Mårten Wadenbäck

Delbarhet

Definition: Låt $a, b \in \mathbb{Z}$. Om det finns ett $m \in \mathbb{Z}$ sådant att $a = mb$ säger vi att b *delar* a (a är en multipel av b).

Detta skrivs då $b \mid a$, och annars $b \nmid a$.

Exempel: Gäller det att

a) $4 \mid 20$? b) $-2 \mid 10$?

c) $7 \mid 10$? d) $0 \mid 0$?

Sats: Delbarhet uppfyller

i) $a \mid 0$ för alla $a \in \mathbb{Z}$

ii) reflexivitet, dvs $a \mid a$ $\forall a \in \mathbb{Z}$

iii) transitivitet, dvs $a \mid b \wedge b \mid c \Rightarrow a \mid c$ $\forall a, b, c \in \mathbb{Z}$

iv) för alla $a, b, c \in \mathbb{Z}$ gäller det att

$$a \mid b \wedge a \mid c \iff \forall m, n \in \mathbb{Z} : a \mid mb + nc.$$

Bevis: i) Eftersom $0 = 0 \cdot a$ för alla $a \in \mathbb{Z}$ gäller att $a \mid 0$.

ii) Eftersom $a = 1 \cdot a$ för alla a gäller det att $a \mid a$.

iii) Antag att $a \mid b$ och $b \mid c$, dvs att $b = ma$ och $c = nb$. Då är $c = nb = n(ma) = (nm)a$, så $a \mid c$.

iv) ($\Leftarrow$) Antag att $\forall m, n \in \mathbb{Z} : a \mid mb + nc$. Väljer vi speciellt $m = 1$ och $n = 0$ får vi $a \mid b$, och på samma sätt ger $m = 0$ och $n = 1$ att $a \mid c$.

($\Rightarrow$) Antag att $a \mid b$ och $a \mid c$, dvs $b = sa$ och $c = ta$. För alla $m, n \in \mathbb{Z}$ är då $mb + nc = m(sa) + n(ta) = (ms + nt)a$, så $a \mid mb + nc$.

Sats: Om a och b är positiva heltal sådana att $a \mid b$ så är $a \leq b$.

Bevis: Om $a \mid b$ så finns ett m så att $b = ma$, men eftersom a och b är positiva är $m \geq 1$, och därför är $b = ma \geq 1 \cdot a = a$.

Vi skall nu se vad som händer i de fall då $b \nmid a$, dvs när divisionen $\frac{a}{b}$ inte går jämnt upp.

Sats (Divisionsalgoritmen): För varje par av positiva heltal a och b finns det entydiga heltal q (kvoten) och r (resten) sådana att

$$a = qb + r \quad \text{och} \quad 0 \leq r < b.$$

Exempel: Om $a=45$ och $b=6$ går b sju gånger i a, och kvar blir en rest på tre. Alltså $45 = 7 \cdot 6 + 3$.

Anmärkning: Om $r=0$ betyder det att $b \mid a$, och om $b \mid a$ blir $r=0$.

Bevis av divisions algoritmen: Vi börjar med att visa existensen av talen q och r. Låt $M = \{a-tb : a-tb \geq 0\}$. Eftersom $a \in M$ är M en icketom delmängd av $\mathbb{N}$, och välordningsprincipen garanterar att M har ett minsta element $r = a-qb \Leftrightarrow a = qb+r$. Vi behöver visa att $0 \leq r < b$. Antag det motsatta, dvs att $r \geq b \Leftrightarrow r-b \geq 0$. Då är $0 \leq r-b = a-qb-b = a-(q+1)b < r$, vilket strider

mot att r skulle vara det minsta elementet i M.

På grund av motsägelsen måste $0 \leq r < b$, som önskat.

För entydigheten, antag motsatsen, dvs att $a = qb + r$ och $a = q'b + r'$ med $q \neq q' \wedge r \neq r'$. Vi kan antaga att $q > q'$. Då är $0 = a - a = qb + r - q'b - r' = (q - q')b + r - r'$, så $r' = (q - q')b + r$. Detta ger motsägelsen att $r' \geq b$, så det kan inte finnas flera olika kvoter och rester.

Definition: Om $c \mid a$ och $c \mid b$ kallas c en gemensam delare till a och b. Det största talet d för vilket $d \mid a$ och $d \mid b$ kallas största gemensamma delaren till a och b, och betecknas $d = \text{sgd}(a, b)$.

Exempel: De gemensamma delarna till 9 och 12 är ± 1 och ± 3. Alltså är $\text{sgd}(9, 12) = 3$.

Sats: Det gäller att

i) $\forall a \in \mathbb{N}: \text{sgd}(a, 0) = a$

ii) $\forall a, b, n \in \mathbb{Z}: \text{sgd}(a + nb, b) = \text{sgd}(a, b)$.

Bevis: Om $d=sgd(a,0)$ så gäller $d|a \Rightarrow d \leq a$, och då $a|a$ gäller det att $d=a$. Detta visar i).

För att visa ii) låter vi $d=sgd(a,b)$ och $d'=sgd(a+nb,b)$.

Nu gäller $d|a \wedge d|b \Rightarrow d|a+nb$, så $d \leq d'$. På samma sätt gäller $d'|a+nb \wedge d'|b \Rightarrow d'|a+nb-nb \Leftrightarrow d'|a$, så $d' \leq d$.

Sats (Euklides algoritm): Låt a och b vara positiva heltal med $a \geq b$. Upprepad användning av divisionsalgoritmen ger

$$\begin{aligned}
a &= q_1 b + r_1, & 0 \leq r_1 < b \\
b &= q_2 r_1 + r_2, & 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 \leq r_3 < r_2 \\
&\vdots & \vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

Då gäller att $sgd(a,b)=r_n$.

Anledningen till att detta gäller är att

$$sgd(a,b)=sgd(a-q_1 b, b)=sgd(r_1,b)=sgd(r_1, b-q_2 r_1)=$$
$$=sgd(r_1,r_2)=\dots=sgd(r_{n-1}-q_{n+1}r_n, r_n)=sgd(0,r_n)=r_n.$$

Exempel: Beräkna sgd(900, 684). Vi använder Euklides algoritm och får

$$900 = 1 \cdot 684 + 216$$
$$684 = 3 \cdot 216 + 36$$
$$216 = 6 \cdot 36.$$

Här ser vi att sgd(900, 684) = 36. Vi fortsätter för att få en guldstjärna, och skriver

$$36 = 684 - 3 \cdot 216 = 684 - 3 \cdot (900 - 1 \cdot 684) = 4 \cdot 684 - 3 \cdot 900.$$

Denna fortsättning, där vi gick baklänges i Euklides algoritm, kommer att visa sig väldigt praktisk. Dessutom visar den

Sats (Bezouts identitet): Låt a och b vara heltal. Då finns det heltal u och v sådana att

$$sgd(a,b) = au + bv.$$

Definition: Ett heltal $a > 1$ sägs vara ett <u>primtal</u> om de enda positiva delarna till a är 1 och a. Om $a > 1$ inte är ett primtal kallas det för ett <u>sammansatt</u> tal.

Notera att om a är ett primtal och $a \nmid b$ så är sgd(a,b) = 1.

Sats: Om a och b är heltal med $\text{sgd}(a,b)=1$ och c är ett heltal så gäller att $a|bc \Rightarrow a|c$.

Bevis: Enligt Bezouts identitet finns det heltal u och v sådana att $au+bv=1$, så $acu+bcv=c$. Eftersom $a|bc$ delar a vänsterledet, och därför måste även $a|c$.

Exempel: Om $a=6$, $b=5$, och $c=12$ så gäller $\text{sgd}(a,b)=1$ och $a|bc$ eftersom $6|60$. Om däremot $a=6$, $b=3$, och $c=8$ gäller $a|bc$ men $a\nmid c$.

Följdsats: Om p är ett primtal och $a,b\in\mathbb{Z}$ så gäller det att $p|ab \Rightarrow p|a \vee p|b$.