2011-(01)jan-17: dag 2

Aritmetikens fundamentalsats

Alla positiva heltal (större än 1) kan faktoriseras
till en unik mängd av (icke-unika) primtal.

Diofantiska ekvationer

Endast heltalslösningar.

Euklides' algoritm

Ger största gemensamma delaren.

Lemma:

Om $d|a$ (d delar a) och $d|b$ så $d|(na + mb)$ för alla hela tal n och m.

Bevis:

$d|a$ innebär att $a = kd$
$d|b$ innebär att $b = k'd$

Då gäller:

$$na + mb = nkd + mk'd = d(nk + mk') = dp, \quad p \in \mathbb{Z}$$

Exempel:

Bestäm sgd(217; 314)
↑
största gemensamma delare

Lösning:

Med hjälp av Euklides' algoritm

$314 = 1 \cdot \underline{217} + \underline{\underline{97}}$
$\underline{217} = 2 \cdot \underline{\underline{97}} + \underline{23}$
$\underline{\underline{97}} = 4 \cdot \underline{23} + 5$
$\underline{23} = 5 \cdot 5 - 2$ eller $23 = 4 \cdot 5 + 3$
$5 = 2 \cdot 2 + \boldsymbol{1}$ $\quad 5 = 1 \cdot 3 + 2$
$2 = 2 \cdot 1 + \mathbf{0}$ $\quad 3 = 1 \cdot 2 + \boldsymbol{1}$
$2 = 2 \cdot 1 + \mathbf{0}$

Alltså $1 = \text{sgd}(314; 217)$

Om $d | 314$ och 217
så $d | (1 \cdot 314 - 1 \cdot 217)$,
det vill säga $d | 97$.

$d | 217 \wedge d | 97 \Leftrightarrow$
$\Leftrightarrow d | (217 - 2 \cdot 97) \Leftrightarrow d | 97$

$d | 23 \wedge d | 5 \Leftrightarrow d | (5 \cdot 5 - 23)$

Exempel:

Sök sgd(332; 512)

Lösning:

$512 = 2 \cdot 332 - 152$
$332 = 2 \cdot 152 + 28$
$152 = 5 \cdot 28 + 12$
$28 = 2 \cdot 12 + 4$
$12 = 3 \cdot 4 + 0$

$4 | 4 \wedge 4 | 12 \Rightarrow 4 | 28$
$4 | 12 \wedge 4 | 28 \Rightarrow 4 | 28$
och så vidare

$4 | 512 \wedge 4 | 332$

Den sista icke-försvinnande: 4

Resten är sgd så:

Svar: sgd(332; 512) = 4

En diofantisk ekvation:

Exempel: Bestäm hela tal, x och y, sådana att $x \cdot 512 + y \cdot 332 = 4$

Lösning: Använder Euklides' algoritm; se ovan

Vi får ur detta att

$$
\begin{aligned}
4 &= 28 - 2\cdot 12 = \\
&= 28 - 2(152 - 5\cdot 28) = \\
&= 11\cdot 28 - 2\cdot 152 = \\
&= 11\cdot(332 - 2\cdot 152) - 2\cdot 152 = \\
&= 11\cdot 332 - 22\cdot 152 - 2\cdot 152 = \\
&= -24\cdot 152 + 11\cdot 332 = \\
&= -24(2\cdot 332 - 512) + 11\cdot 332 = \\
&= -48\cdot 332 + 24\cdot 512 + 11\cdot 332 = \\
&= \underbrace{-37}_{y}\cdot 332 + \underbrace{24}_{x}\cdot 512
\end{aligned}
$$

Svar: $x = 24$, $y = -37$

Sats:

Antag att $D = \text{sgd}(a; b)$; då finns alltid tal, x och y, sådana att $D = xa + yb$.

Exempel:

Bestäm en lösning till den diofantiska ekvationen

$$63x + 97y = 1$$

Lösning:

Euklides' algoritm	Vi finner av algoritmen
$97 = 1\cdot 63 + 34$	$1 = 7\cdot 5 - 34 = 7\cdot(2\cdot 34 - 63) - 34 =$
$63 = 2\cdot 34 - 5$	$= 13\cdot 34 - 7\cdot 63 = 13(97 - 63) - 7\cdot 63 =$
$24 = 7\cdot 5 - 1$	$= 13\cdot 97 - 20\cdot 63$

Svar: $y = 13$, $x = -20$

Lemma:

Antag att p är ett primtal ($p \in \mathbb{P}$).

Då gäller att $\quad p|a \cdot b \Rightarrow p|a \underset{\substack{\uparrow \\ \text{och/eller}}}{\vee} p|b$

$p \nmid a \Rightarrow \text{sgd}(p; a) = 1$ ty enda kandidaterna till sgd är 1
ty $p \nmid a$ och $a \nmid p$ ty $p \in \mathbb{P}$.

Det finns n och m sådana att $1 = np + ma$.

Multiplicera med b: $\quad b = npb + mab$

$p|ab,\ p|p \Rightarrow p|(npb + mab)$ så $p|b$ eftersom $p|ab$.

Bevissats:

Steg 1: Visa att det finns minst en primtalsfaktorisering.

Fall 1: n är ett primtal. Klar!

Fall 2: n är ej ett primtal

$n = a \cdot b,\ a, b > 1$

Fortsätt med a och b och försök faktorisera dess tal.
Och så vidare.

Steg 2: Visa att faktoriseringen är unik.

Antag att faktoriseringen inte är unik, det vill säga

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_e$

Ej nödvändigtvis olika primtal.

Då gäller $p_1 | n$ så: $p_1 | q_1(q_2 \cdot \ldots \cdot q_e)$

Fall 1: $p_1 | q_1 \Rightarrow p_1 = q_1$, ty primtal har (per definition) inga andra delare jämte sig själva.

Fall 2: $p_1 | p_1 \Rightarrow p_1 | (q_2 \cdot \ldots \cdot q_e) \Rightarrow p_1 | q_2(q_3 \cdot \ldots \cdot q_e)$ och så vidare.

Tillslut hittar vi ett q_i sådant att $p_1 | q_i$ och $p_1 = q_i$.

Börja från början med $n' = \frac{n}{p_1} = \frac{n}{q_i}$.

$n' = p_2 p_3 \ldots p_k = q_2 q_3 \ldots q_e$ (ifall $p_1 = q_1$ $(i = 1)$)

Exempel:

Bestäm samtliga lösningar till den diofantiska ekvationen $63x + 97y = \mathbf{1}$.

Lösning:

Vi har från tidigare $x = -20$, $y = 13$.

Antag att x', y' är en annan lösning:

$$
\begin{array}{rr}
13\cdot 97 & -20\cdot 63 = 1 \\
- \quad y'\cdot 97 & +x'\cdot 63 = 1 \\
\hline
(13 - y')\cdot 97 & +(-20 - x')\cdot 63 = 0
\end{array}
$$

Observera att övre raden subtraheras med undre raden ($y'\cdot 97 + x'\cdot 63$). −:et är alltså en operation mellan raderna.

$$\Updownarrow$$

$$(13 - y')\cdot 97 = (20 + x')\cdot 63$$

Relativt prima

Vi vet att $\text{sgd}(63; 97) = 1$ så $63 | (13 - y')$.

Det vill säga
$$13 - y' = k\cdot 63$$
$$y' = 13 - k\cdot 63$$

Vi får att
$$k\cdot 63\cdot 97 = (20 + x')\cdot 63$$
$$k\cdot 97 = 20 + x'$$
$$x' = -20 + k\cdot 97$$

Svar:
$$x' = -20 \cdot k\cdot 97$$
$$y' = 13 - k\cdot 63$$
$$k = 0, \pm 1, \pm 2, \ldots \quad (k \in \mathbb{Z})$$

Om x', y' är en lösning så är

$$x' = -20 + k\cdot 97$$
$$y' = 13 - k\cdot 63$$

för något $k \in \mathbb{Z}$.

Vi måste verifiera att vi får en lösning för olika k, vilket är lätt:

$$63(-20 + k\cdot 97) + 97(13 - 63) =$$
$$= -20\cdot 63 + k\cdot 63\cdot 97 + 13\cdot 97 - k\cdot 63\cdot 97 =$$
$$= -20\cdot 63 + 13\cdot 97 = \mathbf{1}$$

Exempel:

Lös ekvationen $36x + 56y = 2$

Lösning:

$36x + 56y = 2$
$18x + 28y = 1$

Saknar lösning ty sgd$(18; 28) \nmid 1$

Exempel:

Bestäm en lösning till $63x + 97y = 113$

Lösning:

Vi vet att $-20 \cdot 63 + 13 - 97 = 1$

$113 \cdot (-20) \cdot 63 + 113 \cdot 13 \cdot 97 = 113$

$x = 113 \cdot (-20) \quad = -2260$
$y = 113 \cdot 13 \quad = 1599$