sammenhæng for dekrypteringen fra [y] til [x].

d) Dekrypter "IJYJWXTRRJW" ved hjælp af sammenhængen fra c).

Hvis vi tegner graferne for de to diskrete sammenhænge $[y]=[x+5]$ og $[y]=[x+21]$ begge i $\mathbb{Z}_{26}$ i det samme koordinatsystem, får vi




Vi ser, at de røde punkter er grafen for den diskrete sammenhæng $[y]=[x+21]$ i $\mathbb{Z}_{26}$. Vi ser desuden, at de røde punkter svarer til en spejling af de grønne punkter i linjen med ligningen $y=x$. Dette betyder, at vi kan finde en diskret sammenhæng for dekrypteringen grafisk ved at spejle den diskrete sammenhæng for krypteringen i linjen med ligningen $y=x$, og derefter aflæse sammenhængen for dekrypteringen, hvis den vel at mærke findes.

**Øvelse 25** Benyt dit matematiske værktøjsprogram til at efterprøve ovenstående.

**Øvelse 26**

a) Opskriv en diskret sammenhæng for kryptering med Julius Cæsar kryptosystem, hvor skiftet er 20.
b) Opskriv en diskret sammenhæng for dekryptering med Julius Cæsar kryptosystem, hvor skiftet er 20.
c) Tegn graferne for de to diskrete sammenhæng fra hhv. a) og b) i det samme koordinatsystem, og bemærk, at de er en spejling af hinanden.

**Øvelse 27**

Hvor mange forskellige Julius Cæsar kryptosystemer af denne type kan vi konstruere?

I Julius Cæsar kryptosystemet er det nemt at se et mønster fra en kryptotekst til en klartekst, og derfor er kryptosystemet også nemt at bryde. Vi kan på baggrund af diskrete sammenhænge konstruere et andet kryptosystem, hvor mønsteret ikke er helt så nemt at gennemskue.

**Eksempel 19**

Betragt et kryptosystem bestemt ved den diskrete sammenhæng $[y]=[5x]$ i $\mathbb{Z}_{26}$.
Tabelrepræsentationen af nøglen bliver:

| **Klartekst** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Klartal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Kryptotal | 0 | 5 | 10 | 15 | 20 | 25 | 4 | 9 | 14 | 19 | 24 | 3 | 8 |
| Kryptotekst | A | F | K | P | U | Z | E | J | O | T | Y | D | I |

| **Klartekst** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Klartal | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Kryptotal | 13 | 18 | 23 | 2 | 7 | 12 | 17 | 22 | 1 | 6 | 11 | 16 | 21 |
| Kryptotekst | N | S | X | C | H | M | R | W | B | G | L | Q | V |

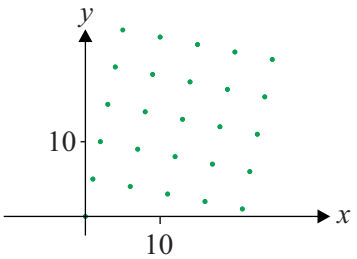
Forklaring på tabellen: Fx bliver klartallet 7 (svarende til bogstavet H), krypteret til kryptotallet 9 svarende til bogstavet J, fordi $5\cdot 7=35\equiv 9 \pmod{26}$.

I kongruensligningen ovenfor indgår der multiplikation. Når vi skal bestemme en diskret sammenhæng for dekryptering, udnytter vi, at tallet 1 er neutralt for multiplikation (ligesom tallet 0 er neutralt for addition).

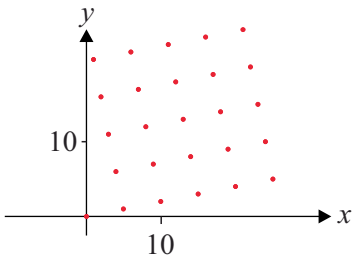
**Opgave 13**

Vi ser nu på kryptosystemet bestemt ved den diskrete sammenhæng $[y]=[5x]$ i $\mathbb{Z}_{26}$.
a) Løs kongruensligningen $[5x]=[1]$ i $\mathbb{Z}_{26}$.

Ud fra løsningen til kongruensligningen i opgave 13 kan man slutte, at dekrypteringen kan udtrykkes ved den diskrete sammenhæng $[y]=[21x]$ i $\mathbb{Z}_{26}$. Vi ser senere (i eksempel 21) på metoden til dette. Vi kan illustrere sammenhængen mellem bogstaverne i klarteksten og det tilhørende bogstav i kryptoteksten ved at tegne graferne for de to diskrete sammenhænge $[y]=[5x]$ og $[y]=[21x]$ i $\mathbb{Z}_{26}$:



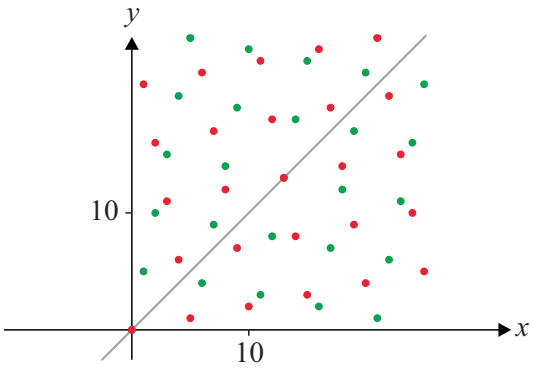

$[y]=[5x]$




$[y]=[21x]$

På det første plot ser vi sammenhængen mellem klartekst og kryptotekst. På det andet plot er udgangspunktet kryptoteksten, så her vil vi finde en sammenhæng mellem kryptotekst og klartekst, således at vi kan kryptere med $[y]=[5x]$ og dekryptere med $[y]=[21x]$ i $\mathbb{Z}_{26}$.

Hvis vi igen vælger at spejle de grønne punkter i linjen med ligningen $y = x$, så får vi netop de røde punkter. Dvs. vi igen kan bestemme grafen for den diskrete sammenhæng for dekrypteringen ved at spejle, som vi kan se på grafen nedenfor.



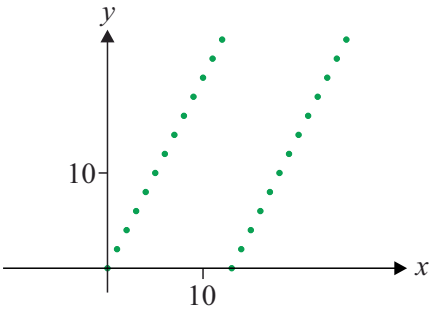

**Eksempel 20** Vi vælger nu at se på et kryptosystem bestemt ved den diskrete sammenhæng $[y] = [2x]$ i $\mathbb{Z}_{26}$.
Tabelrepræsentationen af nøglen bliver:

| **Klartekst** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Klartal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Kryptotal | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 |
| Kryptotekst | A | C | E | G | I | K | M | O | Q | S | U | W | Y |

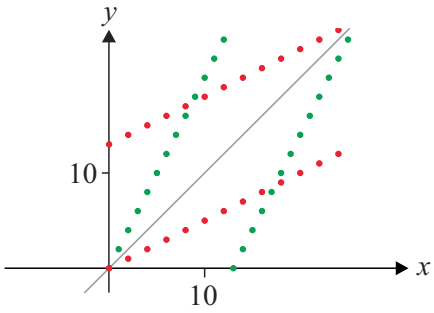
| **Klartekst** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Klartal | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Kryptotal | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 |
| Kryptotekst | A | C | E | G | I | K | M | O | Q | S | U | W | Y |

**Opgave 14**
a) Løs kongruensligningen $[2x] = [1]$ i $\mathbb{Z}_{26}$.
b) Hvad fortæller svaret i a) om en mulig dekryptering?

Vi kan igen tegne grafen for den diskrete sammenhæng $[y] = [2x]$ i $\mathbb{Z}_{26}$ og derefter spejle den i linjen med ligningen $y = x$. Figurerne nedenfor viser dette.




$[y] = [2x]$




De røde punkter på figuren til højre viser, at den diskrete sammenhæng for dekrypteringen ikke er entydig. Dette kan vi fx se ved, der er to prikker over tallet 0. Der findes derfor i dette tilfælde ikke en entydig dekryptering.

**Øvelse 28**

a) Løs kongruensligningen $[a \cdot x] = [1]$ i $\mathbb{Z}_{26}$ for hvert $a \in \{0, 1, 2, \ldots, 25\}$.
b) I hvilke tilfælde har kongruensligningen $[a \cdot x] = [1]$ i $\mathbb{Z}_{26}$ en entydig løsning?
c) For hvilke diskrete sammenhænge $[y] = [a \cdot x]$ i $\mathbb{Z}_{26}$ er der en entydig dekryptering?

Hvis der skal være en entydig dekryptering mellem bogstaverne i kryptoteksten og bogstaverne i klarteksten, (som vi så i tilfældet med $[y] = [5x]$ i $\mathbb{Z}_{26}$, men ikke i tilfældet med $[y] = [2x]$ i $\mathbb{Z}_{26}$), så skal vi kræve, at største fælles divisor mellem 26 og tallet *a*, som vi multiplicerer *x* med, er 1 (Sætning 6).

Generelt ønsker vi et kryptosystem, hvor der til krypteringen ud fra kongruensligningen $[y] = [a \cdot x]$ i $\mathbb{Z}_{26}$ hører en dekrypteringsformel $[x] = [b \cdot y]$ i $\mathbb{Z}_{26}$, hvor $[a] \cdot [b] = [1]$ i $\mathbb{Z}_{26}$ (jævnfør afsnittet "Addition og multiplikation af restklasser").

**Eksempel 21**

Hvis vi som udgangspunkt krypterer med den diskrete sammenhæng $[y] = [15x]$ i $\mathbb{Z}_{26}$, så har vi, at B i klarteksten bliver til 1 som klartal. 1 bliver med den diskrete sammenhæng til 15 som kryptotal, hvilket svarer til P som kryptotekst.
Når vi skal bestemme den omvendte diskrete sammenhæng, så skal vi bestemme en diskret sammenhæng, så vi fra 15 kommer tilbage til 1. Når vi regner med restklasser, så svarer dette til, at vi skal løse ligningen $[15x] = [1]$ i $\mathbb{Z}_{26}$. Vi løser ligningen ved inspektion, dvs. vi skriver restklassen $[1] = \{\ldots, -25, 1, 27, 53, 79, 105, 131, \ldots\}$ i $\mathbb{Z}_{26}$. Vi ser, at 15 går op i $105 = 7 \cdot 15$, hvilket svarer til, at restklassen $[7]$ i $\mathbb{Z}_{26}$ er løsning til ligningen. Den omvendte diskrete sammenhæng er derfor $[x] = [7y]$ i $\mathbb{Z}_{26}$.
Vi kan nu prøve at dekryptere med denne omvendte diskrete sammenhæng. P som kryptotekst svarer til 15 som kryptotal. Multiplicerer vi 15 med 7, så får vi 105, hvilket svarer til 1 i $\mathbb{Z}_{26}$. 1 som klartal svarer til B som klartekst, og vi er tilbage til bogstavet, som vi startede med.

**Opgave 15**

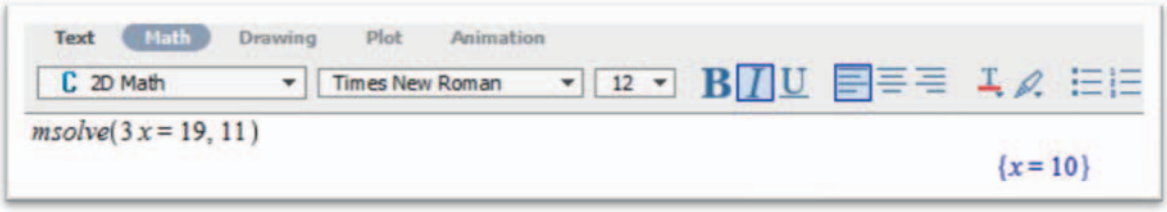
Der er givet en diskret sammenhæng $[y] = [11x]$ i $\mathbb{Z}_{26}$ til at kryptere med.

a) Bestem en omvendt diskret sammenhæng for $[x]$ i $\mathbb{Z}_{26}$ ved at løse en kongruensligning hørende til den diskrete sammenhæng.
b) Bestem en omvendt diskret sammenhæng for $[x]$ i $\mathbb{Z}_{26}$ ved at spejle grafen for den diskrete sammenhæng i linjen med ligningen $y = x$.

# Bilag 1: Talteori i Maple

## Maple og en lineær kongruensligning

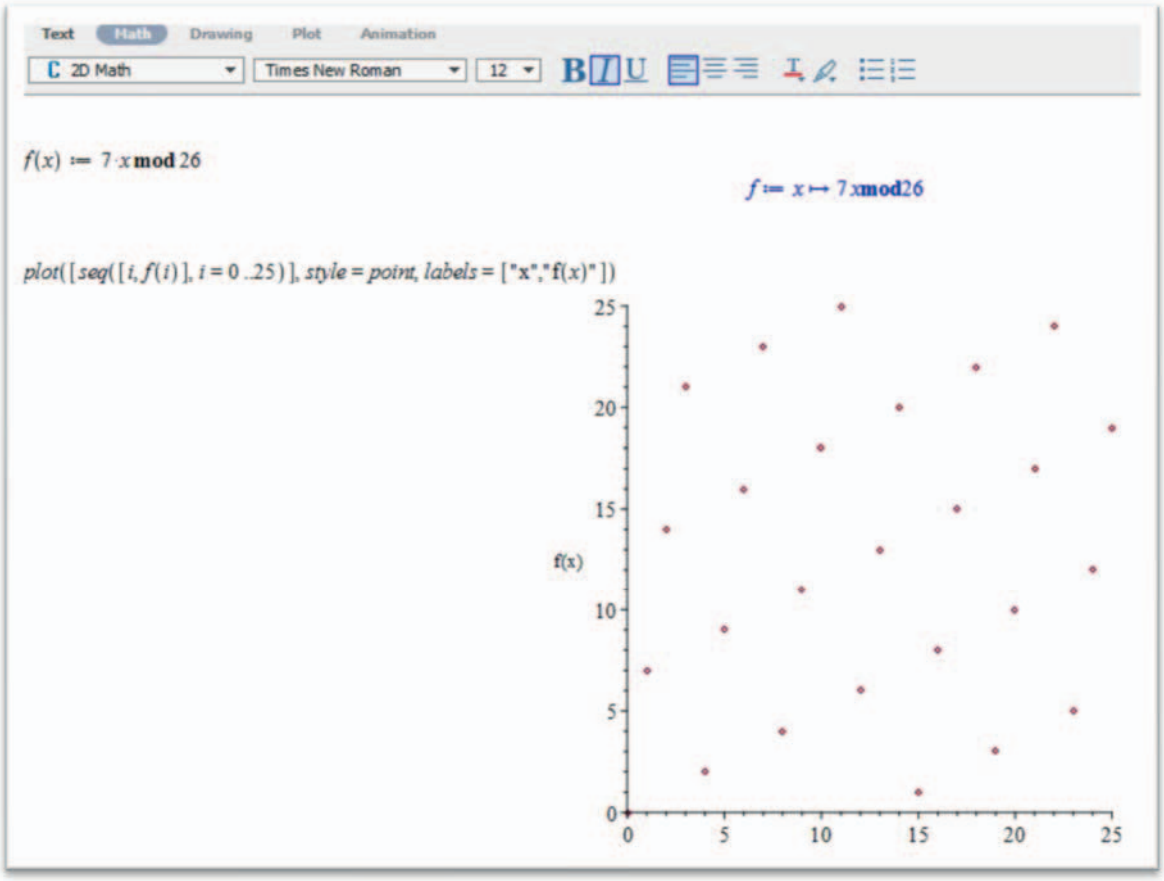
Løsning af den lineære kongruensligning $[3x]=[19]$ i $\mathbb{Z}_{11}$.
Trin 1: Her kan man bruge kommandoen *msolve*.




Konklusion: $[x]=[10]$ i $\mathbb{Z}_{11}$ er løsning.

## Maple og graf for en diskret sammenhæng

Graf for den diskrete sammenhæng $[y]=[7x]$ i $\mathbb{Z}_{26}$.
Trin 1: Definer den diskrete sammenhæng med kommandoen *mod*.
Trin 2: Definer en følge af punkter med kommandoen *seq* i kommandoen *plot*.



# Bilag 2: Talteori i TI-Nspire

## TI-Nspire og en lineær kongruensligning

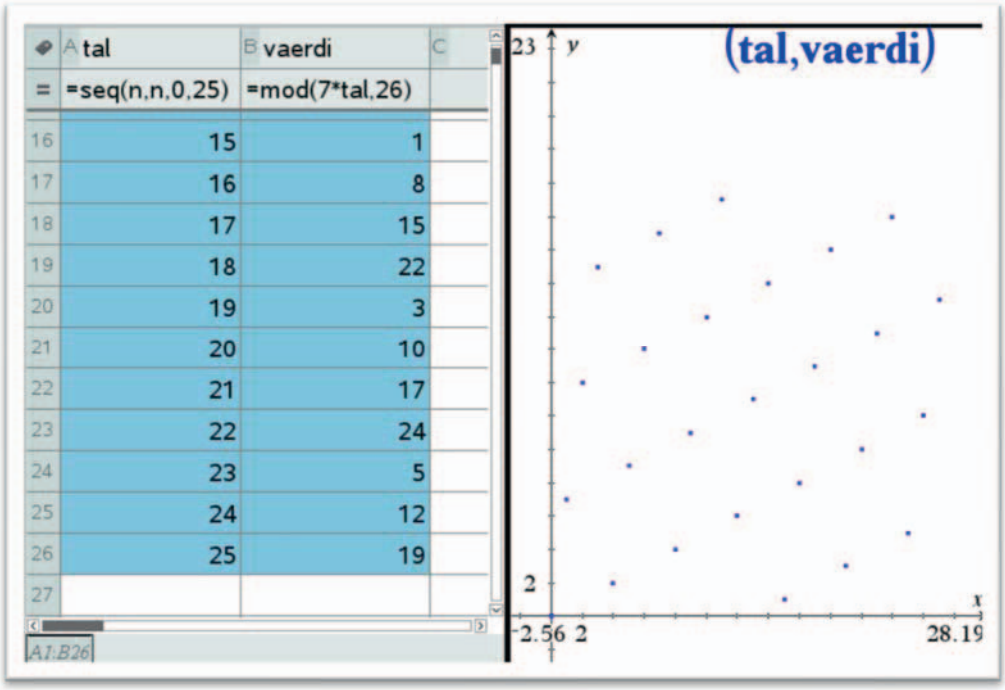
Løsning af den lineære kongruensligning $[3x]=[19]$ i $\mathbb{Z}_{11}$.
Trin 1: Opret en liste af tal fra restklassen $[19]$ i $\mathbb{Z}_{11}$ med i "Lister og regneark" med kommandoen *seq*.

| | A tal |
|---|---|
| = | =seq(19+n*11,n,-2,10) |
| 1 | -3 |
| 2 | 8 |
| 3 | 19 |
| 4 | 30 |
| 5 | 41 |
| 6 | 52 |
| 7 | 63 |
| 8 | 74 |
| 9 | 85 |
| 10 | 96 |
| 11 | 107 |
| 12 | 118 |

Vi ser, at 3 går op i -3, 30, 63, 96, … fra listen af tal med kvotienterne -1, 10, 21, 32, … Dette betyder, at tallene $\{\ldots,-1,10,21,32,\ldots\}$ beskriver den restklasse, der er løsning til kongruensligningen.
Konklusion: $[x]=[10]$ i $\mathbb{Z}_{11}$ er løsning.

## TI-Nspire og graf for en diskret sammenhæng

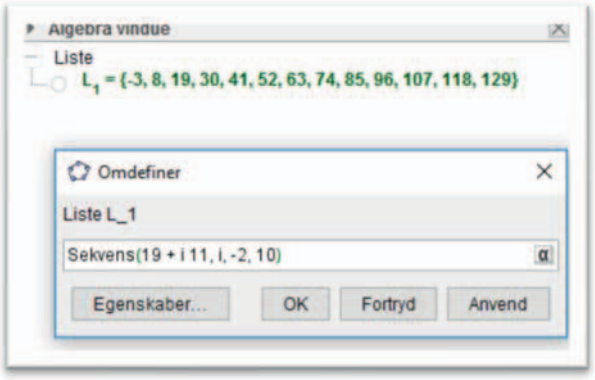
Graf for den diskrete sammenhæng $[y]=[7x]$ i $\mathbb{Z}_{26}$.
Trin 1: Opret to lister i "Lister og regneark". Den ene liste indeholder tallene, som man ønsker at tegne grafen for med kommandoen *seq*. Den anden liste indeholder modulo-værdien af tallene i den første liste.
Trin 2: Opret et punktplot i "Grafer".



# Bilag 3: Talteori i Geogebra

## Geogebra og en lineær kongruensligning

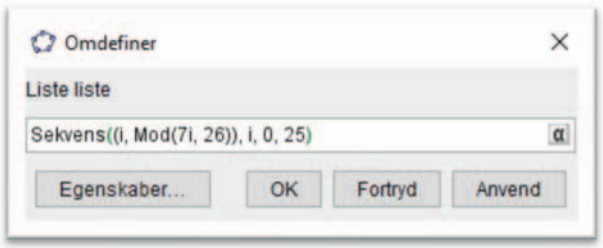
Løsning af den lineære kongruensligning $[3x]=[19]$ i $\mathbb{Z}_{11}$.
Trin 1: Opret en liste af tal fra restklassen $[19]$ i $\mathbb{Z}_{11}$ med kommandoen Sekvens i "Inputlinjen".




Vi ser, at 3 går op i -3, 30, 63, 96, 129, … fra listen af tal med kvotienterne -1, 10, 21, 32, 43, … Dette betyder, at tallene $\{\ldots,-1,10,21,32,43,\ldots\}$ beskriver den restklasse, der er løsning til kongruensligningen.
Konklusion: $[x]=[10]$ i $\mathbb{Z}_{11}$ er løsning.

## Geogebra og graf for en diskret sammenhæng

Graf for den diskrete sammenhæng $[y]=[7x]$ i $\mathbb{Z}_{26}$.
Trin 1: Opret en liste af punkter i "Inputlinjen" med kommandoerne *Sekvens* og *Mod*.




Derefter kommer grafen automatisk frem i "Tegneblokken".