Algebra och talteori

MMGL31

Föreläsning 5

VT 2010

Samuel Bengmark

Repetition

- $\mathbb{Z}_n$ är ring
- $\mathbb{Z}_n^*$
- $\mathbb{Z}_p$ är kropp omm p primtal
- Fermats lilla sats
  - hann inte med beviset men vi visar en generellare sats idag.

Kursmålen

Redogöra för och göra beräkningar

- primtal och irreducibla tal
- 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,
- Gaussiska heltal,
- algebraiska heltal.

Utforskande lärare

Redogöra lättfattligt

Bevis för FLS

- Betrakta p-1!, dvs $1\cdot 2\cdots(p-2)\cdot(p-1)$
- Tag $a\in\mathbb{Z}_n^*$ och bilda $1a\cdot 2a\cdots(p-2)a\cdot(p-1)a$
- Inse: $1a\cdot 2a\cdots(p-2)a\cdot(p-1)a \equiv_p 1\cdot 2\cdots(p-2)\cdot(p-1)$
  - Varje faktor i VL ger något i HL: Tag ka i VL
    - $ka \in \mathbb{Z}_p$, alltså $ka \equiv_p$ något tal i HL.
  - Olika i VL ger olika i HL: Tag ka och la i VL
    - $ka \equiv_p la \Leftrightarrow k \equiv_p l \Leftrightarrow k=l$
  - Lika många i VL som HL ger exakt samma tal.
- Löser ut a:
  - $a^{p-1}1\cdot 2\cdots(p-2)\cdot(p-1) \equiv_p 1\cdot 2\cdots(p-2)\cdot(p-1)$
  - $1,..,p-1\in\mathbb{Z}_p^*$, dvs inverterbara.
  - Kansellerar alla och får $a^{p-1}\equiv_p 1$

FLS förenklar beräkning

Beräkna 2^{74} mod 5.

$2^{74}=18889465931478580854784$

Idag

- Eulers ϕ-funktion
- Eulers formel
- Att beräkna Eulers ϕ-funktion
- Kinesiska restsatsen
- Någon uppgifter

Eulers ϕ-funktion

Definition

$\phi(m)=|\mathbb{Z}_m^*|$, dvs antalet inverterbara element i $\mathbb{Z}_m$.

Minns att $\mathbb{Z}_m^* = \{a;\ 1\leq a\leq m-1,\ SGD(a,m)=1\}$, alltså är $\phi(m)$= antalet tal mellan 1 och m-1 som är relativt prima med m.

Exempel

$\phi(3)=|\{1,2\}|=2$

$\phi(4)=|\{1,2,3\}|=2$

$\phi(5)=|\{1,2,3,4\}|=4$

$\phi(p)=|\{1,2,\ldots,p-1\}|=p-1$ om p är ett irreducibelt/primtal

$\phi(22)=$ … $=10$

Att räkna ut ϕ effektivt

Sats

1. $\phi(p^k)=p^k-p^{k-1}$ om p är ett primtal
2. $\phi(mn)=\phi(m)\phi(n)$ om $SGD(m,n)=1$

Exempel

- $\phi(22)=\phi(2\cdot 11)=\phi(2)\phi(11)=1\cdot 10=10$.

Kontroll:

$|\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22\}|=$

- $\phi(24)=\phi(2^3)\phi(3)=(2^3-2^2)2=8$.

Kontroll:

$|\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24\}|=$

Eulers formel

Sats

Om $a\in\mathbb{Z}_m^*$ så gäller att $a^{\phi(m)} \equiv_m 1$.

FLS är ett specialfall av detta eftersom $\phi(p)=p-1$.

Exempel

7^{11} i $\mathbb{Z}_{22}$?. Minns att $\phi(22)=10$.

$7^{11} \equiv_{22} 7^{10+1} \equiv_{22} 7^{10}\cdot 7^1 \equiv_{22} 1\cdot 7 \equiv_{22} 7$

Bevis av Eulers formel

- Låt $\mathbb{Z}_n^*=\{ b_1, \ldots, b_{\phi(n)} \}$.
- Tag $a\in\mathbb{Z}_n^*$ och bilda produkterna
  - $b_1\cdot \ldots \cdot b_{\phi(n)}$ och
  - $ab_1\cdot \ldots \cdot ab_{\phi(n)}$
- Visa att $b_1\cdot \ldots \cdot b_{\phi(n)} \equiv_n ab_1\cdot \ldots \cdot ab_{\phi(n)}$ genom att visa att $f_a(x)=ax : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$ är bijektion.
- Kansellera alla b_i och erhåll $a^{\phi(n)}\equiv_n 1$.

$f_a(x)=ax : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$ är bijektion om $a\in \mathbb{Z}_n^*$

- Injektivt:
  - $f(x)\equiv_n f(y) \Leftrightarrow ax \equiv_n ay$.
  - Kansellerar a (a inverterbar)
  - Finner att $x \equiv_n y$.
- Surjektiv
  - För godtyckligt $c\in \mathbb{Z}_n^*$ finns x så att f(x)=c
  - Dvs finns x så att $ax \equiv_n c$.
  - Ser att $x \equiv_n a^{-1}c$ är en lösning.

Kinesiska restsatsen

Om m och n två relativt prima tal så gäller att de två ekvationerna $x \equiv_m b$ och $x \equiv_n c$ precis en lösning x i intervallet $0\leq x \leq mn$.

Uppgift …

Bevis för kinesiska restsatsen

$$\begin{cases} x \equiv_m c \\ x \equiv_n b \end{cases} \Leftrightarrow \begin{cases} x = c + mk \\ x = b + nl \end{cases} \Leftrightarrow \begin{cases} x = c + mk \\ c + mk = b + nl \end{cases} \Leftrightarrow \begin{cases} x = c + mk \\ c - b = nl - mk \end{cases}$$

- Den nedre ekvationen har lösning eftersom
  SGD(m,n)=1|c-b.
  Lösningarna har formen $l=l_p+mr$, $k=k_p+nr$, $r\in\mathbb{Z}$
- Övre ekvationen ger då
  $x=c+m(k_0+nr)=(c+mk_0)+(mn)r$
  Lämpligt val av r ger unikt x i önskat intervall.

$\phi(p^k)= p^k-p^{k-1}$ om p är ett primtal bevis

Skiss
- Observera att $\mathbb{Z}_p{}^*$ består av alla tal mellan 1 och p^k utom alla multipler av p, dvs p,2p,3p,…p^{k-1}p. Multiplerna är alltså p^{k-1} till antalet.
- Alltså finner vi att $|\mathbb{Z}_p{}^*|=p^k-p^{k-1}$

$\phi(mn)=\phi(m)\phi(n)$ om SGD(m,n)=1 bevis

Skiss
- Skapar funktionen $f : \mathbb{Z}_{mn}{}^* \rightarrow \mathbb{Z}_m{}^* \times \mathbb{Z}_n{}^*$ definierad av f(x)=(x mod m, x mod n)
- Visar att f är bijektiv.
  - injektiv: f(x)=f(y) ⇒ m|x-y och n|x-y ⇒ mn|x-y, dvs $x\equiv_{mn} y$.
  - surjektiv: finns x så att $x \equiv_m a$ & $x \equiv_n a$ enl. kinesiska restsatsen
- Ger att $\phi(mn) = \phi(m)\phi(n)$ eftersom $|\mathbb{Z}_m{}^* \times \mathbb{Z}_n{}^*| = |\mathbb{Z}_m{}^*||\mathbb{Z}_n{}^*|$

Beviset i fallet m=3, n=5

- $f : \mathbb{Z}_{15}{}^* \rightarrow \mathbb{Z}_3{}^* \times \mathbb{Z}_5{}^*$, f(x)=(x mod 2, x mod 3)
  - $\mathbb{Z}_{15}{}^*$={1,2,4,7,8,11,13,14}→
  - $\mathbb{Z}_3{}^* \times \mathbb{Z}_5{}^*$ ={1,3}×{1,2,3,4}={(1,1)(1,2)(1,3)(1,4)(2,1)(2,2)(2,3)(2,4)}
- Finner att f(1)=(1,1), f(2)=(2,2), f(4)=(1,4), f(7)=(1,2), f(8)=(2,3), f(11)=(2,1), f(13)=(1,3), f(14)=(2,4).
- Observera bijektion, dvs $|\mathbb{Z}_{15}{}^*| = |\mathbb{Z}_3{}^* \times \mathbb{Z}_5{}^*|$
- Slutsats
  - VL = $|\mathbb{Z}_{15}{}^*| =\phi(15)$ enligt definitionen.
  - HL= $|\mathbb{Z}_3{}^* \times \mathbb{Z}_5{}^*| = |\mathbb{Z}_3{}^*| \cdot |\mathbb{Z}_5{}^*| = \phi(3)\phi(5)$

Några uppgifter