MA2047 Algebra och diskret matematik

Något om heltal

Mikael Hindgren

HÖGSKOLAN I HALMSTAD

16 september 2024

Delbarhet

HÖGSKOLAN I HALMSTAD

Exempel 1

$42 = 6 \cdot 7$

- Vi säger: "7 är en faktor i 42" eller "7 delar 42"
- Vi skriver: $7 \mid 42$

Definition 1

- Om $a, b \in \mathbb{Z}$ så säger vi att b delar a ($b \mid a$) om det finns ett $c \in \mathbb{Z}$ sådant att $a = b \cdot c$.
- Om $b \mid a$ men $b \neq \pm a$ och $b \neq \pm 1$ så är b en äkta delare.

Exempel 2

- $54 = 6 \cdot 9 \Rightarrow 6 \mid 54$
- $17 = \underbrace{2}_{kvot} \cdot 7 + \underbrace{3}_{rest} \Rightarrow 7 \nmid 17$
- $75 = (-5) \cdot (-15) \Rightarrow -5 \mid 75$
- $0 = b \cdot 0 \Rightarrow b \mid 0 \ \forall\, b \in \mathbb{Z}$

Delbarhet

Exempel 3

Är talet $131 \cdot 42 + 64 \cdot 63$ delbart med 7?

- $7 \mid 42$ och $7 \mid 63$
  $\Rightarrow 131 \cdot 42 + 64 \cdot 63 = 131 \cdot 7 \cdot 6 + 64 \cdot 7 \cdot 9 = 7(131 \cdot 6 + 64 \cdot 9)$

$\therefore \underset{a}{7} \mid (\underset{x}{131} \cdot \underset{b}{42} + \underset{y}{64} \cdot \underset{c}{63})$

Sats 1

Om $a, b, c \in \mathbb{Z}$ så gäller:

1. $a \mid b$ *och* $b \mid c \Rightarrow a \mid c$
2. $a \mid b$, $a \mid c$ *och* $x, y \in \mathbb{Z} \Rightarrow a \mid (xb + yc)$

Divisionsalgoritmen

Exempel 4

Vi beräknar $\frac{787}{15}$ med trappan:

$$
\begin{array}{r@{\,}l}
 & 52 \\ \cline{2-2}
15 \big) & 787 \\
 & \underline{75} \\
 & 37 \\
 & \underline{30} \\
 & 7
\end{array}
$$

$$\therefore 787 = 50 \cdot 15 + 2 \cdot 15 + 7 = \underbrace{52}_{kvot} \cdot 15 + \underbrace{7}_{rest}$$

Sats 2 (Divisionsalgoritmen)

Om $a, b \in \mathbb{Z}$, $b > 0$, så finns det två entydigt bestämda tal $q, r \in \mathbb{Z}$ sådana att

$$a = \underbrace{q}_{kvot} \cdot b + \underbrace{r}_{rest}, \qquad 0 \leq r < b \qquad (r = \textit{principalrest})$$

Exempel 5

$87 = \underbrace{6}_{kvot} \cdot 14 + \underbrace{3}_{rest} \leftarrow$ principalrest: $0 \leq 3 < 14$

Primtal

Definition 2

Ett heltal $p \geq 2$ som saknar äkta delare kallas ett primtal.

Exempel 6

Primtalen: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$

Exempel 7

$15 = 3 \cdot 5, \quad 42 = 7 \cdot 6 = 7 \cdot 3 \cdot 2, \quad 93500 = 2^2 \cdot 5^3 \cdot 11 \cdot 17$

15, 42 och 93500 är produkter av primtal.

Sats 3 (Aritmetikens fundamentalsats)

Varje heltal $n \geq 2$ kan skrivas som en produkt av primtal:

$$n = p_1 \cdot p_2 \cdots p_k$$

Primtalsfaktorseringen är unik så när som på i vilken ordning primtalen skrivs.

Största gemensamma delare

Exempel 8

- Det största heltal som delar 49 och 35 är 7.
- Vi skriver $\text{SGD}(49, 35) = 7$ (Största gemensamma delare)
- $\text{SGD}(16, 23) = 1 \Rightarrow$ 16 och 23 är relativt prima

Exempel 9

Bestäm $\text{SGD}(996, 516)$

- Divisionsalgoritmen: $996 = 1 \cdot 516 + 480$
- $a \mid 516$ och $a \mid 480$
  $\Rightarrow a \mid \underbrace{516}_{b} \cdot \underbrace{1}_{x} + \underbrace{480}_{c} \cdot \underbrace{1}_{y} \Leftrightarrow a \mid 996$
- $a \mid 996$ och $a \mid 516$
  $\Rightarrow a \mid 996 \cdot \underbrace{1}_{x} + 516 \cdot \underbrace{(-1)}_{y} \Leftrightarrow a \mid 480$

$\Rightarrow$ Varje tal som delar 996 och 516 delar också 516 och 480 och omvänt.

$\therefore \text{SGD}(996, 516) = \text{SGD}(516, 480)$

Sats 1.2

$a \mid b,\ a \mid c \Rightarrow a \mid (xb + yc)$

Euklides algoritm

Exempel 9 (forts)

Vi fortsätter:

- $516 = 1 \cdot 480 + 36 \Rightarrow \text{SGD}(516, 480) = \text{SGD}(480, 36)$
- $480 = 13 \cdot 36 + 12 \Rightarrow \text{SGD}(480, 36) = \text{SGD}(36, 12)$
- $36 = 3 \cdot 12 + 0$

$\therefore \text{SGD}(996, 516) = \text{SGD}(36, 12) = 12$

Euklides algoritm

SGD$(996, 516)$:

Euklides algoritm

$$
\begin{aligned}
996 &= 1 \cdot 516 + 480 \\
516 &= 1 \cdot 480 + 36 \\
480 &= 13 \cdot 36 + 12 \\
36 &= 3 \cdot 12 + 0
\end{aligned}
$$

$$
\begin{aligned}
\text{SGD}(996, 516) &= \text{SGD}(516, 480), && 0 \leq 480 < 516 \\
\text{SGD}(516, 480) &= \text{SGD}(480, 36), && 0 \leq 36 < 480 \\
\text{SGD}(480, 36) &= \text{SGD}(36, 12), && 0 \leq 12 < 36
\end{aligned}
$$

- Vid varje division blir resten minst 1 mindre än föregående rest
  $\Rightarrow$ Till sist får man en rest som blir 0
- $\text{SGD}(996, 516) = 12 =$ Sista icke-försvinnande resten i Euklides algoritm

Euklides algoritm

Exempel 10

Bestäm $\text{SGD}(4379, 3473)$.
Euklides algoritm:

$$\begin{aligned} 4379 &= 1 \cdot 3473 + 906 \\ 3473 &= 3 \cdot 906 + 755 \\ 906 &= 1 \cdot 755 + 151 \leftarrow \text{ Sista icke-försvinnande resten} \\ 755 &= 5 \cdot 151 + 0 \end{aligned}$$

$\therefore \text{SGD}(4379, 3473) = 151$

I Mathematica: `GCD[4379,3473]`

Diofantiska ekvationer

Ekvationer där endast heltalslösningar söks:

- $5x + 7y = 1$ (Linjär). $x = -4,\ y = 3$ är en lösning.
- $x^2 + y^2 = z^2$ (Pythagoras ekvation). $x = 3,\ y = 4,\ z = 5$ är en lösning.
- $x^2 - ny^2 = 1,\ n \neq k^2$ (Pell's ekvation).
  Ex: $x^2 - 5y^2 = 1$. $x = 9$ och $y = 4$ är en lösning.
- Hilberts problem nr 10 (av 23) år 1900: *Går det att skriva en algoritm som för godtyckliga diofantiska ekvationer kan avgöra om de har några lösningar?*
  Nej! Bevisades av Yuri Matiyasevich 1970
- Världens mest berömda diofantiska ekvation:

Fermat's sista sats (Pierre de Fermat 1637):

Om $n, x, y, z \in \mathbb{Z}_+$ och $n \geq 3$ saknar ekvationen $x^n + y^n = z^n$ lösningar.

Bevisades av Andrew Wiles 1995. Beviset är 129 sidor långt...

Advokaten och amatörmatematikern Pierre de Fermat år 1637:
"Jag har ett i sanning underbart bevis för detta påstående, men marginalen är alltför trång för att rymma detsamma."

Diofantiska ekvationer

Exempel 11

Vid en teaterföreställning kostade inträdet 35 kr för barn och 45 kr för vuxna. Biljetter såldes för totalt 10000 kr. Vilket är det maximala antalet barn som kan ha sett föreställningen?

- Sätt $x =$ antal barn, $y =$ antal vuxna
- Vi söker de icke-negativa heltalslösningarna till ekvationen

$$35x + 45y = 10000 \quad \leftarrow \text{Diofantisk ekvation}$$

Hur löser vi den?

Vi söker en lösningsformel för Diofantiska ekvationer av typen $ax + by = c$.

Diofantos var verksam i Alexandria ca 250 e.Kr. Han var bland de första som använde symbolisk notation inom matematiken och kallas ibland algebrans fader. Han skrev *Arithmetika*, en serie böcker som handlar om hur man löser vissa typer av algebraiska ekvationer.

Diofantiska ekvationer

Exempel 12

Sök heltalslösningar till ekvationen $42x + 28y = 56$

- $x = 2,\ y = -1$ är en lösning
- $x = 30,\ y = -43$ är en annan lösning

Finns det fler lösningar?

Exempel 13

Sök heltalslösningar till ekvationen $42x + 28y = 57$

- $\text{SGD}(42, 28) = 14$
- $14 \mid 42$ och $14 \mid 28 \Rightarrow 14 \mid (42x + 28y)$ enl Sats 1.2.
  $\Rightarrow 14 \mid 57$?!? Inte sant!

$\therefore$ Ekvationen saknar heltalslösningar!

Sats 4

Den Diofantiska ekvationen $ax + by = c$ har heltalslösningar omm $SGD(a, b) \mid c$

Diofantiska ekvationer

Exempel 14

Bestäm alla heltalslösningar till

$$36x + 51y = 21 \tag{1}$$

- $\text{SGD}(36, 51) = 3 \mid 21 \Rightarrow$ Ekvationen har heltalslösningar!
- Vi dividerar ekvationen med $\text{SGD}(36, 51) = 3$ för att få en enklare ekvation: $\Rightarrow 12x + 17y = 7$
- Om högerledet hade varit 1 kunde vi fått en lösning med hjälp av Euklides algoritm:

$$\begin{aligned} 17 &= 1 \cdot 12 + 5 \\ 12 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 1 &= 5 - 2 \cdot 2 = \underbrace{17 - 1 \cdot 12}_{=5} - 2\underbrace{(12 - 2 \cdot 5)}_{=2} \\ &= 17 - 1 \cdot 12 - 2(12 - 2(17 - 12)) \\ &= 12(-7) + 17 \cdot 5 \end{aligned}$$

$\therefore (x_0, y_0) = (-7, 5)$ är en lösning till $12x + 17y = 1$

- Multiplicerar vi hjälpekvationen med 7 får vi en lösning till (1): $12(7x_0) + 17(7y_0) = 7 \Rightarrow (x_1, y_1) = (7x_0, 7y_0) = (-49, 35)$

Diofantiska ekvationer

Exempel 14 (forts)

Hur hittar vi alla lösningar till

$$12x + 17y = 7\,?$$

Ansats: $x = x_1 + k, \quad y = y_1 + l, \quad k, l \in \mathbb{Z}$

- Insättning i ekvationen:
  $12(x_1 + k) + 17(y_1 + l) = \underbrace{12x_1 + 17y_1}_{=7} + \underbrace{12k + 17l}_{=0} = 7$
- (x, y) är en lösning omm $12k + 17l = 0 \Leftrightarrow 12k = -17l$
- $\mathrm{SGD}(12, 17) = 1 \Rightarrow 12 \mid l$ och $17 \mid k$
  $\Rightarrow l = 12n,\ n \in \mathbb{Z} \Rightarrow 12k = -17 \cdot 12n \Rightarrow k = -17n$
- Lösningarna till (1) är därför
  $(x, y) = (x_1 - 17n, y_1 + 12n) = (7x_0 - 17n, 7y_0 + 12n)$

Diofantiska ekvationer

Sats 5

Den Diofantiska ekvationen

$$ax + by = c, \quad SGD(a, b) = 1$$

har den allmänna lösningen

$$(x, y) = (cx_0 \mp nb, cy_0 \pm na), \; n \text{ godtyckligt heltal}$$

där (x_0, y_0) *är en lösning till hjälpekvationen* $ax + by = 1$.

Diofantiska ekvationer

HÖGSKOLAN I HALMSTAD

Exempel 11 (Teaterbesök forts)

Ursprunglig ekvation: $35x + 45y = 10000$

- $\text{SGD}(35, 45) = 5 \mid 10000 \Rightarrow$ Ekvationen har heltalslösning!
- Dividera ekv med $\text{SGD}(35, 45) = 5 \Rightarrow 7x + 9y = 2000$
- Bestäm en lösning till hjälpekvationen $7x + 9y = 1$ mha Euklides algoritm:

$$\begin{aligned} 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \quad \Rightarrow \quad 1 = 7 - 3 \cdot 2 = 7 - 3(9 - 1 \cdot 7) = 7 \cdot 4 + 9 \cdot (-3) \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

$\therefore (x_0, y_0) = (4, -3)$

- Allmän lösning enligt Sats 5:

Sats 5 (Diofantiska ekvationer)

$$\begin{cases} ax + by = c, \\ \text{SGD}(a, b) = 1 \end{cases} \Rightarrow (x, y) = (cx_0 \mp nb, cy_0 \pm na)$$

$$(x, y) = (2000x_0 - 9n, 2000y_0 + 7n) = (8000 - 9n, -6000 + 7n), \; n \in \mathbb{Z}$$

Diofantiska ekvationer

Exempel 11 (Teaterbesök forts)

Antal barn $x \geq 0$ och antal vuxna $y \geq 0$:

- $x \geq 0 \Leftrightarrow 8000 - 9n \geq 0 \Leftrightarrow n \leq \dfrac{8000}{9} = 888.888\ldots \Leftrightarrow n \leq 888$
- $y \geq 0 \Leftrightarrow -6000 + 7n \geq 0 \Leftrightarrow n \geq \dfrac{6000}{7} = 857.142\ldots \Leftrightarrow n \geq 858$

$\Rightarrow x_{\text{max}} = 8000 - 858 \cdot 9 = 278$

$\therefore$ Högst 278 barn såg föreställningen.

Diofantiska ekvationer i Mathematica: $492x + 396y = 9552$

- Allmän lösning:

```
Reduce[492x+396y==9552,{x,y},Integers]
```

- Alla positiva lösningar:

```
Reduce[492x+396y==9552 && x>0 && y>0,{x,y},Integers]
```