KTH Matematik

KTHs Matematiska Cirkel

Talteori

Andreas Enblom
Alan Sola

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

1 Heltal

1.1 Grundläggande egenskaper för heltalen

Heltal är tal som 1, 0, -17 och 4712. Vi kommer som tidigare nämnts att använda beteckningen $\mathbb{Z}$ för heltalen. Detta är alltså den mängd som består av alla heltal:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

När man beskriver matematisk teori, måste man alltid utgå från någonting. Inom talteorin utgår man från heltalen tillsammans med räknesätten addition ($+$) och multiplikation ($\cdot$), samt jämförelserelationerna $<$, $=$ och $>$. Vi bestämmer oss alltså för att ta existensen av heltal, samt addition, multiplikation och jämförelse av dessa, för givna. Det kan påpekas att dessa saker faktiskt kan bevisas, om man utgår från ännu enklare förutsättningar.

> I fortsättningen anses läsaren känna till heltalen $\mathbb{Z}$ samt hur man adderar, multiplicerar och jämför dem.

Det kan vara på sin plats att kommentera räknesätten subtraktion och division. Subtraktion är bara ett specialfall av addition, givet att man vet hur man utifrån ett tal $a \in \mathbb{Z}$ bildar talet $-a$. Vi har ju att

$$3 - 8 = 3 + (-8)$$

så för att kunna utföra subtraktionen med 8 räcker det att känna till addition samt hur man bildar talet -8. Division är lite mer komplicerat och det kommer vi till om en sida eller två.

Trots att alla läsare känner till det om heltal, addition och så vidare som vi förväntar oss, kan det ändå vara intressant att skriva upp några av de allra viktigaste egenskaperna för heltalen, och det görs här, utan bevis:

Sats 1.1.1. *Heltalen $\mathbb{Z}$ tillsammans med operationerna $+$ och $\cdot$ uppfyller följande egenskaper för alla $a, b, c \in \mathbb{Z}$:*

1. $a + b \in \mathbb{Z}$
2. $a \cdot b \in \mathbb{Z}$.
3. $a + b = b + a$
4. $a \cdot b = b \cdot a$.
5. $a + (b + c) = (a + b) + c$.

6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
7. $a \cdot (b + c) = a \cdot b + a \cdot c$.
8. *Heltalet* $0 \in \mathbb{Z}$ *uppfyller* $a + 0 = a$.
9. *Heltalet* $1 \in \mathbb{Z}$ *uppfyller* $a \cdot 1 = a$.
10. *För varje heltal* a *finns ett heltal* $-a$ *sådant att* $a + (-a) = 0$.

Av intresse är att notera att om vi har någon godtycklig mängd, antingen $\mathbb{Z}$ eller någon annan mängd, för vilken man definierat några operationer, betecknade med $+$ och $\cdot$, som uppfyller punkterna 1–10 ovan, så kallas den mängden för en *kommutativ ring*, eller ibland *kommutativ talring* eller bara *ring*. Sådana ringar finns det massor av exempel på. Senare ska vi få stifta bekantskap med de *Gaussiska heltalen* som utgör just en kommutativ ring.

Följande egenskaper kan kännas självklara, men är i själva verket några oerhört centrala egenskaper för heltalen. De är tre av de egenskaper som gör tal så unika inom matematiken.

Sats 1.1.2. *För heltalen* $\mathbb{Z}$ *gäller följande:*

1. *Om* $a, b \in \mathbb{Z}$ *så gäller exakt en av* $a < b$, $a = b$ *och* $a > b$.
2. *Om* $k \neq 0$ *är ett heltal och* $a \cdot k = b \cdot k$ *så gäller* $a = b$, *för* $a, b \in \mathbb{Z}$.
3. *Antag att* $A \subseteq \mathbb{Z}$, *att* $A \neq \varnothing$ *samt att det finns en* övre begränsning *för* A, *det vill säga ett tal* $m \in \mathbb{Z}$ *sådant att* $m \geqslant x$ *för alla* $x \in A$. *Då innehåller* A *ett* största element. *Med andra ord finns då ett* $a \in A$ *sådant att* $a \geqslant x$ *för alla* $x \in A$.

Observera att det i punkt 3 *inte* behöver vara så att $m = a$. Talet m behöver inte ligga i mängden A, utan det räcker att det är *någon* övre begränsning för A. Slutsatsen är att det finns en övre begränsning a som ligger i själva mängden A.

Exempel 1.1.3. Låt $A = \{-3, 0, 1, 2, 5, 10, 12\}$. Eftersom exempelvis $57 \geqslant x$ för alla $x \in A$ så är 57 en övre begränsning för A. Talet 12 är ett största element i A eftersom det både är en övre begränsning för A och tillhör A. ▲

1.2 Delbarhet

Av stor vikt inom talteorin är egenskapen för tal att dela andra tal. Exempelvis: eftersom $12 = 4 \cdot 3$ så vet vi att 4 delar 12. Det är just på detta sätt vi definierar *delbarhet*:

Definition 1.2.1. Låt a och b vara heltal. Om det finns ett heltal q sådant att $a = b \cdot q$ så säger vi att b *delar* a, och skriver

$$b \mid a.$$

Om b inte delar a så skriver vi $b \nmid a$.

Exempel 1.2.2. Vi har att

$$3 \mid 24 \quad \text{eftersom} \quad 24 = 8 \cdot 3.$$

Men delbarhet fungerar också för negativa tal. Det gäller att

$$-3 \mid 24 \quad \text{eftersom} \quad 24 = (-8) \cdot (-3).$$

och också att

$$3 \mid -24 \quad \text{samt} \quad -3 \mid -24.$$

Däremot gäller inte $5 \mid 24$. Detta skriver vi alltså som $5 \nmid 24$. ▲

Enligt definitionen av delbarhet delar alla heltal talet 0. Att $0 = a \cdot 0$ innebär ju att $a \mid 0$ för alla $a \in \mathbb{Z}$.

1.3 Division

Nu är det dags att fundera på hur man dividerar heltal. Det är viktigt att tänka på att det är just heltal vi dividerar, och att vi som resultat vill få heltal.

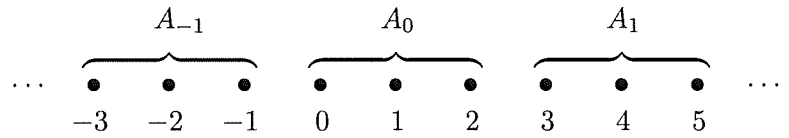
Alla vet att $6/3 = 2$, men var betyder detta egentligen? Och hur utför man divisionen $7/3$ om man bara får använda heltal? Svaren ges av följande sats:

Sats 1.3.1. *Låt a, b vara heltal. Antag att $b > 0$. Då finns unika heltal q och r, där $0 \leqslant r < b$, sådana att*

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

Vi skriver inte ner alla detaljer i beviset för denna sats, utan nöjer oss med att beskriva den grundläggande idén.

Bevisidé. För betrakta mängderna $A_n = \{b \cdot n + m \,:\, 0 \leqslant m < b\}$, där $n \in \mathbb{Z}$. För exempelvis $b = 3$ ser mängderna ut så här:



Man inser nu att det för varje $a \in \mathbb{Z}$ finns ett unikt n sådant att $a \in A_n$. Och enligt definitionen av A_n finns ett unikt m med $0 \leqslant m < b$ sådant att $a = b \cdot n + m$. Låt $q = n$ och $r = m$ och saken är klar. □

Satsen säger faktiskt att vi alltid kan utföra det som brukar kallas för *heltalsdivision*. Vi har exempelvis att

$$7 = 3 \cdot 2 + 1,$$

och då säger vi att heltalsdivision av 7 med 3 ger kvoten 2 och resten 1. Termen r i satsen ovan brukar alltså kallas *rest* eller *restterm*.

Men hur är det med divisionssymbolen / då? Vad betyder $6/3 = 2$? Jo, det är helt enkelt så att

$$6 = 3 \cdot 2 + 0$$

och därför kan vi skriva $6/3 = 2$. Så fort ett tal b delar ett tal a, kommer resttermen r i satsen ovan att vara 0, precis som i fallet $a = 6$ och $b = 3$. I sådana fall skriver vi att $q = a/b$.

Definition 1.3.2. Antag att a, b är heltal där $b \neq 0$, och att $b \mid a$. Enligt definitionen av delbarhet finns då ett heltal q sådant att $a = b \cdot q$. Vi kallar q *kvoten mellan a och b* och skriver

$$q = \frac{a}{b}.$$

Övningar

Övning 1.1. Hitta talen q och r i formeln $a = b \cdot q + r$, där $0 \leqslant r < b$, i fallen då

1. $a = 32$, $b = 13$,
2. $a = -24$, $b = 7$,
3. $a = 1762$, $b = 10$,
4. $a = 10$, $b = 1726$,
5. $a = -70$, $b = 35$.

Övning 1.2. Låt a och b vara heltal, där $b \neq 0$. Visa att om $a \cdot b = 0$ så måste $a = 0$.

Övning 1.3. Betrakta några heltal a och b, där $b \neq 0$. Antag att heltalen q, r och $\tilde{r}$ uppfyller

$$a = b \cdot q + r \quad \text{och} \quad a = b \cdot q + \tilde{r}.$$

Visa att $r = \tilde{r}$.

Övning 1.4. Låt a och b vara heltal där $b \neq 0$. Antag att det finns heltal $q, \tilde{q}$ och r sådana att

$$a = b \cdot q + r \quad \text{och} \quad a = b \cdot \tilde{q} + r.$$

Visa att $q = \tilde{q}$.

Anmärkning: Detta betyder att kvoten q vid heltalsdivision är unikt bestämd.

Övning 1.5. Visa följande egenskaper hos delarrelationen:

1. För alla heltal a gäller $a \mid a$.
2. Låt a, b, c vara heltal. Om $a \mid b$ och $b \mid c$ så gäller $a \mid c$.
3. Det är inte så att om $a \mid b$ så gäller $b \mid a$, för alla heltal a, b.