Algebra och talteori

MMGL31

Föreläsning 10

VT 2010

Samuel Bengmark

Delgrupp

Påstående

Låt $a \in \mathbb{Z}_m^*$. Mängden av alla potenser

$\{1,a,a^2,a^3,\ldots,a^{e_m(a)-1}\}$

bildar multiplikativ delgrupp till $\mathbb{Z}_m^*$.

Elementen i denna delgrupp till $\mathbb{Z}_m^*$ betecknas <a>.

Exempel

(<2>, $\cdot$) = ({1,2,4}, $\cdot$) är en grupp modulo 7.

$\cdot$	**1**	**2**	**4**
1	1	2	4
2	2	4	1
4	4	1	2

Bevis Gör själv.

Delgruppsstorlek

OBS! $e_m(a) \leq \phi(m)$ enligt Eulers formel.

Vi kan också ana att $e_m(a)$ alltid delar $\phi(m)$.

Detta skall vi nu visa.

Ordningen delar $\phi(m)$

Sats Givet $a \in \mathbb{Z}_m^*$ då gäller att $e_m(a) | \phi(m)$.

Bevis

- Låt $G=SGD(e_m(a),\phi(m))$ och låt u och v uppfylla $G= ue_m(a)+v\phi(m)$.
- Betrakta $a^G= a^{ue_m(a)+v\phi(m)} = (a^{e_m(a)})^u(a^{\phi(m)})^v \equiv_m 1^u1^v \equiv_m 1$.
- Eftersom $e_m(a)$ är det minsta positiva talet e s.a. $a^e \equiv_m 1$ och $0 \leq G \leq e_m(a)$ måste $G=e_m(a)$, dvs $e_m(a)$ delar $\phi(m)$.

Antal av varje ordning?

Exempel i $\mathbb{Z}_7$

	1	**2**	**3**	**4**	**5**	**6**	**e_7(a)**
1	1	1	1	1	1	1	$e_7(1)=$
2	2	4	1	2	4	1	$e_7(2)=$
3	3	2	6	4	5	1	$e_7(3)=$
4	4	2	1	4	2	1	$e_7(4)=$
5	5	4	6	2	3	1	$e_7(5)=$
6	6	1	6	1	6	1	$e_7(6)=$

$\mathbb{Z}_6$

	1	**2**	**3**	**4**	**5**	**e_6(a)**
1	1	1	1	1	1	$e_6(1)=$
2	2	4	2	4	2	$e_6(2)=$
3	3	3	3	3	3	$e_6(3)=$
4	4	4	4	4	4	$e_6(4)=$
5	5	1	5	1	5	$e_6(5)=$

Antal av varje ordning!

Sats

Om d är en delare till $\phi(m)$ då finns precis $\phi(d)$ stycken element av ordning d i $\mathbb{Z}_m^*$.

För beviset behöver vi undersöka hjälpfunktion F(n) som definieras på näste bild

Funktionen F(n)

Definition

$F(n)=\Sigma_{d|n}\,\phi(d)$

Exempel

Beräkning av F

Sats

1. $F(p^k)=p^k$
2. $F(mn)=F(m)F(n)$ om $SGD(m,n)=1$.

Exempel

$F(p^k)=p^k$

$F(p^k)= \phi(1)+\phi(p)+\ldots\phi(p^{k-1})+\phi(p^k) =$

$= 1+(p-1)+(p^2-p)+\ldots(p^{k-1}-p^{k-2})+(p^k-p^{k-1}) =$

= en teleskoperande summa =

$= p^k$

$F(mn)=F(m)F(n)$ om $SGD(m,n)=1$

Antag att

- n har delare $d_1,\ldots,d_r$ och
- m har delare $e_1,\ldots,e_s$.

Detta ger att mn har delarna

$d_1 e_1,\ldots,d_r e_1$

$d_1 e_2,\ldots,d_r e_2$

……

$d_1 e_s,\ldots,d_r e_s$

Dessutom gäller att

$\phi(d_i e_j)=\phi(d_i)\phi(e_j)\ \forall\ i,j$

eftersom $SGD(n,m)=1$

Får då att

$F(mn)=$

$\phi(d_1 e_1)+\ldots+\phi(d_r e_1)+$

…..

$\phi(d_1 e_s)+\ldots+\phi(d_r e_s)=$

$\phi(d_1)\phi(e_1)+\ldots+\phi(d_r)\phi(e_1)+$

…..

$\phi(d_1)\phi(e_s)+\ldots+\phi(d_r)\phi(e_s)=$

$(\phi(d_1)+\ldots\phi(d_r))(\phi(e_1)+\ldots+\phi(e_s))=$

$F(n)F(m)$.

$F(n)=n$

Sats: $F(n)=n$

Bevis

Antag att $n=p_1^{k_1}\ldots p_r^{k_r}$. Då får vi att

$F(n) = F(p_1^{k_1}\ldots p_r^{k_r}) =$

$= F(p_1^{k_1})\ldots F(p_r^{k_r}) =$

$= p_1^{k_1}\ldots p_r^{k_r} =$

$= n$

Nu åter till beviset av antalet element av varje ordning.

Bevis

- Låt $\psi(d)$={number of a $\in \mathbb{Z}_m^*$ with $e_m(a)=d$}
- Låt $\phi(m)=nk$.
- Får då $x^{\phi(m)}-1=(x^n)^k-1=(x^n-1)((x^n)^{k-1}+\ldots+(x^n)^2+x^n+1)$
- VL har exakt ϕ{m} nollställen enligt Eulers formel (alla i $\mathbb{Z}_m^*$).
- HL båda polynom har högst n respektive n(k-1) rötter var.
- För att stämma med VL är enda möjligheten att de har exakt n respektive n(k-1) rötter var.
- Å andra sidan gäller att $n=\sum_{d|n}\psi(d)$ ty ekvationen x^n-1 löses precis av alla element som har ordning som är delare till n.
- Slutsats $n=\sum_{d|n}\psi(d)$

fortsättning av beviset

- Minns att $n=F(n)=\sum_{d|n}\phi(d)$
- Skall nu se att $\psi=\phi$ genom induktion.
- Ser först att $\psi(1) = 1 = \phi(1)$
- Antag sant för alla n<N, dvs $\psi(n)=\phi(n)$ för n<N.
- Visa nu att $\psi(N)=\phi(N)$ där N har delarna $d_1=1$, d_2…, $d_k=N$
- Vet att
  $\psi(1) + \psi(d_2) +\ldots+ \psi(N) = n = \phi(1) + \phi(d_2) + + \phi(N)$
- Enligt induktionsantagandet gäller likhet för varje term utom möjligtvis för den sista.
- Stryker termer och finner $\psi(N) = \phi(N)$.

Nu går vi över till m=p, primtal

Hittills har jag låtit m vara ett godtyckligt positivt tal, vilket är mer allmänt än i boken,

Nu övergår vi dock till att låta m=p vara ett primtal.

Räkneregler

Sats

- $I(ab) = I(a)+I(b) \bmod p-1$
- $I(a^k) = k\cdot I(a) \bmod p-1$

Bevis

Låt g vara den underliggande primitiva roten.

1. $g^{I(ab)}=ab=g^{I(a)}\,g^{I(b)}=g^{I(a)+I(b)} \Leftrightarrow g^{I(ab)-I(a)-I(b)}\equiv_p 1$. Då måste $I(ab)-I(a)-I(b) \equiv_{p-1} 0$ då g primitiv rot.
2. Upprepad användning av 1.

Lösa ekvationer mha index

Uppgift Lös $3x^5 \equiv_7 4$.

Lösning

Väljer primitiv rot 3 och tar fram indextabell

a	1	2	3	4	5	6
$\mathbf{I_3(a)}$	6	2	1	4	5	3

Ibland saknas lösning

Uppgift Lös $3x^2 \equiv_7 4$.

Lösning

Väljer primitiv rot 3 och tar fram indextabell

a	1	2	3	4	5	6
$\mathbf{I_3(a)}$	6	2	1	4	5	3

$ax^k \equiv_p b$

$ax^k \equiv_p b$ har lösning $\Leftrightarrow$

$k \cdot I(x) \equiv_{p-1} I(b)$ har lösning $\Leftrightarrow$

$SGD(k,p-1) \mid I(b)$

Vi behöver primitiva rötter

Vi har alltså stor nytta av primitiva rötter.

Finns det alltid sådana för för varje $\mathbb{Z}_p$?

Ja, det finns precis $\phi(\phi(p)) = \phi(p-1)$ stycken enligt satsen vi tittade på nyss.

Är a en primitiv rot i $\mathbb{Z}_p$?

Hur vet jag vilka tal som är primitiva rötter? Hur vet jag för vilka p ett givet tal är en primitiv rot?

Det är svåra problem.

- För att kolla om a är en primitiv rot får vi i denna kurs undersöka om $a^k \equiv_m 1$ för något värde $k < p-1$.
- Räcker kolla om $a^d \equiv_p 1$ för någon delare d till p-1.

Artins förmodan

Varje tal $\neq -1$, och som inte är en kvadrat, är primitiv rot modulo p för oändligt många olika värden på p.