Kapitel 3: Aritmetik

Kasper K. S. Andersen

23 september 2021

Division med rest

Exempel 1. Vi har $\frac{23}{4} = 5 + \frac{3}{4}$. Ekvivalent gäller (multiplicera med 4)

$$23 = \underbrace{5}_{\text{kvot}} \cdot 4 + \underbrace{3}_{\text{rest}}$$

Observera att resten uppfyllar $0 \leq 3 < 4$.

Sats 3.1: Om $a, b \in \mathbb{Z}$, $b \neq 0$ finns *unika* tal $k, r \in \mathbb{Z}$ så att

$$a = \underbrace{k}_{\text{kvot}} \cdot b + \underbrace{r}_{\text{rest}} \qquad \text{och } 0 \leq r < |b|.$$

Anmärkning: Observera att vi skriver $|b|$ och inte b då vi tillåter $b < 0$.

Delare i $\mathbb{Z}$

Om man får resten 0 vid division prater vi om *delare*.

Definition 1. Låt $a, b \in \mathbb{Z}$. Vi säger att b *delar* a eller b *är delare i* a om det finns heltal k så att $a = k \cdot b$. Detta skrivas $b \,|\, a$. Om inte det finns ett sådant k skrivs $b \nmid a$, i ord: b *delar inte* a.

Exempel 2. Vi har

- $3 \,|\, 12$, 3 delar 12, ty $\underbrace{12}_{a} = \underbrace{4}_{k} \cdot \underbrace{3}_{b}$
- $-3 \,|\, 12$
- $2 \,|\, -6$

- $5 \nmid 6$
- Delarne i 30: $\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$

Anmärkning:

- Uppenbart gäller $\pm 1 \,|\, a$ och $\pm a \,|\, a$ för alla heltal a.
- Dessutom gäller $b \,|\, 0$ för alla heltal b.
- Det gäller att $0 \,|\, 0$ ty $\underbrace{0}_{a} = \underbrace{k}_{k} \cdot \underbrace{0}_{b}$ för alla heltal k (observera att definitionen *inte* involverar $\frac{0}{0}$). Dessutom gäller $0 \nmid a$ för $a \neq 0$ ty det finns inga heltal k så att $\underbrace{a}_{a} = \underbrace{k}_{k} \cdot \underbrace{0}_{b}$

Definition 2. Ett heltal $p > 1$ som endast har delarne ± 1 och $\pm p$ kallas ett *primtal*, tex. $2, 3, 5, 7, 11, 13, 17, 19, \ldots$

Ett heltal $n > 1$ kallas *sammansatt* om det inte är ett primtal, dvs. om det har andra delare än ± 1 och $\pm n$.

Exempel 3.
- 7 är ett primtal då det endast har delarne ± 1 och ± 7.
- 91 är sammansatt då $7 \,|\, 91$.
- Talen $x^2 - x + 41$ ett primtal för $x = 0, \ldots, 40$ (Leonhard Euler 1707–1783).
- Det största kända primtal i nuläget är $2^{82,589,933} - 1$ (december 2018) men det finns oändligt många (Euklides från Alexandria ca. 325–265 f.Kr.).

Moduloräkning

När man bara intresserar sig för resterna och inte bryr sig om kvoten, pratar man om *moduloräkning* (också kallad *klockaritmetik*, jmf. figuren i Exempel 3.6, s. 55).

Definition 3. Två heltal a och b kallas *kongruenta modulo* n om de ger *samma rest* vid division med n. Detta skrivs: $a \equiv b \pmod{n}$.

Anmärkning: Det gäller $a \equiv b \pmod{n} \iff n \,|\, a - b$.

Exempel 4. Vi sätter oss på tåget kl. 21. När kommer vi fram om resan tar 35h?

Lösning: Vi utför division med 24 och kollar på resten.

$$21 + 35 = 56 = \underbrace{2}_{\text{kvot}} \cdot 24 + \underbrace{8}_{\text{rest}} \equiv 8 \pmod{24}.$$

Anmärkning: Om man räknar med resterna vid *division med* n så räknar man *modulo* n.

Exempel 5. (a) $5 \equiv 14 \pmod 3$, ty

$$\left.\begin{array}{rl} 5 = 1 \cdot 3 + 2 \equiv 2 & \pmod 3 \\ 14 = 4 \cdot 3 + 2 \equiv 2 & \pmod 3 \end{array}\right\} \text{samma rest}$$

Alternativ: $5 - 14 = -9$ och $3 | -9$.

(b) $25 \equiv -3 \pmod 7$, ty

$$\left.\begin{array}{rl} 25 = \quad 3 \cdot 7 + 4 \equiv 4 & \pmod 7 \\ -3 = -1 \cdot 7 + 4 \equiv 4 & \pmod 7 \end{array}\right\} \text{samma rest}$$

Alternativ: $-3 - 25 = -28$ och $7 | -28$.

• Läs Exempel 3.4, s. 53, Exempel 3.5, s. 54 och Exempel 3.6, s. 55..

Exempel 6. Beräkna $16 + 43 \pmod 3$.

Lösning:
Alternativ 1: $16 + 43 = 59 = 19 \cdot 3 + 2 \equiv 2 \pmod 3$.
Alternativ 2: $16 = 5 \cdot 3 + 1 \equiv 1 \pmod 3$ och $43 = 14 \cdot 3 + 1 \equiv 1 \pmod 3$ varför

$$16 + 43 \equiv 1 + 1 = 2 \pmod 3.$$

Exempel 7. Beräkna $16 \cdot 43 \pmod 3$.

Lösning:
Alternativ 1: $16 \cdot 43 = 688 = 229 \cdot 3 + 1 \equiv 1 \pmod 3$.
Alternativ 2: $16 \equiv 1 \pmod 3$ och $43 \equiv 1 \pmod 3$ varför

$$16 \cdot 43 \equiv 1 \cdot 1 = 1 \pmod 3.$$

Restklasser

Definition 4. Om a och n är heltal, $n \neq 0$, definieras *restklassen*

$$[a]_n = \{b \mid b \equiv a \pmod{n}\} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$

som mängden av alla tal som är kongruenta med a modulo n.

Anmärkning: Observera att $a \equiv b \pmod{n} \iff [a]_n = [b]_n$.

Exempel 8. För $n = 6$ fås de 6 restklasserna

$$\begin{aligned}
[0]_6 &= \{\ldots, -18, -12, -6, 0, \ \ 6, 12, 18, 24, \ldots\},\\
[1]_6 &= \{\ldots, -17, -11, -5, 1, \ \ 7, 13, 19, 25, \ldots\},\\
[2]_6 &= \{\ldots, -16, -10, -4, 2, \ \ 8, 14, 20, 26, \ldots\},\\
[3]_6 &= \{\ldots, -15, -9, -3, 3, \ \ 9, 15, 21, 27, \ldots\},\\
[4]_6 &= \{\ldots, -14, -8, -2, 4, 10, 16, 22, 28, \ldots\},\\
[5]_6 &= \{\ldots, -13, -7, -1, 5, 11, 17, 23, 29, \ldots\},
\end{aligned}$$

Sats: For $n > 0$ ger de n restklasserna

$$[0]_n, [1]_n, \ldots, [n-1]_n$$

en *partition* av $\mathbb{Z}$, dvs. de är disjunkta och unionen är $\mathbb{Z}$.

Definition 5. För $n > 0$ betecknar

$$\mathbb{Z}_n = \left\{ [a]_n \,|\, a \in \mathbb{Z} \right\} = \left\{ [0]_n, [1]_n, \ldots, [n-1]_n \right\}$$

mängden av möjliga restklasser modulo n. Vi har $|\mathbb{Z}_n| = n$.

Exempel 9. Vi har $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$, $\quad |\mathbb{Z}_6| = 6$.