REPETISJON AV DIVISJON MED REST

EKS) A° DELE 57 PA° 6 MED REST

$$57 : 6 = 9$$
$$\underline{54}$$
$$3$$

SA° $57 = 9 \cdot 6 + 3$, HVOR $\underline{q = 9}$ ER KVOSIENTEN OG $\underline{r = 3}$ ER RESTEN.

VIKTIG) FOR ETHVERT HELTALL a OG ETHVERT HELTALL $m \geq 1$ FINNES ET HELTALL Q OG ET HELTALL r MED $0 \leq r \leq m-1$ SLIK AT

$$a = Qm + r$$

EKS) A° DELE 47865 PA° 136 MED REST VED HJELP AV KALKULATOR:

$$47865 / 136 = 351,94...$$

DA ER KVOSIENTEN $\underline{Q = 351}$, SA°

$$\underline{r} = a - Qm = 47865 - 351 \cdot 136$$

$$= 47865 - 47736 \underline{= 129}$$

OPPG) A° DELE 123321 PA° 5581 MED REST VED HJELP AV KALKULATOR.

RESTKLASSER

EKS) DEN 1/1/2009 FALT PÅ EN TORSDAG.

NUMMERER FREMOVER OG BAKOVER SLIK AT 1/1/2009 HAR NUMMER $n=1$, 2/1/2009 HAR NUMMER $n=2$, 31/12/2008 HAR NUMMER $n=0$ OSV.

SPØR VI HVILKE NUMMER n ALLE TORSDAGENE HAR, SÅ ER SVARET

$$n = \ldots, -13, -6, 1, 8, 15, \ldots$$

FORDI

$$1+7=8 \qquad 1-7=-6$$

$$1+2\cdot 7=15 \qquad 1-2\cdot 7=-13$$

$$\vdots \qquad \vdots$$

VI SER AT ALLE NUMRENE TIL TORSDAGEM HAR REST LIK 1 VED DIVISJON MED 7.

PÅ HVILKEN UKEDAG FALLER DAG NUMMER $n=100$?

$$100 = 14\cdot 7 + 2$$

SÅ RESTEN VED DIVISJON AV 100 PÅ 7 ER 2, ALTSÅ PÅ EN FREDAG.

NUMRENE TIL DE SYV UKEDAGENE FALLER I 7 KLASSER

MANDAG : ..., -16, -9, -2, 5, 12, ...

TIRSDAG : ..., -15, -8, -1, 6, 13, ...

ONSDAG : ..., -14, -7, 0, 7, 14, ...

TORSDAG : ..., -13, -6, 1, 8, 15, ...

FREDAG : ..., -12, -5, 2, 9, 16, ...

LØRDAG : ..., -11, -4, 3, 10, 17, ...

SØNDAG : ..., -10, -3, 4, 11, 18, ...

DISSE KLASSENE KALLES <u>RESTKLASSER MODULO 7</u>

DEF) EN <u>RESTKLASSE MODULO</u> m ($m \geq 1$ HELTALL) BESTÅR AV ALLE HELTALLENE SOM HAR SAMME FASTE REST VED DIVISJON MED m

EKS) DET FINNES TO RESTKLASSER MODULO 2 :

REST 0 VED DIVISJON MED 2 (JAMNTALLENE) : ..., -4, -2, 0, 2, 4, ...

REST 1 VED DIVISJON MED 2 (ODDETALLENE) : ..., -3, -1, 1, 3, ...

MERK) FOR FAST REST r OG <u>MODULUS</u> m GIR FORMELEN $a = qm + r$ HELE RESTKLASSEN TIL r MODULO m NÅR q GJENNOMLØPER ALLE HELTALLENE : $q = ..., -2, -1, 0, 1, 2, ...$

EKS) RESTKLASSEN TIL 2 MODULO 3 ER GITT VED FORMELEN

$$a = q \cdot 3 + 2$$

NÅR $q = \ldots, -2, -1, 0, 1, 2, \ldots$, SÅ° DEN ER $a = \ldots, -4, -1, 2, 5, 8, \ldots$

MERK) MODULO m FINNES m FORSKJELLIGE RESTKLASSER, FORDI r ER HELTALL MED $0 \leq r \leq m-1$, OG DERMED KAN TA m FORSKJELLIGE VERDIER I $a = qm + r$.

DEF) ET <u>FULLSTENDIG SYSTEM AV RESTER MODULO</u> m ER ET SETT $a_1, a_2, \ldots, a_m$ AV HELTALL SLIK AT HVER RESTKLASSE MODULO m INNEHOLDER EN OG BARE EN a_k, $1 \leq k \leq m$.

EKS) HELTALLENE 14, 18, 25 ER ET FULLSTENDIG SYSTEM AV RESTER MODULO 3, FOR

$$14 = 4 \cdot 3 + (2)$$

$$18 = 6 \cdot 3 + (0)$$

$$25 = 8 \cdot 3 + (1)$$

SÅ° RESTKLASSEN TIL 0 MODULO 3 INNEHOLDER 18, RESTKLASSEN TIL 1 INNEHOLDER 25 OG RESTKLASSEN TIL 2 INNEHOLDER 14.

KONGRUENSER

EN VIKTIG RELASJON MELLOM HELTALL a OG b MODULO m ER AT BEGGE LIGGER I SAMME RESTKLASSE MODULO m.

EKS) HELTALLENE $a = 43$ OG $b = 64$ LIGGER I SAMME RESTKLASSE MODULO 7. FOR SIDEN

$$43 : 7 = 6 \qquad 64 : 7 = 9$$
$$\underline{42} \qquad\qquad \underline{63}$$
$$1 \qquad\qquad 1$$

LIGGER DE BEGGE I RESTKLASSEN TIL 1 MODULO 7.

EKS) VI KAN SJEKKE OM $a = 43$ OG $b = 64$ LIGGER I SAMME RESTKLASSE MODULO 7 MED MINDRE REGNEARBEID. FOR VI HAR

$$43 = q_1 \cdot 7 + r \quad , \quad 64 = q_2 \cdot 7 + r$$

MED SAMME r, $0 \leq r \leq 6$ (OG UKJENTE q_1, q_2) HVIS OG BARE HVIS 43 OG 64 LIGGER I SAMME RESTKLASSE MODULO 7. MEN DET SKJER HVIS OG BARE HVIS

$$43 - 64 = q_1 \cdot 7 + r - q_2 \cdot 7 - r = (q_1 - q_2) \cdot 7$$

ALTSÅ HVIS $7 \mid (43-64)$. SIDEN $43-64=-21$ OG $7 \mid 21$, SER VI AT 43 OG 64 HAR SAMME REST MODULO 7.

EKS) AVGJØR OM 511 OG 223 LIGGER I SAMME RESTKLASSE MODULO 18.
VI HAR $511-223=288$, OG

$$
\begin{array}{r}
288 : 18 = 16 \\
\underline{18} \\
108 \\
\underline{108} \\
0
\end{array}
$$

SER VI AT $18 \mid 288$, SÅ 511 OG 223 HAR SAMME REST VED DIVISJON MED 18. DETTE VET VI UTEN Å GJØRE DET EKSTRA REGNEARBEIDET SOM ER NØDVENDIG FOR Å FINNE DENNE RESTEN.

MERK) BETINGELSEN FOR AT a OG b LIGGER I SAMME RESTKLASSE MODULO m ER AT

$$a = q_1 m + r \quad , \quad b = q_2 m + r$$

MED SAMME REST r, $0 \leq r \leq m-1$, OG HELTALL q_1, q_2. DET GIR

$$a - b = q_1 m + r - q_2 m - r = (q_1 - q_2) m$$

ALTSÅ AT $a-b$ ER ET MULTIPLUM AV m, DET VIL SI AT $a-b = km$ FOR ET HELTALL k, ELLER AT $a-b$ ER DELELIG MED m.

OPPG) AVGJØR VED HJELP AV KALKULATOR OM 53188 OG 27953 LIGGER I SAMME RESTKLASSE MODULO 315.

DEF) TO HELTALL a OG b ER KONGRUENTE MODULO m, SKRIVES $a \equiv b \pmod{m}$ HVIS $a - b = km$ MED k ET HELTALL.

EKS) VI HAR $418 \equiv 314 \pmod{13}$ FORDI $418 - 314 = 104$ OG $104 = 8 \cdot 13$.

EKS) VI HAR $53188 \not\equiv 27953 \pmod{315}$ VED OPPGAVEN OVENFOR.

MERK) $a \equiv b \pmod{m} \iff m \mid (a-b)$

MERK) $a \equiv b \pmod{m} \iff a$ OG b LIGGER I SAMME RESTKLASSE MODULO m.

EKS) DE TRE RESTKLASSENE MODULO 3 ER GITT VED DE TRE KONGRUENSBETINGELSENE

$a \equiv 0 \pmod{3}$ $\quad a = \ldots, -6, -3, 0, 3, \ldots$

$a \equiv 1 \pmod{3}$ $\quad a = \ldots, -5, -2, 1, 4, 7, \ldots$

$a \equiv 2 \pmod{3}$. $\quad a = \ldots, -4, -1, 2, 5, 8, \ldots$

SATS) HVIS $m \geq 1$ ER HELTALL, SÅ GJELDER

(i) $a \equiv a \pmod m$

(ii) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

(iii) $a \equiv b \pmod m$ & $b \equiv c \pmod m$
$\Rightarrow a \equiv c \pmod m$

FOR a, b, c HELTALL.

BEVIS) (i) $m \mid 0 \Rightarrow m \mid (a-a) \Rightarrow a \equiv a \pmod m$

$a \equiv b \pmod m \Rightarrow$

(ii) $a - b = km \Rightarrow b - a = (-k)m$
$\Rightarrow b \equiv a \pmod m$

$a \equiv b \pmod m$, $b \equiv c \pmod m$ (iii) $(a - b = k_1 m$ & $b - c = k_2 m) \Rightarrow$
$a - b + b - c = k_1 m + k_2 m \Rightarrow$
$a - c = (k_1 + k_2) m \Rightarrow a \equiv c \pmod m$

MERK) KONGRUENSRELASJONEN HAR EGENSKAPENE (i), (ii) OG (iii) FELLES MED LIKHETSRELASJONEN FOR REELLE TALL

(i) $x = x$ (REFLEKSIV)

(ii) $x = y \Rightarrow y = x$ (SYMMETRISK)

(iii) $x = y$ & $y = z \Rightarrow x = z$
(TRANSITIV)

RELASJONER SOM ER REFLEKSIVE, SYMMETRISKE OG TRANSITIVE KALLES <u>EKVIVALENSRELASJONER.</u>

KONGRUENSREGNING

EKS) SIDEN $14 - 2 = 3 \cdot 4$ OG $9 - 1 = 2 \cdot 4$, SÅ ER

$$(14+9) - (2+1) = (14-2) + (9-1)$$

$$= 3 \cdot 4 + 2 \cdot 4 = (3+2) \cdot 4$$

SÅ $14 \equiv 2 \pmod 4$ OG $9 \equiv 1 \pmod 4$ MEDFØRER AT $14+9 \equiv 2+1 \pmod 4$.

SATS) HVIS a, b, c, d OG $m \geq 1$ ER HELTALL, SÅ IMPLISERER $a \equiv b \pmod m$ OG $c \equiv d \pmod m$ AT $a+c \equiv b+d \pmod m$.

BEVIS) ETTER FORUTSETNING ER $a - b = k_1 m$ OG $c - d = k_2 m$ MED k_1 OG k_2 HELTALL. DA FØLGER

$$(a+c) - (b+d) = (a-b) + (c-d)$$

$$= k_1 m + k_2 m = (k_1 + k_2) m$$

MED $k_1 + k_2$ HELTALL, SÅ $a+c \equiv b+d \pmod m$.

MERK) VI VET AT $c \equiv c \pmod m$ FOR ALLE HELTALL, SÅ VED SATSEN OVER IMPLISERER $a \equiv b \pmod m$ AT $a+c \equiv b+c \pmod m$.

EKS) SIDEN $14-2=3\cdot 4$ OG $9-1=2\cdot 4$, SÅ ER

$$14\cdot 9-2\cdot 1=(3\cdot 4+2)\cdot 9-2\cdot 1$$

$$=27\cdot 4+2\cdot(9-1)=27\cdot 4+2\cdot 2\cdot 4$$

$$=(27+4)\cdot 4$$

SÅ $14\equiv 2 \pmod 4$ OG $9\equiv 1 \pmod 4$ MEDFØRER AT $14\cdot 9\equiv 2\cdot 1 \pmod 4$.

SATS) HVIS a, b, c, d OG $m\geq 1$ ER HELTALL, SÅ IMPLISERER $a\equiv b \pmod m$ OG $c\equiv d \pmod m$ AT $ac\equiv bd \pmod m$

BEVIS) ETTER FORUTSETNING ER $a-b=k_1 m$ OG $c-d=k_2 m$. DA FØLGER

$$ac-bd=(b+k_1 m)c-bd$$

$$=ck_1 m+b(c-d)$$

$$=ck_1 m+bk_2 m=(ck_1+bk_2)m$$

MED ck_1+bk_2 HELTALL SIDEN k_1 OG k_2 ER HELTALL. ALTSÅ ER $ac\equiv bd \pmod m$.

MERK) VI VET AT $c\equiv c \pmod m$ FOR ALLE HELTALL, SÅ VED SATSEN OVER IMPLISERER $a\equiv b \pmod m$ AT $ac\equiv bc \pmod m$. ✓

EKS) FORDI $17 \equiv 3 \pmod 7$ SÅ ER
$17 \cdot 17 \equiv 3 \cdot 3 \pmod 7$ OG DERMED

$$17^2 \equiv 3^2 \pmod 7$$

OG PÅ SAMME MÅTE FOR HØYERE POTENSER.

SATS) HVIS $a \equiv b \pmod m$ SÅ ER

$$a^n \equiv b^n \pmod m$$

FOR ALLE POSITIVE HELTALL n.

BEVIS) VED FORRIGE SATS OG MATEMATISK INDUKSJON.

EKS) FINN SISTE SIFFER TIL 7^{64}.
DETTE ER LIK RESTEN TIL 7^{64} MODULO 10, SOM VI KAN FINNE VED KONGRUENSREGNING.
SIDEN $64 = 2^6 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$ KAN VI BRUKE GJENTATT KVADRERING

$$7^2 \equiv 49 \equiv 9 \equiv -1 \pmod{10}$$

$$7^4 \equiv (7^2)^2 \equiv (-1)^2 \equiv 1 \pmod{10}$$

$$7^8 \equiv (7^4)^2 \equiv 1^2 \equiv 1 \pmod{10}$$

$$7^{16} \equiv 1 \pmod{10}, \quad 7^{32} \equiv 1 \pmod{10}$$

$$7^{64} \equiv 1 \pmod{10}$$

SÅ SISTE SIFFER TIL 7^{64} ER $\underline{\underline{1}}$.

OPPG) FINN SISTE SIFFER TIL 536^{1024}.

SATS) HVIS $ca \equiv cb \pmod{m}$ OG $\gcd(c,m) = 1$ SÅ ER $a \equiv b \pmod{m}$.

BEVIS) HVIS $c = 0$ SÅ ER $\gcd(c,m) = m$, OG DA MÅ $m = 1$ ETTER FORUTSETNING. MEN $a \equiv b \pmod{1}$ ER TRIVIELT SANN, SÅ VI KAN ANTA AT $c \neq 0$.
KONGRUENSEN $ca \equiv cb \pmod{m}$ MEDFØRER AT $ca - cb = km$ FOR ET HELTALL k. MEN $c(a-b) = km$ IMPLISERER AT $c \mid km$, OG DA MÅ $c \mid k$ SIDEN $\gcd(c,m) = 1$. ALTSÅ ER $k = ck_1$ FOR ET HELTALL k_1, SÅ $c(a-b) = ck_1 m$. DET GIR $a - b = k_1 m$ VED Å DELE MED $c \neq 0$, DERMED ER $a \equiv b \pmod{m}$.

EKS) UTREGNINGEN

$$(6-1)(6^7 + 6^6 + \cdots + 6 + 1)$$

$$\equiv 6^8 - \cancel{6^7} + \cancel{6^7} - \cancel{6^6} + \cdots + \cancel{6^2} - \cancel{6} + \cancel{6} - 1$$

$$\equiv 6^8 - 1 \equiv (6^2)^4 - 1 \equiv 36^4 - 1$$

$$\equiv 3^4 - 1 \equiv 81 - 1 \equiv 80 \equiv 5 \cdot 16 \pmod{11}$$

VISER AT

$$6^7 + 6^6 + \cdots + 6 + 1 \equiv 16 \pmod{11}$$

SIDEN $\gcd(5, 11) = 1$.

HELTALL PÅ DESIMAL OG BINÆR FORM

SATS) HVIS $a \equiv b \pmod{m}$ OG $d \mid m$, SÅ VIL $a \equiv b \pmod{d}$.

BEVIS) ETTER FORUTSETNING FINNES ET HELTALL k SLIK AT $a - b = km$ OG ET HELTALL ℓ SLIK AT $m = \ell d$. DA ER $a - b = k\ell d$, ALTSÅ ER $a \equiv b \pmod{d}$.

EKS) HELTALLET $N = 4762$ ER UNDERFORSTÅTT Å VÆRE SKREVET PÅ DESIMAL FORM

$$N = 4 \cdot 10^3 + 7 \cdot 10^2 + 6 \cdot 10 + 2 \cdot 1$$

OG VI SER AT $N \equiv 2 \pmod{10}$ SIDEN $10^3 \equiv 10^2 \equiv 10 \equiv 0 \pmod{10}$. VED FOREGÅENDE SATS FØLGER $N \equiv 2 \pmod{5}$ SIDEN $5 \mid 10$. HVIS $5 \mid N$ SÅ ER $N \equiv 0 \pmod{5}$, SOM STRIDER MOT AT $N \equiv 2 \pmod{5}$. VI SLUTTER AT $5 \nmid 4762$.

MERK) DEN VANLIGE TESTEN FOR OM ET HELTALL GITT PÅ DESIMAL FORM ER DELELIG MED 5 KAN ALTSÅ BEGRUNNES VED KONGRUENSREGNING.

VI INNFØRER NOTASJONEN

$$(a_m a_{m-1} \cdots a_1 a_0)_b = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

FOR REPRESENTASJONER MED GRUNNTALL b.

VI SKAL BEGRUNNE EN VELKJENT TEST FOR DELELIGHET MED 9 VED KONGRUENSREGNING.

GITT ET HELTALL

$$N = (a_m a_{m-1} \cdots a_1 a_0)_{10} \qquad 0 \le a_k \le 9$$

PÅ DESIMAL FORM, SÅ KALLES

$$S = a_m + a_{m-1} + \cdots + a_1 + a_0$$

TVERRSUMMEN TIL N.

SATS) HVIS N ER ET POSITIVT HELTALL OG S DETS TVERRSUM, SÅ ER $9 \mid N \Leftrightarrow 9 \mid S$.

BEVIS) VI HAR $10 \equiv 1 \pmod 9$, SÅ $10^k \equiv 1^k \equiv 1 \pmod 9$. DERFOR ER

$$N \equiv a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$$

$$\equiv a_m \cdot 1 + a_{m-1} \cdot 1 + \cdots + a_1 \cdot 1 + a_0$$

$$\equiv S \pmod 9.$$

SIDEN N OG S LIGGER I SAMME RESTKLASSE MODULO 9, SÅ ER DE ENTEN BEGGE DELELIGE MED 9 (HVIS DETTE ER RESTKLASSEN TIL 0), ELLER BEGGE IKKE DELELIGE MED 9.

ET POSITIVT HELTALL N KAN FREMSTILLES PÅ FORMEN

$$N = a_m \cdot b^m + \cdots + a_1 b + a_0$$

MED SIFRE a_k SOM ER HELTALL MED $0 \leq a_k \leq b-1$, OG MED GRUNNTALL $b \geq 2$. HVIS $b=10$ KALLER VI EKSPANSJONEN DESIMAL, HVIS $b=2$ ER DEN BINÆR, HVIS $b=3$ TERNÆR, HVIS $b=16$ HEKSADESIMAL OSV.

DET ER KLART AT a_0 ER RESTEN TIL N VED DIVISJON. MEN DA FØLGER

$$\frac{N-a_0}{b} = a_m b^{m-1} + \cdots + a_2 b + a_1$$

SÅ a_1 ER RESTEN TIL $(N-a_0)/b$ VED DIVISJON MED b, OG SLIK KAN VI FORTSETTE. DETTE GIR EN REGNEMETODE TIL Å FINNE SIFRENE I EN EKSPANSJON AV ET HELTALL N RELATIVT TIL ET GRUNNTALL b.

EKS) VI HAR

$$(17)_{10} = 1 \cdot 16 + 1 = (10001)_2$$

$$(17)_{10} = 1 \cdot 9 + 2 \cdot 3 + 2 \cdot 1 = (122)_3$$

$$(17)_{10} = 1 \cdot 16 + 1 = (11)_{16}$$

EKS) GITT HELTALLET $N = (83)_{10}$ SKAL VI FINNE DETS BINÆRE REPRESENTASJON $N = (a_m \cdots a_1 a_0)_2$. VI FINNER SIFRENE a_k FRA

$$N = a_m \cdot 2^m + \cdots + a_1 \cdot 2 + a_0$$

VED GJENTATT DIVISJON MED 2 MED REST:

$$\begin{aligned}
83 &= 2 \cdot 41 + 1 \quad): \ a_0 = 1 \\
41 &= 2 \cdot 20 + 1 \quad): \ a_1 = 1 \\
20 &= 2 \cdot 10 + 0 \quad): \ a_2 = 0 \\
10 &= 2 \cdot 5 + 0 \quad): \ a_3 = 0 \\
5 &= 2 \cdot 2 + 1 \quad): \ a_4 = 1 \\
2 &= 2 \cdot 1 + 0 \quad): \ a_5 = 0 \\
1 &= 2 \cdot 0 + 1 \quad): \ a_6 = 1
\end{aligned}$$

ALTSÅ ER $(83)_{10} = \underline{\underline{(1\,0\,1\,0\,0\,1\,1)_2}}$.

OPPG) FINN DEN TERNÆRE EKSPANSJONEN $(a_m \cdots a_1 a_0)_3$ TIL 83.

BINÆRE EKSPANSJONER GJØR DET MULIG Å REGNE UT RESTEN r TIL EN POTENS a^n MODULO m EFFEKTIVT VED GJENTATT KVADRERING

$$a^n \equiv r \pmod{m} \qquad 0 \leq r \leq m-1$$

HER KAN r BEREGNES RASKT VED Å SKRIVE n PÅ FORM $n = c_j \cdot 2^j + \cdots + c_1 \cdot 2 + c_0$ OG REGNE UT a^2, $a^4 = (a^2)^2$, ... SUKSESSIVT VED Å KVADRERE FLERE GANGER.

EKS) FINN RESTEN TIL 5^{83} MODULO 11.
VED FORRIGE EKSEMPEL ER

$$5^{83} = 5^{2^6 + 2^4 + 2 + 1} = 5^{2^6} \cdot 5^{2^4} \cdot 5^2 \cdot 5$$

SÅ VED

$$5^2 \equiv 25 \equiv 3 \pmod{11}$$
$$5^4 \equiv (5^2)^2 \equiv 3^2 \equiv 9 \pmod{11}$$
$$5^8 \equiv (5^4)^2 \equiv 9^2 \equiv 81 \equiv 4 \pmod{11}$$
$$5^{16} \equiv (5^8)^2 \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$$
$$5^{32} \equiv (5^{16})^2 \equiv 5^2 \equiv 3 \pmod{11}$$
$$5^{64} \equiv (5^{32})^2 \equiv 3^2 \equiv 9 \pmod{11}$$

FØLGER

$$5^{83} \equiv 5^{64} \cdot 5^{16} \cdot 5^2 \cdot 5$$

$$\equiv 9 \cdot 5 \cdot 3 \cdot 5 \equiv 45 \cdot 15 \equiv \underline{4} \pmod{11}$$

LINEÆRE KONGRUENSLIKNINGER

EKS) LØS KONGRUENSLIKNINGEN

$$3x \equiv 2 \pmod{11}$$

FOR DEN UKJENTE x MODULO 11.
FOR HVERT HELTALL x SLIK AT KONGRUENSE
OPPFYLLES, MÅ DET FINNES ET
HELTALL y SLIK AT

$$3x - 2 = 11y$$

DETTE ER EN LINEÆR DIOFANTISK
LIKNING SOM KAN LØSES VED EN
STANDARD TEKNIKK (EUKLIDS ALGORITME):

$$11 = 3 \cdot 3 + 2 \quad , \quad 3 = 1 \cdot 2 + 1$$

DERMED

$$1 = 3 - 2 = 3 - (11 - 3 \cdot 3) = 4 \cdot 3 - 11$$

MULTIPLISER MED 2 SÅ FØLGER

$$2 = 8 \cdot 3 - 2 \cdot 11 \quad): \quad 3 \cdot 8 - 2 = 11 \cdot 2$$

OG DA ER $x_0 = 8$ OG $y_0 = 2$ EN
PARTIKULÆR LØSNING. SIDEN $\gcd(3, 11) = 1$
ER ALLE LØSNINGENE GITT VED

$$x = 8 - 11t \quad , \quad y = 2 - 3t$$

NÅR t GJENNOMLØPER ALLE HELTALLENE

VI FÅR ALTSÅ UENDELIG MANGE HELTALLSLØSNINGER

$$x = 8 - 11t \quad , \quad t = \ldots, -2, -1, 0, 1, 2, \ldots$$

TIL KONGRUENSEN $3x \equiv 2 \pmod{11}$, MEN MERK AT

$$x \equiv 8 - 11t \equiv 8 \pmod{11}$$

SÅ OPP TIL KONGRUENS MODULO 11 ER DET BARE ÉN LØSNING. DENNE LØSNINGEN SKRIVER VI $x \equiv 8 \pmod{11}$

MERK) LØSNINGER TIL EN KONGRUENSLIKNING

(*) $ax \equiv b \pmod{11}$

REGNES BARE SOM FORSKJELLIGE HVIS DE ER INKONGRUENTE MODULO m.
SAGT PÅ EN ANNEN MÅTE SÅ ER LØSNINGENE TIL EN KONGRUENSLIKNING HELE RESTKLASSER MODULO m.
SPESIELT KAN KONGRUENSLIKNINGEN (*) HØYST HA m LØSNINGER MODULO m.

EKS) KONGRUENSLIKNINGEN $3x \equiv 2 \pmod{11}$ KAN OGSÅ LØSES VED INSPEKSJON:

$$x \equiv 12x \equiv 4 \cdot 3 \cdot x \equiv 4 \cdot 2 \equiv 8 \pmod{11}$$

ENHVER KONGRUENSLIKNING

$$ax \equiv b \pmod{m}$$

KAN SKRIVES OM TIL EN LINEÆR DIOFANTINSK LIKNING

$$(*) \qquad ax - b = my.$$

PÅ DEN ENE SIDEN GIR DETTE EN LØSNINGSMETODE, SIDEN VI ALLEREDE VET HVORDAN VI SKAL LØSE (*). PÅ DEN ANNEN SIDE LEDER TEORIEN FOR LINEÆRE DIOFANTISKE LIKNINGER TIL TEORETISK INNSIKT OM LINEÆRE KONGRUENSLIKNINGER.

SATS) GITT EN LINEÆR KONGRUENSLIKNING $ax \equiv b \pmod{m}$, SETT $d = \gcd(a, m)$. HVIS $d \nmid b$ SÅ HAR KONGRUENSEN INGEN LØSNINGER, HVIS $d \mid b$ SÅ HAR KONGRUENSEN d LØSNINGER MODULO m.

BEVIS) SE LÆREBOKA.

EKS) KONGRUENSLIKNINGEN $6x \equiv 5 \pmod{4}$ HAR INGEN LØSNING, SIDEN $d = \gcd(6, 4) = 2$ OG $2 \nmid 5$. DETTE KAN VI OGSÅ SE DIREKTE, FOR $6x$ MÅ VÆRE JAMN, MEN 5 ER ODDE, SÅ $6x - 5$ MÅ VÆRE ODDE, OG ET ODDETALL ER IKKE DELELIG MED 4

EKS) VI SKAL LØSE KONGRUENSLIKNINGEN

$$15x \equiv 6 \pmod{21} \iff 15x - 6 = 21y$$

SIDEN $d = \gcd(15, 21) = 3$ OG $3 \mid 6$, SÅ HAR KONGRUENSLIKNINGEN 3 INKONGRUENTE LØSNINGER MODULO 21.

SIDEN $21 = 1 \cdot 15 + 6$, $15 = 2 \cdot 6 + 3$, SÅ ER $3 = 15 - 2 \cdot 6 = 15 - 2(21 - 15) = 3 \cdot 15 - 2 \cdot 21$. MULTIPLIKASJON MED 2 GIR

$$15 \cdot 6 - 6 = 21 \cdot 4$$

SÅ

$$\left.\begin{aligned} x &= 6 - \frac{21}{3}t = 6 - 7t \\ y &= 4 - \frac{15}{3}t = 4 - 5t \end{aligned}\right\} \quad t \text{ VILKÅRLIG HELTALL}$$

ER LØSNINGENE TIL DEN DIOFANTINSKE LIKNINGEN $15x - 6 = 21y$.

SETTER VI $t = 3s$, $t = 3s + 1$, $t = 3s + 2$ I UTTRYKKET FOR x OVER, SÅ FÅR VI

$$x = 6 - 21s$$

$$x = 6 - 21s - 7 = -1 - 21s$$

$$x = 6 - 21s - 14 = -8 - 21s$$

OG DERMED ER $\underline{\underline{x \equiv 6, -1, -8 \pmod{21}}}$ DE TRE PARVIS INKONGRUENTE LØSNINGEN TIL KONGRUENSLIKNINGEN.

DET KINESISKE RESTTEOREMET

EKS) LØS DE TO SIMULTANE KONGRUENSLIKNINGENE

$$\text{I}: \quad x \equiv 2 \pmod 5$$

$$\text{II}: \quad x \equiv 3 \pmod 7$$

FRA I FØLGER $x - 2 = 5y$, SÅ
$x = 2 + 5y$ OG INNSETTING I II GIR

$$2 + 5y \equiv 3 \pmod 7 \iff 5y \equiv 1 \pmod 7.$$

MERK AT $d = \gcd(5,7) = 1$, SÅ DEN SISTE KONGRUENSLIKNINGEN HAR ÉN LØSNING MODULO 7. DA $5 \cdot 3 \equiv 15 \equiv 1 \pmod 7$ ER $y \equiv 3 \pmod 7$ DENNE LØSNINGEN.

SETT $y_0 = 3$ OG $x_0 = 2 + 5y_0$. AT $x_0 \equiv 2 + 5y_0 \equiv 2 \pmod 5$ ER INNLYSENDE, OG $x_0 \equiv 2 + 5y_0 \equiv 3 \pmod 7$ FØLGER AV UTREGNINGEN OVER. DERFOR ER $x_0 = 2 + 5y_0 = 2 + 5 \cdot 3 = 17$ EN LØSNING TIL I OG II. FORDI $5 \mid 35$ OG $7 \mid 35$ $(35 = 5 \cdot 7)$ ER $\underline{\underline{x \equiv 17 \pmod{35}}}$ EN LØSNING TIL I OG II MODULO 35.

HVIS x_1 ER EN LØSNING TIL I OG II MODULO 35 SÅ ER $x_1 \equiv 2 \equiv 17 \pmod 5$ OG $x_1 \equiv 3 \equiv 17 \pmod 7$, SÅ $5 \mid (x_1 - 17)$ OG $7 \mid (x_1 - 17)$. MEN $\gcd(5,7) = 1$ SÅ DA MÅ $5 \cdot 7 \mid (x_1 - 17)$, ALTSÅ $x_1 \equiv 17 \pmod{35}$. DERFOR ER LØSNINGEN $x \equiv 17 \pmod{35}$ TIL I OG II UNIK MODULO 35.

EKS) VI ILLUSTRERER FOREGÅENDE EKSEMPEL VED Å SKRIVE UT LØSNINGENE TIL $x \equiv 2 \pmod 5$ MODULO $5 \cdot 7 = 35$, OG TESTER HVER AV DISSE MOT KONGRUENSLIKNINGEN $x \equiv 3 \pmod 7$:

$x \equiv 2 \pmod{35}$	$2 \not\equiv 3 \pmod 7$
$x \equiv 7 \pmod{35}$	$7 \not\equiv 3 \pmod 7$
$x \equiv 12 \pmod{35}$	$12 \not\equiv 3 \pmod 7$
$x \equiv 17 \pmod{35}$	$17 \equiv 3 \pmod 7$ ✓
$x \equiv 22 \pmod{35}$	$22 \not\equiv 3 \pmod 7$
$x \equiv 27 \pmod{35}$	$27 \not\equiv 3 \pmod 7$
$x \equiv 32 \pmod{35}$	$32 \not\equiv 3 \pmod 7$

VI SER UMIDDELBART AT $x \equiv 17 \pmod{35}$ ER ENESTE LØSNING MODULO 35.

DET KINESISKE RESTTEOREMET

GITT $a_1, a_2, \cdots, a_\ell$ HELTALL OG $m_1, m_2, \cdots, m_\ell$ POSITIVE HELTALL MED $\gcd(m_i, m_j) = 1$ FOR $1 \le i < j \le \ell$. DA HAR SYSTEMET

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_\ell \pmod{m_\ell} \end{aligned}$$

AV KONGRUENSLIKNINGER EN UNIK SIMULTAN LØSNING MODULO $m_1 m_2 \cdots m_\ell$

BEVIS) SE LÆREBOKA.

EKS) LØS SYSTEMET

$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$
$$x \equiv -1 \pmod{11}$$

AV KONGRUENSLIKNINGER.

VI VET ALLEREDE AT $x \equiv 17 \pmod{35}$ ER DEN UNIKE SIMULTANE LØSNINGEN TIL DE TO FØRSTE KONGRUENSLIKNINGENE. SÅ $x - 17 = 35y$ OG INNSETTING I DEN TREDJE KONGRUENSLIKNINGEN GIR

$$17 + 35y \equiv -1 \pmod{11} \iff 35y \equiv -18 \pmod{11}$$
$$\iff 2y \equiv 4 \pmod{11}$$
$$\iff y \equiv 2 \pmod{11}$$

VELGER VI $y_0 = 2$ SÅ ER $x_0 = 17 + 35y_0 = 8$
EN FELLES LØSNING TIL ALLE TRE KONGRUENSLIKNINGENE. FORDI $5 \cdot 7 \cdot 11 = 385$ SÅ FØLGER VED DET KINESISKE RESTTEOREMET AT $\underline{\underline{x \equiv 87 \pmod{385}}}$ ER DEN UNIKE FELLES LØSNINGEN.

$x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$ $\Rightarrow$ $x \equiv 17 \pmod{35}$

$x \equiv 17 \pmod{35}$, $x \equiv -1 \pmod{11}$ $\Rightarrow$ $x \equiv 87 \pmod{385}$

VI SKAL GÅ GJENNOM EN MER EFFEKTIV METODE FOR Å LØSE ET SETT

(*) $x \equiv a_1 \pmod{n_1}, \cdots, x \equiv a_r \pmod{n_r}$

AV KONGRUENSLIKNINGER MED $\gcd(n_i, n_j) = 1$ FOR $i \neq j$.

DEFINER $n = n_1 n_2 \cdots n_r$ OG

$$N_1 = \frac{n}{n_1}, \cdots, N_r = \frac{n}{n_r}$$

FINN DERETTER $x_1, \ldots, x_r$ MED

$$N_1 x_1 \equiv 1 \pmod{n_1}, \cdots, N_r x_r \equiv 1 \pmod{n_r}.$$

DA ER $x \equiv \bar{x} \pmod{n}$ MED

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r$$

DEN UNIKE FELLES LØSNINGEN TIL (*) MODULO n.

BEGRUNNELSEN FOR AT DENNE METODEN VIRKER FINNES I BEVISET FOR DET KINESISKE RESTTEOREMET PÅ SIDE 79 I LÆREBOKA.

EKS) VI LØSER

(*) $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$, $x \equiv -1 \pmod{11}$

ENDA EN GANG.

HER ER $a_1 = 2$, $a_2 = 3$, $a_3 = -1$ OG
$n_1 = 5$, $n_2 = 7$, $n_3 = 11$. DET GIR
$n = n_1 n_2 n_3 = 5 \cdot 7 \cdot 11 = 385$ OG
$N_1 = n/n_1 = 77$, $N_2 = n/n_2 = 55$,
$N_3 = n/n_3 = 35$. VI FINNER HELTALL
x_1, x_2, x_3 SLIK AT

$N_1 x_1 \equiv 1 \pmod{n_1}$): $77x_1 \equiv 1 \pmod 5$
$\Leftrightarrow$ $2x_1 \equiv 1 \pmod 5$
): $x_1 = 3$ (F. EKS.)

$N_2 x_2 \equiv 1 \pmod{n_2}$): $55x_2 \equiv 1 \pmod 7$
$\Leftrightarrow$ $6x_2 \equiv 1 \pmod 7$
): $x_2 = -1$ (F. EKS.)

$N_3 x_3 \equiv 1 \pmod{n_3}$): $35x_3 \equiv 1 \pmod{11}$
$\Leftrightarrow$ $2x_3 \equiv 1 \pmod{11}$
): $x_3 = 6$ (F. EKS.)

DET GIR

$$\bar{x} = 2 \cdot 77 \cdot 3 + 3 \cdot 55 \cdot (-1) + (-1) \cdot 35 \cdot 6 = 87$$

SÅ $\underline{x \equiv 87 \pmod{385}}$ ER DEN UNIKE LØSNINGEN TIL (*) MODULO 385.