Diskret matematikk – onsdag 1. okt. 2014

Avsnitt 4.1 fra læreboken Heltallsdivisjon

La a og b være to heltall med $a \neq 0$. Vi sier at

a går opp i b (eng: a divides b) hvis det finnes et heltall c slik at $b = ac$. I så fall kalles a en faktor i b og omvendt er da b et multiplum av a. (eng: b is a multiple of a).

Symboler Vi skriver $a \mid b$ hvis a går opp i b og $a \nmid b$ hvis a ikke går opp i b.

Eksempler

3 går opp i 12 siden $12 = 3 \cdot 4$, dermed $3 \mid 12$.
4 går opp i 28 siden $28 = 7 \cdot 4$, dermed $4 \mid 28$
5 går ikke opp i 28, dermed $5 \nmid 28$.

OBS

a) Tallet 1 går opp i alle hele tall.
b) Alle hele tall $\neq 0$ går opp i 0.
c) Alle hele tall $\neq 0$ går opp i seg selv.

Regneregler

1) Hvis $a \mid b$ og $a \mid c$, så $a \mid (b+c)$.
2) Hvis $a \mid b$ og $a \mid c$, så $a \mid (mb+nc)$.
3) Hvis $a \mid b$ og $b \mid c$ $(b \neq 0)$, så $a \mid c$.
4) Hvis $a \mid b$, så $a \mid b \cdot c$ for alle c.
5) Hvis $a \mid b$ og $a \nmid c$, så $a \nmid (b+c)$.

Eksempel på bruk av regel 5

1) Går 7 opp i 101? Vi vet at 7 går opp i 77, men 7 går ikke opp i $101-77=24$. Da kan 7 ikke gå opp i 101.

2) Går 3 opp i 1001? Vi vet at 3 går opp i 999, men 3 går ikke opp i $1001-999=2$. Dermed kan 3 ikke gå opp i 1001.

Divisjonsalgoritmen

La a og d være hele tall med $d>0$. Da fennes det entydige hele tall q og r slik at $a=qd+r$ og $0 \leq r < d$. Her kalles a dividend, d divisor, q kvotient og r rest.

Eksempler

1) $a=33, d=17$. Da blir $q=1$ og $r=16$.
2) $a=123, d=7$. Da blir $q=17$ og $r=4$.
3) $a=7, d=11$. Da blir $q=0$ og $r=7$.
4) $a=0, d=3$. Da blir $q=0$ og $r=0$.

Definisjon av div og mod

$$\boxed{a \text{ div } d = q \;,\; a \text{ mod } d = r}$$

OBS I Java (og andre programmeringsspråk) vil hvis $a \geq 0$ og $d>0$, $a/d = a \text{ div } d$ og $a\%d = a \text{ mod } d$. Hvis $a<0$ og $d>0$, er det annerledes. Da vil $a \text{ div } d = -(1+(-a)/d)$ og $a \text{ mod } d = d-(-a\%d)$.

Div og mod ved gjentatt subtraksjon

Vi starter med a og d. Vi trekker fortløpende d fra a inntil vi får et resultat som er mindre enn d. Resultatet blir resten r og antallet ganger vi trakk fra blir kvotienten q.

Javakode for gjentatt subtraksjon:

```
public static void divisjon(int a, int d)
{
  int r = a < 0 ? -a : a; // skifter fortegn hvis a er negativ
  int q = 0;

  while (r >= d)
  {
    r -= d;
    q++;
  }

  if (a < 0)
  {
    q = -(q + 1);
    r = d - r;
  }

  System.out.println("Kvotient: " + q + "  Rest: " + r);
}
```

OBS Den matematiske definisjonen av kvotient q og rest r sier at $0 \leq r < d$ der d er divisor. Med andre ord er resten aldri negativ.

Hvis $a = -123$ og $d = 7$, vil $q = -18$ og $r = 3$ siden $-123 = -18 \cdot 7 + 3$. Hvis a er negativ, finner en først q og r for $-a$ (her $--123 = 123$). Det gir $q = 17$ og $r = 4$. Rett svar for a blir da $q = -(q+1) = -(17+1) = -18$ og $r = d - r = 7 - 4 = 3$.

OBS I Java vil $-123 \% 7 = -4$ og $-123 / 7 = -17$.

Modulo regning

La m være et positivt heltall (dvs. $m > 0$).
Vi sier at to hele tall a og b er kongruente modulo m hvis m går opp i $a - b$.
Dette betegnes med

$$a \equiv b \pmod{m}$$

Vi skriver $a \not\equiv b \pmod{m}$ hvis a og b ikke er kongruente modulo m.

OBS Hvis $a \equiv b \pmod{m}$, så er $b \equiv a \pmod{m}$.

Setning La $m > 0$. Da er $a \equiv b \pmod{m}$ hvis og bare hvis $a \bmod m = b \bmod m$.

Eksempel 1 La $m = 3$, $a = 2$, $b = 17$.

Er $a \equiv b \pmod{m}$? Dvs. er $2 \equiv 17 \pmod{3}$?

1) Ja, fordi 3 går opp i $2 - 17 = -15$. Definisjonen
2) Ja, fordi $2 \bmod 3 = 2$ og $17 \bmod 3 = 2$. Setningen

Eksempel 2 La $m = 3$, $a = 8$, $b = 4$.

Er $8 \equiv 4 \pmod{3}$?

1) Nei, fordi 3 går ikke opp i $8 - 4 = 4$. Definisjonen.
2) Nei, fordi $8 \bmod 3 = 2$ er ulik $4 \bmod 3 = 1$. Setningen.

Eksempel 3 Vi fant at $2 \equiv 17 \pmod 3$.

Hvilke andre tall enn 17 er kongruent med 2 modulo 3? Vi ser at f.eks $2 \equiv 14 \pmod 3$, $2 \equiv 11 \pmod 3$, osv. $\cdots$ $2 \equiv 2 \pmod 3$.

Vi forstår dermed at alle heltall på formen $2+3k$ vil være kongruent med 2 modulo 3.

Regel La $m > 0$ og a et heltall. Da vil alle heltall på formen $a+mk$ der k er et vilkårlig heltall, være kongruent med a modulo m.

Eksempel $m = 7$, $a = 1$. Finn fem forskjellige heltall b slik $a \equiv b \pmod m$.

Svar: La $b = a + mk = 1 + 7k$. Vi kan f.eks. velge $k = 0, 1, 2, -1, -2$. Da får vi flg. tall

$$1, 8, 15, -6, -13$$

Regneregler for kongruenser

La $m > 0$ og anta at $a \equiv b \pmod m$ og $c \equiv d \pmod m$.

i) $a + c \equiv b + d \pmod m$

ii) $ac \equiv bd \pmod m$

Eksempel: $1 \equiv 8 \pmod 7$ og $15 \equiv -6 \pmod 7$. Dermed er $1 \cdot 15 \equiv 8 \cdot (-6) \pmod 7$. Dvs. $15 \equiv -48 \pmod 7$. –