
Euklides algoritm för största gemensamma delaren

Givet två naturliga tal a och b , som inte båda två är 0, hur räknar man ut största gemensamma delaren av a och b ?

Euklides har kommit på en metod (algoritm) för detta:

0. Börja med att skriva ner de två talen a och b på en rad.

Nu upprepar vi detta:

1. Titta på raden vi har just skrivit ner, där vi har talen x och y .

2. Vi är färdiga om ...:

- ... något av talen är 0: Slutgiltiga svaret är det andra talet.
- (- ... något av talen är 1: Slutgiltiga svaret är då 1.
- ... talen är lika: Slutgiltiga svaret är då det talet.)

3. Om vi inte är färdiga än, då skapar vi en ny rad med två nya tal:

- om $x > y$, då är de nya talen $(x-y)$ och y
- om $x < y$, då är de nya talen x och $(y-x)$

4. Gå tillbaka till 1.

Exempel 1: Största gemensamma delaren av 6 och 21 är 3:

6	21	(start)
6	15	($15 = 21 - 6$)
6	9	($9 = 15 - 6$)
6	3	($3 = 9 - 6$)
3	3	($3 = 6 - 3$)

vi är färdiga och svaret är 3.

Exempel 2: Största gemensamma delaren av 8 och 21 är 1:

8	21	(start)
8	13	(13 = 21 - 8)
8	5	(9 = 13 - 8)
3	5	(3 = 8 - 5)
3	2	(2 = 5 - 3)
1	2	(1 = 3 - 2)

vi är färdiga och svaret är 1.

Varför fungerar detta? Vi behöver visa två saker: (1) processen kommer att ta slut någon gång, och (2) när den tar slut producerar den rätt svar.

För att visa (1) räcker det med att konstatera att summan av de två talen på varje rad alltid är positiv. Dessutom minskar summan av talen på varje rad i varje steg. Alltså finns det bara ett begränsat antal steg vi kan ta innan vi är färdiga.

För att visa (2) konstaterar vi först att största gemensamma delaren av de två talen på varje rad är samma som den största gemensamma delaren av de två talen på föregående raden. Detta är så för att vi vet att:

$$\text{sgd}(x,y) = \text{sgd}(x-y,y) = \text{sgb}(x,y-x)$$

Vi har alltså hittat en *invariant*. Största gemensamma delaren av de två talen på varje rad är alltså samma som den största gemensamma delaren av de två talen vi började med: a och b.

Dessutom producerar vi rätt svar när vi slutar därför att:

$$\begin{aligned} \text{sgd}(0,x) &= x \\ \text{sgd}(x,0) &= x \\ \text{sgd}(x,x) &= x \\ \text{sgd}(1,x) &= 1 \\ \text{sgd}(x,1) &= 1 \end{aligned}$$

Vi kan göra en liten ändring i metoden. I stället för att hela tiden räkna ut $a-b$ eller $b-a$ kan vi istället räkna ut $a \text{ `rest` } b$ eller $b \text{ `rest` } a$. Detta är korrekt eftersom $a \text{ `rest` } b$ är ju resultatet man får när man drar av b från a upprepade gånger.

Detta leder till metoden som beskrivs i boken.

Detta är också metoden man ska använda när man implementerar detta i ett program. (När man räknar för hand har man sällan så stora tal att det lönar sig.)

Bezouts identitet

Givet a, b . Vi vill lösa följande ekvation:

$$a \cdot u + b \cdot v = \text{gcd}(a,b)$$

Där u och v måste vara heltal!

För att hitta en lösning föreslår boken att man kör Euklides algoritm "baklänges". Jag beskriver en annan metod här som jag finner enklare.

Man börjar med att göra tabellen som tillhör att räkna sgd:n av a och b . Denna består utav 2 kolumner som vi kallar för A och B. (Överst i kolumn A skriver vi a , och överst i kolumn B skriver vi b .)

Sen lägger man till 2 kolumner på vänster sidan, och 2 kolumner på höger sidan.

I de vänstra 2 kolumnerna skriver vi värden på u och v sådant att $a \cdot u + b \cdot v$ blir lika med talet som står på motsvarande rad i kolumn A. Och i de högre 2 kolumnerna skriver vi värden på u och v sådant att $a \cdot u + b \cdot v$ blir lika med talet som står på motsvarande rad i kolumn B.

I de vänstra 2 kolumnerna börjar vi således med $(1,0)$ eftersom $a \cdot 1 + b \cdot 0 = a$. Och i de högre 2 kolumnerna börjar vi med $(0,1)$ eftersom $a \cdot 0 + b \cdot 1 = b$.

I varje rad subtraherar vi antingen de vänstra kolumnerna från de högre, eller tvärtom, beroende på vad vi gjorde i sgd-tabellen.

Resultatet är att vi har en lösning (u,v) för alla tal som förekommer i sgd-tabellen! Inklusivt $\text{sgd}(a,b)$, som var det vi ville ha.

Bäst är att titta på några exempel.

Exempel 1. Vi vill lösa $6u + 21v = 3$.

Vi tar sgd-tabellen för $\text{sgd}(6,21)$, och lägger till 2 kolumner på vänstersidan och 2 kolumner på högersidan.

u	v			u	v	
1	0	6	21	0	1	(start!)
“	“	6	15	-1	1	$21 - 6$, alltså $(0,1) - (1,0) = (-1,1)$
“	“	6	9	-2	1	$15 - 6$, alltså $(-1,1) - (1,0) = (-2,1)$
“	“	6	3	-3	1	$9 - 6$, alltså $(-2,1) - (1,0) = (-3,1)$
		3	3			

Jag skriver “ “ när värdena är samma som raden ovan.

Vi kan sluta räkna när vi har nått en rad där sgd:n finns med (3 i detta fall).

Du kan kolla att (u,v)-kolumnerna har värden så att $6u + 21v$ är lika med respektive A och B kolumnen:

$$- 6 \cdot 1 + 21 \cdot 0 = 6$$

$$- 0 \cdot 6 + 1 \cdot 21 = 21$$

$$- (-1) \cdot 6 + 1 \cdot 21 = 15$$

$$- (-2) \cdot 6 + 1 \cdot 21 = 9$$

$$- (-3) \cdot 6 + 1 \cdot 21 = 3$$

Alltså har vi hittat en lösning: $u=-3, v=1$.

Exempel 2. Vi vill lösa $8u + 21v = 1$.

Vi tar sgd-tabellen för $\text{sgd}(8,21)$, och lägger till 2 kolumner på vänstersidan och 2 kolumner på högersidan.

u	v			u	v	
1	0	8	21	0	1	(start)
“	“	8	13	-1	1	$21 - 8$, alltså $(0,1) - (1,0) = (-1,1)$
“	“	8	5	-2	1	$13 - 8$, alltså $(-1,1) - (1,0) = (-2,1)$

3	-1	3	5	“	“	8 - 5, alltså (1,0) - (-2,1) = (3,-1)
“	“	3	2	-5	2	5 - 3, alltså (-2,1) - (3,-1) = (-5,2)
8	-3	1	2	“	“	3 - 2, alltså (3,-1) - (-5,2) = (8,-3)

Vi kan sluta räkna när vi har nått en rad där sgd:n finns med (1 i detta fall).

Du kan kolla att (u,v)-kolumnerna har värden så att $8u + 21v$ är lika med respektive A och B kolumnen:

$$- 8 \cdot 1 + 21 \cdot 0 = 8$$

$$- 8 \cdot 0 + 21 \cdot 1 = 21$$

$$- 8 \cdot (-1) + 21 \cdot 1 = 13$$

$$- 8 \cdot (-2) + 21 \cdot 1 = 5$$

$$- 8 \cdot 3 + 21 \cdot (-1) = 3$$

$$- 8 \cdot (-5) + 21 \cdot 2 = 2$$

$$- 8 \cdot 8 + 21 \cdot (-3) = 1$$

Alltså har vi hittat en lösning: $u=8$, $v=-3$.