Diskret matematik 2018-03-21 #2

IDAG:
- Diofantiska ekvationer
  - Vilka är lösbara?
  - Hur kan vi hitta en lösning?
  - Hur kan vi hitta samtliga lösningar?
- Primtal och primtalsfaktorisering
- Aritmetikens fundamentalsats

Q: är $11\cdot 21\cdot 41\cdot 57 = 13\cdot 19\cdot 47\cdot 53$? Nej!

Def^n En ekvation kallas diofantisk om den ska lösas i heltalsvariabler.

a, b, d bestämda, m, n variabler

$\rightarrow am + bn = d$ ⊛

Problem Går det att lösa den diofantiska ekvationen
$9m + 12n = 4$
$3(3m + 4n)$

Svar: Nej: VL är en multipel av $3 = \gcd(9,12)$
men 4 är inte en multipel av 3 ∎

Sats (gcd delar linjärkombinationer)

Låt a & b vara heltal. Då gäller det att
$\gcd(a,b) \mid am + bn$ för alla heltal m, n.

Går det att lösa ⊛ om d är en multipel av $\gcd(a,b)$?

Ex. Går $133m + 56n = 7$ att lösa?

Svar: Ja: "läs Euklides baklänges":

$$\begin{aligned} 7 &= 21 - 14 \\ &= 21 - (56 - 2\cdot 21) \\ &= 3\cdot 21 - 56 \\ &= 3\cdot(133 - 2\cdot 56) - 56 \\ &= 3\cdot 133 - 7\cdot 56 \end{aligned}$$

Så en lösning är $m = 3$, $n = -7$ ∎

Detta funkar alltid:

Sats: (gcd som linjärkombination)

Låt a, b vara heltal. Då finns det heltal m, n sådana att

$\gcd(a,b) = am + bn$

$(\gcd(0,0) = 0)$

Går det alltid att lösa

$am + bn = d$ om $\gcd(a,b) \mid d$?

Ja: <u>Metod</u> (partikulärlösning) Låt a, b, d vara heltal.

För att hitta en lösning till den diof. ekv.

$am + bn = d,$

där d är en multipel av $\gcd(a,b)$:

1) lös $am_0 + bn_0 = \gcd(a,b)$ (t.ex. genom "Euklides baklänges")

2) multiplicera igenom med $\frac{d}{\gcd(a,b)}$

– då är

$$a \cdot \left(m_0 \cdot \frac{d}{\gcd(a,b)}\right) + b\left(n_0 \cdot \frac{d}{\gcd(a,b)}\right) = d$$

Så $m = \uparrow$ och $n = \uparrow$ är en lösning

<u>Ex.</u> Hitta en lösning till $133m + 56n = 28$

Svar: enligt metoden:

1) Lös $\underset{\substack{\uparrow \\ 3}}{133m_0} + \underset{\substack{\uparrow \\ -7}}{56n_0} = 7$

$(m_0, n_0) = (3, -7)$

2) Multiplicera med $\frac{HL}{\gcd} = \frac{28}{7} = 4$

och då $(m,n) = 4(m_0, n_0) = (12, -28)$.

<u>Sats</u> (Lösbarhet)

Låt a, b, d vara heltal. Den diof. ekv.

$am + bn = d$

går att lösa om och endast om $\gcd(a,b) \mid d$

<u>Bevis</u> "Om": Partikulärlösn.-metoden

"Endast om": Sats "gcd delar L.K." ∎

En 7kr & en 23kr

48kr?

$7m + 23n = 48$

<u>Hitta alla lösningar?</u>

Finn relationer mellan lösn:

om $am_1 + bn_1 = d$

& $am_2 + bn_2 = d$

då gäller det att $am_1 + bn_1 - (am_2 + bn_2) = 0$

dvs

$a(m_1 - m_2) + b(n_1 - n_2) = 0$

Så $(m_1 - m_2, n_1 - n_2)$ är en lösn. till den homogena ekvationen $am + bn = 0$

Def. Två tal a, b sägs vara relativt prima om $\gcd(a,b) = 1$.

Sats (Delbarhet hos produkt)

Låt a, b vara relativt prima. Om $a \mid b \cdot n$ för något heltal n gäller att $a \mid n$.

Bevis Vi vet enligt ~~tidigare~~ sats att det finns heltal p & q sådana att $ap + bq = 1$. $(= \gcd(a,b))$

Multiplicera med n:

$$apn + bnq = n.$$

Eftersom apn är en multipel av a och bn är en multipel av a så är HL (dvs n) det också.

Dvs. $a \mid n$ ▨

Sats Låt a, b vara heltal, inte båda 0.

Då är $\frac{a}{\gcd(a,b)}$, $\frac{b}{\gcd(a,b)}$ relativt prima.

Bevis Vi vet enligt sats att det finns m, n så att

$$am + bn = \gcd(a,b).$$

Dela med $\gcd(a,b)$:

$$\underbrace{\frac{a}{\gcd(a,b)}}_{a'} m + \underbrace{\frac{b}{\gcd(a,b)}}_{b'} n = 1$$

Eftersom denna ekvation har en lösning måste högerledet vara en multipel av $\gcd(a', b')$.

Alltså $\gcd(a', b') \mid 1$
Därför är $\gcd(a', b') = 1$ ▨

Sats (Hjälpekvation/noll-lösning/homogen ekvation)

Låt a, b vara heltal, inte båda 0.

Samtliga lösningar till ekv.

$$am + bn = 0$$

ges då av

$$\begin{cases} m = \frac{-b}{\gcd(a,b)} \cdot k \\ n = \frac{a}{\gcd(a,b)} \cdot k \end{cases}$$

för godtyckliga heltal k.

Bevis Att alla sådana m, n är lösningar följer från direkt-substitution

$$a\left(\frac{-b}{gcd}k\right) + b\left(\frac{a}{gcd}k\right) = 0 \quad \checkmark$$

Att alla lösn. har denna form:

Om $am + bn = 0$, då är $am = -bn$

så $\underbrace{\frac{a}{gcd(a,b)}}_{a'} m = -\underbrace{\frac{b}{gcd(a,b)}}_{b'} n \qquad a'm = -b'n$

Så $a' | b'n$.

Men a', b' är relativt prima enligt tidigare sats, så enligt satsen innan gäller $a'|n$.

Alltså finns det ett heltal k så att

$$n = a'k = \frac{a}{gcd(a,b)}k$$

och $a'm = -b'n = -b'a'k$,

så $m = -b'k = -\frac{b}{gcd(a,b)}k \qquad \blacksquare$

Metod (Hitta samtliga lösn.)

Låt a, b, d vara heltal, a & b inte båda 0, och där $gcd(a,b)|d$.

Samtliga lösningar till ekv.

$$am + bn = d$$

ges då av

$$\begin{cases} m = m_p - \frac{b}{gcd(a,b)}k \\ n = n_p + \frac{a}{gcd(a,b)}k \end{cases} \quad \text{för godtyckliga heltal } k,$$

där (m_p, n_p) är en partikulärlösning enligt tidigare Metod.

Ex Finn alla lösn. till ekv.

$$\underset{a}{133}m + \underset{b}{58} = 28$$

Svar En part. lösn ges av $(m_p, n_p) = (12, -28)$.

Så enl. sats ges alla lösningar av

$$\begin{cases} m = 12 - \frac{56}{7}k = 12 - 8k \\ n = -28 + \frac{133}{7}k = -28 + 19k \end{cases} \quad \text{för godtyckliga heltal } k,$$

Primtal

Def^n Ett heltal större än 1 kallas ett primtal om det endast har ± 1 och $\pm$(sig självt) som delare.

Ett heltal större än 1 kallas sammansatt om det inte är ett primtal.

2, 3, 5, 7, 11, 13, 17... är primtal.

Sats (Primtalsfaktorisering)

Låt $m \geq 2$ vara ett heltal. Då finns det primtal $p_1, p_2, \dots p_k$ (där $k \geq 1$) sådana att

$$m = p_1 p_2 \cdots p_k.$$

Bevis Vi kör en algoritm.

Om m är ett primtal, då är vi klara ($p_1 = m$)
Om m inte är ett primtal, då har det en positiv faktor som inte är 1 eller m, dvs vi kan skriva

$$m = q \cdot d$$

där $1 < q, d < m$

Repetera nu detta med q & d:
om q är ett primtal, stoppa där,
annars dela upp $q = q_1 q_2$ där $1 < q_1, q_2 < q$
och samma för d.

Denna algoritm terminerar, för alla talen inblandade blir mindre och mindre, men är ≥ 2

Enda anledningen till att vi inte kan fortsätta är att alla tal är primtal. ∎