Algebra och talteori

MMGL31

Föreläsning 2

VT 2010

Samuel Bengmark

Repetition

- Liten inledning till kursen: Pytagoreiska trippler
  - Talteoretisk metod (delbarhet, SGD, primtalsfaktor, kongruens)
  - Geometrisk metod (rationella punkter på en cirkel, skärningspunkter med linje, ekvationssystem)

Vidareutveckling …

Fermats sista sats

Kursmålen

Redogöra för och göra beräkningar

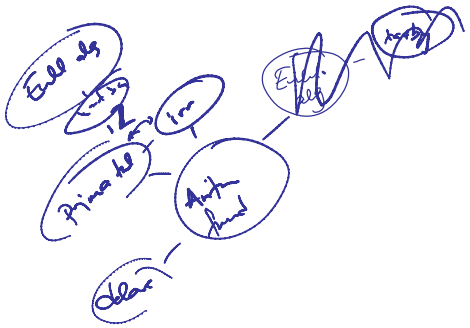
- primtal
- unik faktorisering
- grupp, ring, kropp
- Kongruensräkning,
- Fermats lilla sats,
- Eulers phi-funktion och
- kvadratisk reciprositet
- metoder för ekvationslösning
- primtalstestning,
- perfekta tal,
- summor av två kvadrater,
- några diofantiska ekvationer,
- Gaussiska heltal,
- algebraiska heltal.

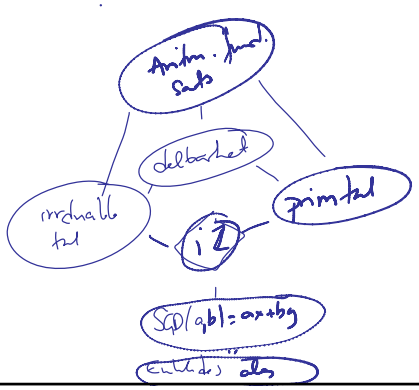
Utforskande lärare matematik, fascination

Redogöra lättfattligt

Idag

- Unik faktorisering
- Irreducibla tal och primtal
- Euklides algoritm, SGD(a,b) och xa+yb
- Grupp, ring och kropp
- Lite om $\mathbb{Z}_n$s struktur





Heltalen, $\mathbb{Z}$

$\mathbb{Z}$ utgör en talmängd med operationer addition och multiplikation.

- Addition ger enkel strukturen. 1 det enda odelbara (irreducibla) talet, (enda byggstenen).
- Multiplikation med komplicerad. Oändligt många odelbara tal.
- Idag skall vi titta lite på den multiplikativa strukturen.

Aritmetikens fundamentalsats

Varje heltal $n > 2$ kan faktoriseras på ett unikt sätt i odelbara tal

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

Ordningen i vilken talen p_i skrivs upp bryr man sig inte om.

Exempel

$12=2^2 \cdot 3$

Detta kan tyckas självklart efter alla år, men det gäller inte i alla talmängder som vi nu skall se.

The $\mathbb{E}$-zone

$\mathbb{E}$={0,2,4,6,…}, de jämna talen

1. Kan dessa tal delas upp i odelbara tal på ett unikt sätt?
2. Vilka är de odelbara talen?

Svar 2.

Svar 1.

Vad är orsaken?

Vilka egenskaperna hos talen i $\mathbb{Z}$ och $\mathbb{E}$ är det som orsakar skillnad i beteende när det gäller faktorisering?

Skillnaden synliggörs med följande definitioner.

Irreducibelt och primt

Definition

Ett heltal p kallas irreducibelt (odelbart) om det för varje annat heltal d gäller att

$$d \mid p \Rightarrow d \in \{\pm 1, \pm p\}$$

Definition

Ett heltal p kallas primt om det för varje andra tal m och n gäller att

$$p \mid n \cdot m \Rightarrow p \mid n \text{ eller } p \mid m$$

Exempel

$\mathbb{Z}$	$\mathbb{E}$
Irreducibla tal	Irreducibla tal
Prima tal	Prima tal

Vi skall strax se att beviset för unik faktorisering bygger på att alla irreducibla tal är primtal.

Innan dess skall vi dock förvissa oss om att det vi tyker oss se om $\mathbb{Z}$ ovan verkligen stämmer

Påstående: Irreducibla tal är prima tal i $\mathbb{Z}$!

- Man kallar de irreducibla talen i $\mathbb{Z}$ för primtal.
- Det är okej eftersom de, förutom att vara irreducibla, även uppfyller definitionen för primtal.
- För att bevisa det behöver vi Euklides algoritm.

Repetition: Euklides algoritm

Exempel
SGD(123, 36)

$$a = bq_1 + r_1$$
$$b = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1}q_n + r_n$$
$$r_{n-1} = r_nq_{n+1} + 0$$

SGD(a,b)

Argument för att Euklides ger SGD

r_n är delare
”gå uppåt”

r_n är största delaren
”gå neråt”

$$a = bq_1 + r_1$$
$$b = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1}q_n + r_n$$
$$r_{n-1} = r_nq_{n+1} + 0$$

Linjära ekvationer och SGD

- SGD(a,b) | xa+yb, oberoende av koefficienterna x och y.
- Man kan få precis SGD med rätt val av x och y. De hittas med Euklides enligt följande exempel

Exempel

Euklides ger

$123 = 36*3+15$
$36 = 15*2+6$
$15 = 6*2+3$
$6 = 3*2+0$
dvs $\mathrm{SGD}(123,36) = 3$

$3 = 15 - 6\cdot 2$
$6 = 36 - 15\cdot 2$
$15 = 123 - 36\cdot 3$

$3 = 15 - 6\cdot 2$
$= 15 - (36 - 15\cdot 2)\cdot 2$
$= -2\cdot 36 + 5\cdot 15$
$= -2\cdot 36 + 5(123 - 36\cdot 3)$
$= 5\cdot 123 - 17\cdot 36$

Åter till: Irreducibla är prima i $\mathbb{Z}$!

Skall alltså visa att om p är ett irreducibelt tal och p|mn så kommer p|m eller p|n.

- Antag att p är irreducielt
- Skall nu visa att p|m·n $\Rightarrow$ p|m eller p|n.
- Om p|m är vi klara.
- Antag därför att p|mn och och att p$\not|$m. Visa att p|n.
- Att p inte delar m och p är irreducibelt finner vi att SGD(p,m)=1, dvs 1=xp+ym.
- Multiplicera med n och får n=xpn+ymn=xpn+ykp=p(xn+yk), dvs p|n.

p|mn $\Leftrightarrow$ mn=kp

Dags för beviset för Aritmetikens fundamentalsats

- Vi skall se att vi måste veta att de irreducibla talen är primtal för att vårt argument för unik faktorisering skall fungera.

Beviset för aritmetikens fundamentalsats

Kan faktorisera i irreducibla

Induktion: Antag alla tal $n \leq N$ kan faktoriseras. Visa att även N+1 kan faktoriseras.

- Om N+1 irreducibelt är det sin egen faktorisering. Klara!
- Annars $N+1=n_1 n_2$.
  - Enligt ind. ant. gäller:

$$n_1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$
$$n_2 = q_1^{\beta_1} \cdots q_l^{\beta_l}$$

  - Detta ger

$$n = N+1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdots q_l^{\beta_l}$$

Unik faktorisering

- Antag att vi har två fakt.

$$p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_l$$

- Detta ger att

$$p_1 \mid n \Leftrightarrow p_1 \mid q_1 q_2 \cdots q_l \Rightarrow p_1 \mid q_1$$

- q_1 irreducibelt ger $p_1=q_1$.
- Stryker p_1 och q_1 får likheten

$$p_2 \cdots p_k = q_2 \cdots q_l$$

- Fortsätter pss tills vi får 1 i ena ledet.

$$p_{k-l} \cdots p_k = 1$$

- Enda chansen att detta stämmer är att k=l.