

Föreläsning 13

Antecknin... TMV200 Föreläsningar

Skapad: 2020-12-04 07:56

Ändrad: 2020-12-04 09:48

Författare: hchristian.johansson@gmail.com

TMV200 4/12 - 20

Protokollet för mittmötet ligger uppe på Canvas.

(8/12)

Schema: Föreläsningen på tisdag är 13.15-15.00.

Tidigare: Delbarhet, primtal.

Idag:

Kongruenser

Idag är det fredag. Vilken veckodag är det om

4 dagar? Tisdag.

12 dagar? Onsdag.

108 dagar? Måndag.

Hur kan man räkna? Cyklar om 7 dagar.

12 dagar blir samma som 5 dagar, eftersom

$$12 = 7 + 5$$

$108 = 7 \cdot 15 + 3$ blir samma som 3 dagar.

Matematiskt kan man ställa upp det så här:

Måndag - söndag blir 1 till 7, så

fredag = 5.

$$5+4-9 = 7+2, \quad 2 = tisdag$$

$$5+12 = 17 = 2 \cdot 7 + 3, \quad 3 = onsdag.$$

$$5+108 = 113 = 7 \cdot 16 + 1, \quad 1 = måndag.$$

Det här kallas för resträkning modulo 7 eller
Kongruensräkning modulo 7

7 är "cykeln".

Man kan alltid byta ut ett tal mot sin rest vid
division med 7 utan att ändra "slutresten":

$$108 = 7 \cdot 15 + 3$$

$$5+108 = 113 \text{ gav rest } 1$$

$$5+3 = 8 \text{ ger också rest } 1.$$

Finner andra naturliga exempel med andra cykler,
exempelvis klockan, har cykel 12 eller 24 timmar.

Rent matematiskt kan vi välja vilket $n \in \mathbb{Z}_+$
som cykel.

Sen vill vi betrakta alla heltalet med samma
rest vid division med n som "samma".

... \Rightarrow Ekvivalensrelation!

Hur - -

Def Låt $n \in \mathbb{Z}_+$. Vi definierar en relation
 $a \equiv b \pmod{n}$ (kongruens modulo n)

på \mathbb{Z} genom att säga att

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

om $n \mid (a-b)$, dvs $a-b$ är en
multipel av n .

Utläses "a är kongruent med b modulo n".

Skrivs oftast $a \equiv b \pmod{n}$ eller
 $a \equiv b \pmod{n}$

Ex $n = 4$:

$$3 \equiv 7 \pmod{4}, \text{ eftersom}$$

$3-7 = -4$ är en multipel av 4.

$2 \not\equiv 5 \pmod{4}$: $2-5 = -3$ är
inte en multipel
av 4.

$$86 \equiv 2 \pmod{4}, \text{ eftersom}$$

$$86-2 = 84 = 4 \cdot 21.$$

Sats Kongruens modulo n är en ekvivalensrelation.

Bem: Reflexivitet:

$$a \equiv a \pmod{n} \text{ eftersom } n \mid a-a=0$$

Symmetri:

$$\begin{aligned} \overline{a \equiv b \pmod{n}} &\stackrel{\text{def}}{\iff} n \mid a-b \iff n \mid -(a-b) = b-a \\ &\stackrel{\text{def}}{\iff} b \equiv a \pmod{n}. \end{aligned}$$

Transitivitet:

$$\begin{aligned} a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} &\stackrel{\text{def}}{\iff} n \mid a-b \wedge n \mid b-c \\ \Rightarrow n \mid (a-b)+(b-c) &= a-c \stackrel{\text{def}}{\iff} a \equiv c \pmod{n}. \end{aligned}$$

Alltså är kongress modulo n reflexiv, transitiv
och symmetrisk, dvs en ekvivalensrelation.

□

Låt oss tolka $\equiv \pmod{n}$ i termer av rester vid
division med n .

Divisionsalgoritmen gäller även för $a \in \mathbb{Z}, b \in \mathbb{Z}_+$:

Det finns tra, minsta, heltal $q, r \in \mathbb{Z}$ så att

$$a = bq + r, \quad 0 \leq r < b.$$

Så om $a \in \mathbb{Z}, n \in \mathbb{Z}_+$ finns det ett unikt
 $r \in \mathbb{Z}$ med $0 \leq r \leq n-1$ så att

$$n \mid a-r, \quad \text{dvs}$$

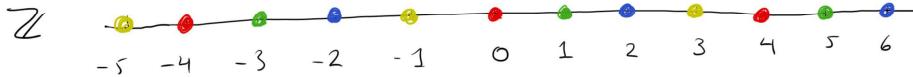
$$a \equiv r \pmod{n}$$

Dvs: Varje heltal är kongruent med ett unikt
heltal mellan 0 och $n-1$.

Ekvivalensklasserna för $\equiv \pmod{n}$ är alltså

$$[0], [1], [2], \dots, [n-1]$$

$$\begin{array}{l} \text{Ex : } \\ \hline = \end{array}$$

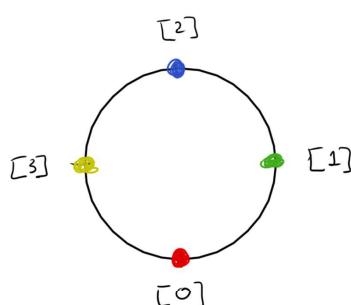


$$R \circ d : \text{Equivalezklassen } [0] = \{-4, 0, 4, 8, 12, \dots\}$$

Frage: Äquivalenzklassen [1]

B12 : Äquivalenzklassen [2]

Einf.: Äquivalenzklassen [3]



Kan finna oss
en "talcykel".

$$Vi \text{ skriver } \mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

for mängden av alla elevrikets klasser modulo n .

Vi shall definiera addition, subtraktion och multiplikation på \mathbb{Z}_n .

Följande sats s̄ges här +, - och · interagerar
med \equiv (n):

Sats: Antag att $a \equiv c \pmod{n}$ och $b \equiv d \pmod{n}$.

Då är :

$$1) \quad a+b \equiv c+d \quad (n)$$

$$2) \quad a - b \equiv c - d \pmod{n}$$

$$3) \quad ab \equiv cd \pmod{n}$$

"Om man räknar +, - eller \cdot modulo n kan alltid byta ut sina tal mot tal som är kongruenta modulo n med dem".

Vadför? 1) $a \equiv c \pmod{n} \wedge b \equiv d \pmod{n} \iff$

$$\iff n \mid a - c \wedge n \mid b - d \Rightarrow$$
$$\Rightarrow n \mid (a - c) + (b - d) = (a + b) - (c + d) \iff$$
$$\iff a + b \equiv c + d \pmod{n}$$

3) Vill visa att $n \mid ab - cd$.

$$\begin{aligned} ab - cd &= ab - ad + ad - cd = \\ &= a(b - d) + \underbrace{(a - c)d}_{\substack{\text{delbart med } n \\ \text{delbart med } n}} \\ &\quad \underbrace{ }_{\text{delbart med } n} \end{aligned}$$

Så $ab \equiv cd \pmod{n}$. □

Ex Vilken veckodag är 1 april 2021?

Idag: 4 december, fredag (2020)

Dagar kvar mod 7:

$$\begin{aligned} 27 + 31 + 28 + 31 + 1 &\equiv 6 + 3 + 0 + 3 + 1 \equiv \\ &\equiv -1 + 3 + 0 + 3 + 1 \equiv 6 \equiv -1 \pmod{7} \end{aligned}$$

så 1 april 2021 är en torsdag.

Definition

Vi definierar addition, subtraktion och multiplikation på \mathbb{Z}_n genom

Väldefinierade
enligt satser
övan:
T.ex om $[a] = [c]$
och $[b] = [d]$, då
 $a+b = c+d$ (n),
så $[a+b] = [c+d]$

$$\text{Ex: } \begin{matrix} | & \mathbb{Z}_4: & [3] + [2] &= [3+2] &= [5] &= [1] \end{matrix}$$

$$[1] - [3] = [1-3] = [-2] = [2]$$

$$[2] \cdot [2] = [2 \cdot 2] = [4] = \cancel{[0]}$$

$$[6] \cdot [-2] = [-12] = [0]$$

Definitionerna av $+$, $-$, \cdot på \mathbb{Z}_n är väldefinierade:

Om $[a] = [c]$ och $[b] = [d]$. Då måste

$$[a] + [b] = [c] + [d]$$

om definitionen shall vara vettig, dvs

$$[a+b] = [c+d]$$

Men detta stämmer, enligt satser ovan, eftersom
 $a+b \equiv c+d \pmod{n}$.

Subtraktion och multiplikation fungerar på samma sätt.