Mårten Wadenbäck

Kongruens

Kongruensräkning (moduloräkning) liknar att räkna på klockan, dvs när talen blir för stora börjar man om från noll.

Exempel: Om klockan är prick 22 och det sedan går nio timmar blir klockan 7. I någon mening är alltså $22+9=7$ på klockan. Klockan x och klockan $x+24k$ är "samma" för alla heltal k.

Definition: Låt $n \geq 2$ vara ett heltal och låt $a, b \in \mathbb{Z}$. Om $n \mid a-b$ säger vi att a och b är <u>kongruenta modulo n</u>. Detta skriver vi $a \equiv b \mod n$.

För ett givet n kan vi studera kongruensrelationen på $\mathbb{Z}$,

$aRb \Leftrightarrow a \equiv b \bmod n$. Eftersom $n|0 \Leftrightarrow n|a-a$ gäller

det att $a \equiv a \bmod n$, så kongruens är reflexiv.

Symmetri följer av att $a \equiv b \bmod n \Leftrightarrow n|a-b \Leftrightarrow$

$n|b-a \Leftrightarrow b \equiv a \bmod n$. Om $a \equiv b \bmod n$ och $b \equiv c \bmod n$

så är $a-c = \underbrace{a-b}_{sn} + \underbrace{b-c}_{tn} = (s+t)n \Leftrightarrow n|a-c$,

dvs $a \equiv c \bmod n$, och kongruens är alltså transitiv.

De tre egenskaperna tillsammans gör att kongruens

är en ekvivalensrelation.

Vi erinrar oss att varje ekvivalensrelation svarade mot

en partition. Kongruensrelationen modulo n delar alltså in

heltalen i olika ekvivalensklasser. Hur många?

För ett godtyckligt heltal a säger divisionsalgoritmen

att det finns entydigt bestämda heltal q och r med $0 \leq r < n$

så att $a = qn + r \Leftrightarrow a - r = qn \Leftrightarrow a \equiv r \bmod n$.

Det finns alltså precis n olika ekvivalensklasser.

Definition: Vi betecknar $\mathbb{Z}_n = \{[0],[1],\dots,[n-1]\}$ och kallar $\mathbb{Z}_n$ för heltalen modulo n.

Anmärkning: Ekvivalensklasserna innehåller olika element beroende på vad n är. Om $n=7$ är $[2]=\{\dots,-12,-5,2,9,\dots\}$, men om $n=5$ är istället $[2]=\{\dots,-13,-8,-3,2,7,\dots\}$. Det måste alltså framgå vilket n vi menar.

Vi skall nu införa räkneoperationer på $\mathbb{Z}_n$, och för detta behöver vi följande sats.

Sats: Låt $n \geq 2$ och låt a, b, c, och d vara heltal sådana att $a \equiv b \mod n$ och $c \equiv d \mod n$. Då gäller att $a+c \equiv b+d \mod n$ och $ac \equiv bd \mod n$.

Bevis: Vi vet att $n | a-b \Leftrightarrow a-b = sn$ för något $s \in \mathbb{Z}$, och på samma sätt att $c-d = tn$ för något $t \in \mathbb{Z}$. Nu är $(a+c)-(b+d) = (a-b)+(c-d) = sn+tn = (s+t)n$, och alltså gäller $a+c \equiv b+d \mod n$.

För multiplikationen får vi

$$ac - bd = ac - ad + ad - bd =$$
$$= a(c-d) + (a-b)d = atn + snd = (at+sd)n,$$

så $ac \equiv bd \mod n$.

Definition: Vi inför nu de binära operatorerna $+$ och $\cdot$ på $\mathbb{Z}_n$ enligt följande formler:

$[a]+[b]=[a+b]$ för alla $[a],[b] \in \mathbb{Z}_n$,

$[a]\cdot[b]=[a\cdot b]$ för alla $[a],[b] \in \mathbb{Z}_n$.

Att resultatet av dessa operationer är entydigt garanteras av satsen ovan.

Exempel: Vad blir

a) $[31]+[6]$ i $\mathbb{Z}_{12}$? b) $[-2]\cdot[4]$ i $\mathbb{Z}_3$?

c) $[7]+[3]$ i $\mathbb{Z}_5$? d) $[2]\cdot[8]$ i $\mathbb{Z}_{13}$?

Sats: För varje heltal $n \geq 2$ gäller det att $[0]$ är identiteten med avseende på addition och $[1]$ är identiteten med avseende på multiplikation.

Exempel: I $\mathbb{Z}_4$ kan vi göra upp följande tabeller för addition och multiplikation:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Anmärkning: När vi beräknade $[2]\cdot[2]$ blev resultatet "noll" trots att $[2]\neq[0]$. I $\mathbb{Z}_n$ kan det alltså förekomma så kallade <u>nolldelare</u>. Detta är vi inte vana vid eftersom $ab=0 \Rightarrow a=0 \vee b=0$ för vanliga tal a och b. Detta gör att vi inte alltid kan förkorta: $[2]\cdot[1]=[2]\cdot[3]$ i $\mathbb{Z}_4$ men $[1]\neq[3]$.

För fullständighets skull inför vi även $[a]-[b]=[a-b]$ $\forall a,b\in\mathbb{Z}$ och $[a]^m=\underbrace{[a]\cdot[a]\cdots[a]}_{m \text{ st}}=[a^m]$ för heltal $m\geq 0$ och a.

Division går inte att definiera så att den alltid fungerar.

Exempel: Beräkna $[3]^{2017}$ i $\mathbb{Z}_{20}$. Eftersom 3^{2017} är ett tal med 963 siffror vill vi undvika att behöva räkna ut 3^{2017} och sedan beräkna resten när detta tal delas på 20. Istället kan vi räkna

$$[3]^{2017} = [3]\cdot[3]^{2016} = [3]\cdot([3]^2)^{1008} = [3]\cdot[9]^{1008} =$$
$$= [3]\cdot([9]^2)^{504} = [3]\cdot[1]^{504} = [3].$$

Sats: Låt $n \geq 2$ vara ett heltal och låt $[b] \in \mathbb{Z}_n$.

Då finns det ett unikt element $[c] \in \mathbb{Z}_n$ sådant att $[b][c] = [1]$ om och endast om $sgd(b,n) = 1$.

Bevis: Vi vill alltså ha ett c sådant att $bc \equiv 1 \mod n$, eller med andra ord $bc = 1 + kn \Leftrightarrow bc - kn = 1$ för något heltal k. Detta är en diofantisk ekvation, och vi har tidigare visat att den är lösbar precis då $sgd(b,n) = 1$.

Exempel: $[1]$ är alltid sin egen invers i $\mathbb{Z}_n$, och likadant är $[-1] = [n-1]$ sin egen invers. Däremot saknar $[0]$ alltid invers eftersom $sgd(0,n) = n \neq 1$.

Exempel: Finns det någon invers till $[40]$ i $\mathbb{Z}_{77}$?

Vi använder Euklides algoritm och

beräknar sgd(77,40):

$$77 = 1\cdot 40 + 37$$
$$40 = 1\cdot 37 + 3$$
$$37 = 12\cdot 3 + 1$$
$$12 = 12\cdot 1$$

Alltså är sgd(77,40) = 1, och [40] har en invers.

För att bestämma inversen räknar vi baklänges i Euklides algoritm:

$$1 = 37 - 12\cdot 3 = 37 - 12(40 - 1\cdot 37) = 37 - 12\cdot 40 + 12\cdot 37 =$$
$$= 13\cdot 37 - 12\cdot 40 = 13(77 - 1\cdot 40) - 12\cdot 40 =$$
$$= 13\cdot 77 - 13\cdot 40 - 12\cdot 40 = 13\cdot 77 - 25\cdot 40.$$

Inversen till [40] är [-25] = [52]. Vi kan kontrollera att [40]·[52] = [40·52] = [2080] = [540] = [1].