Algebra och talteori

MMGL31

Föreläsning 9

VT 2010

Samuel Bengmark

Repetition

- Beräkna a^k mod n för stora k (och n).
  - Succesiv kvadrering
- Lösa $x^k \equiv_n b$
  - Upphöj båda led i k^{-1} mod $\phi(n)$. Funkar bara om SGD(k,ϕ(n))=1 och SGD(b,n)=1!
- RSA-kryptering.
  - Välj p,q och k. Publicera m=pq och k.
  - Beräkna m=pq, k^{-1} mod \phi(m).

Repetition

- FLS och primtalstestning
  - FLS-vittne: a sa $a^{n-1} \not\equiv_n 1$.
- Carmichaeltal
  - Saknar FLS-vittnen.
  - Tex 1105
- Rabin-Millers primtalstest
  - Låt $n-1=q2^k$ och välj potentiellt vittne a.
  - Kolla att $a^q \not\equiv_n \pm 1$ och att alla kvadrater av denna upp till $a^{q2^{k-1}} \not\equiv_n -1$.

Uppgift 19.7

Idag

- Nollställen till $x^2=1$ i kropp och ring.
- Ordning av ett element i $\mathbb{Z}_m$
- Primitiv rot
- Index (diskret logaritm)

x^2-1 i kropp och ring

$x^2-1=0 \Leftrightarrow (x-1)(x+1)=0$

- I kropp måste minst en av faktorerna vara noll eftersom om ab=0 och om a=0 har a invers och vi finner att
  $a^{-1}ab=a^{-1}0 \Rightarrow b=0$.
- I ring kan kvadraten bli ett för andra än ± 1. Tex i uppgift 19.7 såg vi att $781^2 \equiv_{1105} 1$

Ordning

Definition

Ordningen av ett element $a \in \mathbb{Z}_m^*$ är det minsta naturliga tal e för vilket $a^e \equiv_m 1$.

Det betecknas $e_m(a)$.

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	$e_6(5)=$

Primitiv rot

Definition

$a \in \mathbb{Z}_p^*$ kallas en primitiv rot om $e_p(a) = \phi(p)=p-1$, dvs om $<a>=\mathbb{Z}_p^*$.

OBS en primitiv rot a genererar hela $\mathbb{Z}_p^*$.

Vi skall nu se att vi med hjälp av så kallade indextabeller kan använda primitiva rötter för att lösa ekvationer.

Indextabell

Exempel

3 är en primitiv rot i $\mathbb{Z}_7$

I	1	2	3	4	5	6
3^I	3	2	6	4	5	1

Får indextabell

a	1	2	3	4	5	6
$I_3(a)$	6	2	1	4	5	3

Indextabell allmänt

- Ta fram primitiv rot g
- Lista g^I för alla värden $1 \leq I \leq p-1$
- Listan innehåller varje $a \in Z_p^*$ exakt en gång.
- Sortera om.
- I(a) är alltså den exponent I som ger $g^I \equiv_p a$, dvs uppfyller $g^{I(a)} \equiv_p a$.

Index kallas också diskret logaritm

- **Sats**
- $\log_g(ab) = \log_g(a)+\log_g(b) \bmod p-1$
- $\log_g(ak) = k \cdot \log_g(a) \bmod p-1$