KTH Matematik

KTHs Matematiska Cirkel

Talteori

Andreas Enblom
Alan Sola

Institutionen för matematik, 2008
Finansierat av Marianne och Marcus Wallenbergs Stiftelse

2 Gemensamma delare

2.1 Största gemensamma delare

Vi ska nu göra en precis definition av vad vi menar med den *största gemensamma delaren* till två tal. Inutitivt är det klart vad som menas. Betrakta exempelvis talen 8 och 12. Talet 8 har följande positiva delare:

$$1, \quad 2, \quad 4, \quad 8,$$

och talet 12 har följande positiva delare.

$$1, \quad 2, \quad 3, \quad 4, \quad 6, \quad 12.$$

Det största talet som är en delare till både 8 och 12 är alltså 4. Vi säger alltså att 4 är den största gemensamma delaren till 8 och 12, och skriver $4 = \text{sgd}\,(8, 12)$. Låt oss nu göra en allmän definition av detta.

Definition 2.1.1. Låt n vara ett heltal. Betrakta mängden

$$D(n) = \{a \in \mathbb{Z} \,:\, a > 0,\ a \mid n\}.$$

Denna mängd kallar vi *delarmängden till* n.

Mängden $D(n)$ innehåller alltså alla positiva delare till n. Vi har exempelvis att $D(12) = \{1, 2, 3, 4, 6, 12\}$.

Definition 2.1.2. Låt a, b vara heltal, där inte både a och b är 0. Det största talet i mängden $D(a) \cap D(b)$ kallar vi för *den största gemensamma delaren till* a *och* b. Vi betecknar detta tal med $\text{sgd}\,(a, b)$.

När man ger en definition som denna måste man fundera på om mängden $D(a) \cap D(b)$ verkligen innehåller ett största element, för alla val av a och b, så att definitionen har en innebörd. Detta bevisas här:

Sats 2.1.3. *Låt* a *och* b *vara heltal som inte båda är* 0. *Då innehåller mängden* $D(a) \cap D(b)$ *ett största element.*

Bevis. Enligt påstående 3 i Sats 1.1.2 räcker det att visa att $D(a) \cap D(b) \neq \varnothing$ samt att $D(a) \cap D(b)$ har en övre begränsning.

Observera att $1 \in D(n)$ för varje heltal n. Alltså kommer även $1 \in D(a) \cap D(b)$. Detta betyder att $D(a) \cap D(b) \neq \varnothing$.

Att $D(a) \cap D(b)$ har en övre begränsning följer om vi kan visa att minst en av mängderna $D(a)$ och $D(b)$ har en övre begränsning. Vi vet att minst ett av talen a och b inte är 0. Antag utan inskränkning att $a \neq 0$ (fallet $b \neq 0$ hanteras på samma sätt). Låt

$$M = \begin{cases} a & \text{om } a > 0 \\ -a & \text{om } a < 0, \end{cases}$$

Vi väljer alltså M sådant att $M > 0$. Tag ett godtyckligt $x \in D(a)$. Då är x en delare till a, och därmed också en delare till M. Detta betyder att det finns ett tal q sådant att $M = xq$, och eftersom $M > 0$ så måste $x \leqslant M$. Alltså är M en övre begränsning till $D(a)$. □

Definition 2.1.4. Låt a, b vara heltal, inte båda 0. Om $\text{sgd}\,(a, b) = 1$ så säger vi att a och b är *relativt prima.*

Exempel 2.1.5. Betrakta talen $9 = 3 \cdot 3$, $10 = 2 \cdot 5$, och $12 = 2 \cdot 2 \cdot 3$. Klart är att

$$D(9) = \{1, 3, 9\}, \quad D(10) = \{1, 2, 5, 10\}, \quad D(12) = \{1, 2, 3, 4, 6, 12\}.$$

Alltså gäller

$$\text{sgd}\,(9, 10) = 1, \quad \text{sgd}\,(9, 12) = 3, \quad \text{sgd}\,(10, 12) = 2.$$

Detta betyder att talen 9 och 10 är relativt prima, medan varken 9 och 12 eller 10 och 12 är relativt prima. ▲

Exempel 2.1.6. Det kan vara intressant att fundera på vad största gemensamma delaren till ett positivt tal och 0 är. Låt $a > 0$. Enligt definitionen är det faktiskt så att

$$D(0) = \{1, 2, 3, \ldots\},$$

och därmed får vi

$$D(a) \cap D(0) = D(a).$$

Observera nu att det största talet i $D(a)$ är a, och därför är

$$\text{sgd}\,(a, 0) = a.$$ ▲

2.2 Euklides algoritm

Sats 2.2.1. *Låt a, b vara heltal där $b \neq 0$. Antag att heltalen p, q uppfyller*

$$a = b \cdot q + r.$$

Då gäller

$$\text{sgd}\,(a, b) = \text{sgd}\,(b, r)\,.$$

Bevis. Tag $x \in D(b) \cap D(r)$. Då gäller $x \mid b$ och $x \mid r$. Det betyder att det finns heltal m_1, m_2 sådana att $b = xm_1$ och $r = xm_2$. Vi får att

$$a = bq + r = xm_1q + xm_2 = x(m_1q + m_2).$$

Alltså gäller $x \mid a$ och därmed $x \in D(a)$. Eftersom $x \in D(b)$ så får vi $x \in D(a) \cap D(b)$. Vi har alltså visat att

$$D(b) \cap D(r) \subseteq D(a) \cap D(b).$$

Omvänt, tag $y \in D(a) \cap D(b)$. Då finns heltal k_1 och k_2 sådana att $a = yk_1$ och $b = yk_2$. Nu får vi

$$r = a - bq = yk_1 - yk_2q = y(k_1 - k_2q).$$

Alltså gäller $y \mid r$ och därmed $y \in D(r)$. Eftersom $y \in D(b)$ så följer $x \in D(b) \cap D(r)$. Detta visar att

$$D(a) \cap D(b) \subseteq D(b) \cap D(r).$$

Eftersom vi nu har visat att $D(b) \cap D(r) \subseteq D(a) \cap D(b)$ och $D(a) \cap D(b) \subseteq D(b) \cap D(r)$, så följer

$$D(a) \cap D(b) = D(b) \cap D(r). \qquad \square$$

Denna sats kan användas för att räkna ut största gemensamma delaren till två tal. Denna uträkningsmetod, som här illustreras med ett exempel, brukar kallas *Euklides algoritm.*

Exempel 2.2.2 (Euklides algoritm)**.** Låt oss bestämma $\operatorname{sgd}(6\,396, 525)$. Eftersom

$$6\,396 = 525 \cdot 12 + 96$$

så följer

$$\operatorname{sgd}(6\,396, 525) = \operatorname{sgd}(525, 96).$$

Vidare, vi har att

$$525 = 96 \cdot 5 + 45,$$

och därmed

$$\operatorname{sgd}(525, 96) = \operatorname{sgd}(96, 45).$$

Fortsätt på detta sätt så ser det ut så här:

$$\begin{array}{rl|l} 6\,396 = & 525 \cdot 12 + 96 & \operatorname{sgd}(6\,396, 525) = \operatorname{sgd}(525, 96) \\ 525 = & 96 \cdot 5 + 45 & = \operatorname{sgd}(96, 45) \\ 96 = & 45 \cdot 2 + 6 & = \operatorname{sgd}(45, 6) \\ 45 = & 6 \cdot 7 + 3 & = \operatorname{sgd}(6, 3) \\ 6 = & 3 \cdot 2 + 0 & = \operatorname{sgd}(3, 0) = 3. \end{array}$$

Vi ser alltså att $\operatorname{sgd}(6\,396, 525) = 3$. Algoritmen går alltså ut på att utföra heltalsdivision ett antal gånger tills den går jämnt ut (det vill säga att resten blir 0), och sedan använda det faktum att $\operatorname{sgd}(n, 0) = n$ för alla $n > 0$, vilket diskuterades i Exempel 2.1.6. ▲

Sats 2.2.3. *Låt a, b vara heltal som är relativt prima. Då finns heltal x, y sådana att*

$$1 = xa + yb.$$

Bevis. Vi kan utan inskränkning anta att $b > 0$. Använd nu Sats 1.3.1 för att utföra heltalsdivision om och om igen, tills resttermen blir 0, och få:

$$\begin{aligned}
a &= b \cdot q_1 + r_1 && \text{där} && 0 < r_1 < b \\
b &= r_1 \cdot q_2 + r_2 && \text{där} && 0 < r_2 < r_1 \\
r_1 &= r_2 \cdot q_3 + r_3 && \text{där} && 0 < r_3 < r_2 \\
r_2 &= r_3 \cdot q_4 + r_4 && \text{där} && 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n && \text{där} && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n \cdot q_{n+1} + r_{n+1} && \text{där} && r_{n+1} = 0
\end{aligned} \tag{2.1}$$

Att denna process verkligen tar slut, och att resten på den sista raden blir 0 inser man eftersom

$$b > r_1 > r_2 > \cdots > r_n > 0.$$

En sådan följd av heltal, som blir mindre och mindre hela tiden måste så småningom nå 0. Enligt Sats 2.2.1 vet vi att

$$\begin{aligned}
1 &= \operatorname{sgd}(a, b) \\
&= \operatorname{sgd}(b, r_1) \\
&= \operatorname{sgd}(r_1, r_2) \\
&= \operatorname{sgd}(r_2, r_3) \\
&\;\;\vdots \\
&= \operatorname{sgd}(r_{n-1}, r_n) \\
&= \operatorname{sgd}(r_n, 0) \\
&= r_n,
\end{aligned}$$

det vill säga att $r_n = 1$. Använd nu (2.1) baklänges och få

$$\begin{aligned}
1 &= r_n \\
&= r_{n-2} - q_n \cdot r_{n-1} = r_{n-2} - q_n \cdot (r_{n-3} - r_{n-2} \cdot q_{n-1}) \\
&= -q_n \cdot r_{n-3} + (1 - q_{n-1} q_n) \cdot r_{n-2} \\
&\;\;\vdots \\
&= x \cdot a + y \cdot b
\end{aligned}$$

för några heltal x, y. □

Exempel 2.2.4. Talen 4 712 och 585 är relativt prima. Det visas på följande sätt:

$$\begin{array}{rcl|rcl}
4\,712 &=& 585 \cdot 8 + 32 & \operatorname{sgd}(4\,712, 585) &=& \operatorname{sgd}(585, 32) \\
585 &=& 32 \cdot 18 + 9 & &=& \operatorname{sgd}(32, 9) \\
32 &=& 9 \cdot 3 + 5 & &=& \operatorname{sgd}(9, 5) \\
9 &=& 5 \cdot 1 + 4 & &=& \operatorname{sgd}(5, 4) \\
5 &=& 4 \cdot 1 + 1 & &=& \operatorname{sgd}(4, 1) \\
4 &=& 1 \cdot 4 + 0 & &=& \operatorname{sgd}(1, 0) = 1.
\end{array} \tag{2.2}$$

Detta visar att $\operatorname{sgd}(4\,712, 585) = 1$, men uträkningarna kan också användas för att hitta de tal x, y som enligt satsen ovan finns och gör

$$1 = 4\,712 \cdot x + 585 \cdot y.$$

Använd (2.2) baklänges och få

$$\begin{aligned} 1 &= 5 - 4 \cdot 1 && = 5 - (9 - 5 \cdot 1) \cdot 1 \\ &= -9 + 5 \cdot 2 && = -9 + (32 - 9 \cdot 3) \cdot 2 \\ &= 32 \cdot 2 - 9 \cdot 7 && = 32 \cdot 2 - (585 - 32 \cdot 18) \cdot 7 \\ &= -585 \cdot 7 + 32 \cdot 128 && = -585 \cdot 7 + (4\,712 - 585 \cdot 8) \cdot 128 \\ &= 4\,712 \cdot 128 - 585 \cdot 1\,031. \end{aligned}$$

Alltså gäller

$$x = 128 \quad \text{och} \quad y = -1\,031. \qquad \blacktriangle$$

Sats 2.2.5. *Låt a, b vara relativt prima heltal, och c ett godtyckligt heltal. Om $a \mid bc$ så gäller $a \mid c$.*

Bevis. Enligt Sats 2.2.3 finns heltal x, y sådana att $1 = xa + yb$. Multiplicera detta med c och få

$$c = xac + ybc.$$

Eftersom $a \mid bc$ så finns ett heltal q sådant att $bc = aq$. Nu följer

$$c = xac + ybc = xac + yaq = a(xc + yq),$$

vilket visar att $a \mid c$. □

Övningar

Övning 2.1. Låt a, b vara heltal. Antag att heltalet $d > 0$ uppfyller

$$d \mid a \quad \text{och} \quad d \mid b.$$

Antag att $x \mid d$ för varje $x \in D(a) \cap D(b)$. Visa att $d = \operatorname{sgd}(a, b)$.

Övning 2.2. Använd Euklides algoritm för att bestämma $\operatorname{sgd}(8\,860, 1\,075)$.

Övning 2.3. Talen 139 och 117 är relativt prima. Enligt Sats 2.2.3 finns heltal x och y sådana att $1 = x \cdot 139 + y \cdot 117$. Använd tekniken i Exempel 2.2.4 för att bestämma x och y.

Övning 2.4. Låt a och b vara relativt prima heltal. Antag att heltalet c uppfyller att

$$a \mid c \quad \text{och} \quad b \mid c.$$

Visa att $ab \mid c$.