2011-(01)jan-25: dag 4

Sist:

Sats: Om m, n är heltal (båda $\neq 0$) existera $\mathrm{sgd}(m; n)$ entydligt och är $am + bn$, några heltal a, b.

Euklides' algoritm:

($\mathrm{sgd}(m; n) = \mathrm{sgd}(n; m - qn)$ upprepat $\mathrm{sgd}(d; 0) = d$)

Tag $m \geq n \geq 0$

$$
\begin{array}{ll}
m = q_1 n + r_1 & 0 \leq r_1 < n \\
n = q_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 \leq r_3 < r_2 \\
r_2 = q_4 r_3 + r_4 & 0 \leq r_4 < r_3 \\
\quad\vdots & \quad\vdots
\end{array}
$$

$$
\begin{array}{ll}
r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} & \\
r_{k-2} = q_k r_{k-1} + \mathbf{0} & \text{(slutar allt med } \mathbf{0}\text{)}
\end{array}
$$

$r_{k-1} = \mathrm{sgd}(m; n)$

$r_{k-1} = r_{k-3} - q_{k-1} r_{k-2} = \ldots$

Följdsats: Om $d|mn$ och $\underbrace{\mathrm{sgd}(d; m) = 1}_{d,\, m \text{ relativt prima}}$ så $d|n$

↑

d, m relativt prima

För alla heltal k, m, n:

$m|m$, $k|n$, $m|n \Rightarrow k|n$

Definition: Om m, n är heltal så är en minsta gemensamma multipel, mgm (en. lcm) för m, n ett heltal g sådant att

i) $m, n \mid g$
ii) $m, n \mid n \Rightarrow g|h$
iii) $g \geq 0$

Sats: Om m, n är heltal existerar mgm(m; n) entydigt och uppfyller mgm(m; n) · sgd(m; n) = mn

(mgm(0; 0) = 0)

Sats: Den linjära diofantiska ekvationen (heltalslösningar sökes)

mx + ny = 1

har lösningar omm sgd(m; n) | c.

Om sgd(m; n) = am + bn, a, b heltal ges alla lösningar av

$$\begin{cases} x = a\dfrac{c}{d} + q\dfrac{n}{d} \\ y = b\dfrac{c}{d} - q\dfrac{m}{d} \end{cases} \qquad q \text{ heltal}$$

Defintion: Ett prital är ett heltal p > 1 som bara har delarna ±1 och ±p.

Exempel: 2, 3, 17, 101, 123449

Aritmetikens fundamentalsats:

Varje heltal ≥ 1 kan på ett entydigt (bortsätt från ordningen) sätt skrivas som en produkt av primtal

$$\operatorname{sgd}\left(p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k};\; p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}\right) = p_1^{\min(s_1;\, t_1)} p_2^{\min(s_2;\, t_2)} \cdots p_k^{\min(s_k;\, t_k)}$$

Likadant för mgm, fast max istället för min.

Så sgd(m; n) · mgm(m; n) = mn.

Euklides: Det finns oändligt många primtal.

$$\left(\text{Det gäller att } \sum_{p \in \mathbb{P}} \frac{1}{p} = \infty\right)$$

Idag:

Modulär aritmetik, $\mathbb{Z}_m$

Räkna med rester (mod m)

+- och ×-tabeller i $\mathbb{Z}_m$

Inverterabara (invertabla) element i $\mathbb{Z}_m$

Linjära ekvationer

$ax + b$ i $\mathbb{Z}_m$

Lite mängdlära

$\{x \mid \dots\dots\}$

$a \in A$, $A \subseteq B$

$|A|$, $A \cup B$, $A \cap B$, $A \setminus B$, A^c, $\mathcal{P}(A)$

Räkneregler för $\cap, \cup, ^c, \emptyset, \mathcal{U}$

$|A \cup B| = |A| + |B| - |A \cap B|$

Produktmängden $A \times B$

Idag, först, om modulär aritmetik

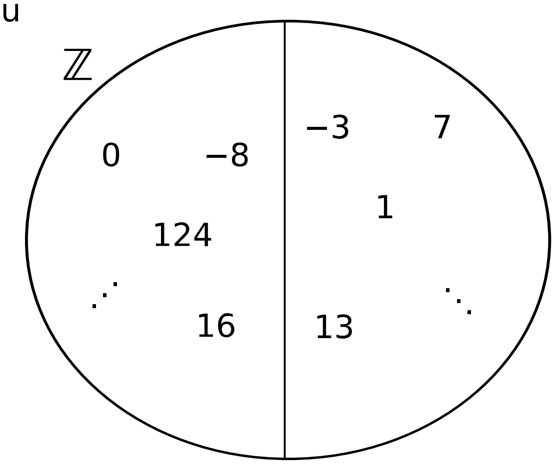
Minns "räknereglerna" för jämna (j) och udda (u) tal

j + j = j, j + u = u, u + j = u, u + u = j

j · j = j, j · u = j, u · j = j, u · u = u

+	j	u
j	j	u
u	u	j

·	j	u
j	j	j
u	j	u



Allmänt med $m \geq 2$ heltal.

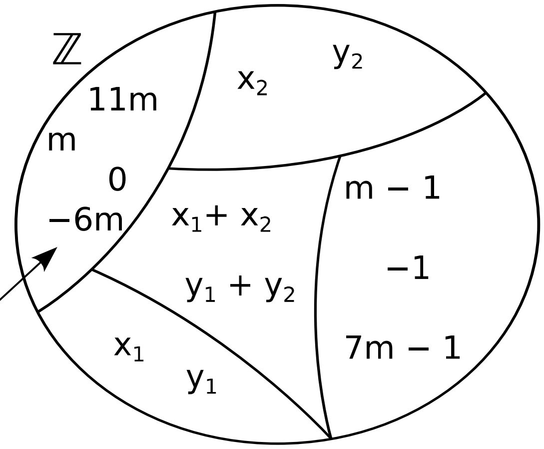
Att räkna <u>modulo m</u>

$x \equiv y \pmod{m} \overset{\text{def}}{\Leftrightarrow} m \mid (x - y)$

$\uparrow$

eller $x \equiv_m y$

"kongruenta modulo m "



Resten 0 vid ÷ med m

x och y ger samma rest vid division med m.

Då: $x_1 \equiv_m y_1,\ x_2 \equiv_m y_2 \Rightarrow x_1 + x_2 \equiv_m y_1 + y_2$

$x_1 \cdot x_2 \equiv_m y_1 \cdot y_2$

$qm + r_1 \equiv_m q'm + r_1$

Man skriver ofta = (istället för ≡) och säger att man räknar
i $\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$

Tabeller i $\mathbb{Z}_m$

$\mathbb{Z}_3$

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

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Exempel:

Vad blir (principala) resten då 67^{380} divideras med 31?

Det vill säga ved är 67^{380} mod 31?

$$67^{380} \equiv_{31} (67 \bmod 31)^{380} = 5^{380} = 5^{3\cdot 126 + 2} = 125^{126} \cdot 5^2 \equiv$$

$$\{125 = 4\cdot 31 + 1 \equiv_{31} 1\} \equiv_{31} 1^{126} \cdot 25 = 1 \cdot 25 = \underline{25}$$

$$5^{380} = \underbrace{(((\cdots((}_{\times 8} 1\cdot\overset{1}{5})^2\cdot\overset{0}{1})^2\cdot\underbrace{\overset{1}{5})^2\cdots\overset{1}{5}}_{\times 5})^2\cdot\overset{0}{1})^2\cdot\overset{0}{1}$$

Allt räknat modulo 31

ty $\quad 380 = 101111100_2$

De flesta räknereglerna i $\mathbb{Z}_m$ är samma som i $\mathbb{Z}$,
men man kan ha $x\cdot y = 0$ i $\mathbb{Z}_m$ fast $x, y \neq 0$ i $\mathbb{Z}_m$.
Till exempel $3\cdot 4 = 0$ i $\mathbb{Z}_6$.

Definition: r i $\mathbb{Z}_m$ är invertabel om det finns x i $\mathbb{Z}_m$ så att $r_x = 1$ i $\mathbb{Z}_m$, $x = r^{-1}$.

Exempel: I $\mathbb{Z}_4$ är 1 och 3 invertabla, men inte 0 och 2.

$1^{-1} = 1 \qquad 3^{-1} = 3 \qquad$ ty $\quad 1\cdot 1 = 1$ och $3\cdot 3 = 9 = 1$

$3x = 2 \qquad$ i $\mathbb{Z}_4$

ger $\quad 3\cdot 3x = 3\cdot 2 = 2 \qquad$ i $\mathbb{Z}_4$

Sats: r i $\mathbb{Z}_m$ är invertabel omm $\mathrm{sgd}(r; m) = 1$.

ty: r är invertabel i $\mathbb{Z}_m \Leftrightarrow rx \equiv_m 1$,
något x i $\mathbb{Z} \Leftrightarrow rx - 1 = km$,
några x, k i $\mathbb{Z} \Leftrightarrow rx - km = 1$,
några $x, k \Leftrightarrow \mathrm{sgd}(r; m) = 1$.

Så i $\mathbb{Z}_p$, $p \in \mathbb{P}$, är alla utom 0 invertabla.

Exempel: Vad är 11^{-1} i $\mathbb{Z}_{32}$?

Vi ser att $11 \cdot 3 = 33 \equiv_{32} 1$, så $11^{-1} = 3$. $\left(\text{“}\ \frac{1}{11} = 3\ \text{”}\right)$

$11x = 7$ i $\mathbb{Z}_{32}$ har lösningen $x = 3 \cdot 7 = 21$ i $\mathbb{Z}_{32}$.

$11x = 26$ i $\mathbb{Z}_{32}$ har lösningen $x = 3 \cdot 26 = 14$ i $\mathbb{Z}_{32}$.

Exempel: Bestäm 11^{-1} i $\mathbb{Z}_{47}$

$\mathrm{sgd}(11; 47) = 1$, så 11^{-1} existerar. Vad är den?

Euklides' algoritm:

$$47 = 4 \cdot 11 + 3$$
$$11 = 3 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$$1 = 3 - 2 = 3 - (11 - 3 \cdot 3) = -11 + 4 \cdot 3 =$$
$$= -11 + 4(47 - 4 \cdot 11) = 4 \cdot 47 - 17 \cdot 11 =$$
$$= 4 \cdot 47 - 11 \cdot 47 + 47 \cdot 11 - 17 \cdot 11 =$$
$$= -7 \cdot 47 + 30 \cdot 11$$

så $11 \cdot 30 = 1$ i $\mathbb{Z}_{47}$.

$11^{-1} = 30$ i $\mathbb{Z}_{47}$.

(Alternativt: $11^{-1} = -17 = 30$ i $\mathbb{Z}_{47}$)

Den linjära ekvationen

$ax = b$ i $\mathbb{Z}_m$ $\quad$ ($ax \equiv b \pmod{m}$)

Ekvationen är ekvivalent med den diofantiska ekvationen

$$a\underline{x} - \underline{k}m = b$$

så lösningar finns omm $\mathrm{sgd}(a; m) | b$.

Exempel:

Lös $5x \equiv 4 \pmod{11}$

Euklides':

$$11 = 2\cdot5 + 1$$
$$1 = 11 - 2\cdot5$$

Så $4 = 4\cdot11 - 5\cdot8 = 4\cdot11 - 5\cdot11 + 11\cdot5 - 8\cdot5 = -11 + 3\cdot5$.

Och allmän lösning: $\quad x = 3 + q\cdot11,\ q \in \mathbb{Z}$

Entydig lösning i $\mathbb{Z}_{11}$, ty $\mathrm{sgd}(5; 11) = 1$

Alternativt:

$$5x \equiv_{11} 4 \Leftrightarrow 2 \cdot 5x \equiv_{11} 2\cdot4 \Leftrightarrow -x \equiv_{11} 8 \Leftrightarrow x \equiv_{11} 3$$

$\Leftarrow$: $\mathrm{sgd}(2; 11) = 1$

Exempel:

Lös $5x \equiv_{15} 7$

Inga lösningar, ty $\mathrm{sgd}(5; 15) = 5 \nmid 7$.

($15 \nmid 5x - 7$, ty $5 \nmid 5x - 7$)

Exempel:

Lös $5x \equiv_{15} 10$

Lösbar ty sgd(5; 15) = 5 | 10

$5x - k \cdot 15 = 10 \Leftrightarrow x - 3k = 2 \Leftrightarrow x = 3k + 2, \quad k \in \mathbb{Z}$

Allmänt:

d = sgd(a; m)

$$\frac{a}{d} x \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{m}{d} \right)$$

Exempel:

Lös $\begin{cases} 2x + 3y = 2 \\ 4x + 2y = 1 \end{cases}$ i $\mathbb{Z}_5$ (5 (i $\mathbb{Z}_5$) är primtal så alla utom 0 är invertabla.)

Som vanligt:

$$\left(\begin{array}{cc|c} 2 & 3 & 2 \\ 4 & 2 & 1 \end{array}\right) \overbrace{r2 - 3 \cdot r1} \left(\begin{array}{cc|c} 2 & 3 & 2 \\ 0 & 1 & 2 \end{array}\right) \overbrace{r1 - 2 \cdot r2} \left(\begin{array}{cc|c} 2 & 0 & 1 \\ 0 & 1 & 2 \end{array}\right) \overbrace{3 \cdot r1} \left(\begin{array}{cc|c} 1 & 0 & 3 \\ 0 & 1 & 2 \end{array}\right)$$

så $\begin{cases} x = 3 \\ y = 2 \end{cases}$ i $\mathbb{Z}_5$.

Notera: Om sgd(m; n) = 1

$a \equiv b \pmod{mn} \Leftrightarrow \begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$

ty: $\Rightarrow$: $mn | \underbrace{n - b}_{=hmn} \Rightarrow m, n | \underbrace{a - b}_{(hn)m - (hm)n}$

$\Leftarrow$: m, n | a − b ⇒ a − b = km och
n | km ⇒ a − b = km och
n | k = qn, det vill säga
a − b = qmn.

Lite mängdlära (matematikens språk) (2 kap.)

Vi kan tänka på mängder som “påsar” med (pekare till) “saker” (element).

Exempel: $A = \{\text{Kalle, Olla, Lisa}\}$ (Kalle, Olla, Lisa är mängdes element.)

$B = \{\sqrt{2}, c, -7, i\}$

$C = \{n \mid n \text{ är ett heltal och } n^2 \equiv_4 1\} =$ $(n \equiv_2 1)$
$= \{\text{udda heltal}\}$

$\{\cdot \mid \cdots\}$ “mängdbyggaren”

$\emptyset = \{x \mid x \neq x\} = \{\}$ Den tomma mängden

Två mängder är lika omm de innehåller samma element.

$\{\emptyset\}$ är inte $\emptyset$, utan en mängd som innehåller $\emptyset$.

Standardbeteckningar:

$\mathbb{Z}$	$= \{0, \pm 1, \pm 2, \ldots\}$	heltalen
$\mathbb{N}$	$= \{\mathbf{0}, 1, 2, \ldots\}$	de naturliga talen
$\mathbb{Z}_+$	$= \{\mathbf{1}, 2, \ldots\}$	($\mathbb{Z}^+$ används också)
$\mathbb{Q}$	$= \{n \div m \mid m, n \in \mathbb{Z}, n \neq 0\}$	rationella talen
$\mathbb{R}$	reella talen	
$\mathbb{C}$	complexa talen	
$\mathbb{Z}_m$	$= \{0, 1, 2, \ldots, m-1\}$	