Algebra och talteori

MMGL31

Föreläsning 8

VT 2011

Samuel Bengmark

Repetition

- Beräkna a^k mod n för stora k (och n).
- Lösa $x^k \equiv_n b$
- RSA-kryptering

Idag

- FLS och primtalstestning
- Carmichaeltal
- Rabin-Millers primtalstest
- F-funktionen (behövs senare i kursen)

Leta primtal

Eratostenes soll

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
19 20 21 22 23 24 25 26 27 28 29 30 31
32 33 34 35 36 37 38 39 40 41 42 43 44
45 46 47 48 49 50

Att avgöra om ett tal är sammansatt genom att identifiera en faktor är mycket arbete. Finns snabbare sätt!

FLS som primtalstest?

Vi vet att för primtal p gäller om SGD(a,p)=1 gäller $a^{p-1} \equiv_p 1$.

Definition

Ett tal a sådant att SGD(a,m)=1 och $a^{m-1} \not\equiv_m 1$ kallas ett FLS-vittne för m.

OBS

Ett FLS-vittne vittnar om att m är sammansatt.

De flesta tal har gott om FLS-vittnen

Exempel

Carmichaeltal

Det finns dock sammansatta tal som helt saknar FLS-vittnen.

Definition

Sammansatta tal som saknar FLS-vittnen kallas Carmichaeltal.

Exempel

I uppgift 10.3 såg vi att 561 är ett sådant eftersom

$a^{560} \equiv_{561} 1$ för alla $0<a<561$.

Ett annat exempel är 1105.

Korselts kriterium

Sats

Ett udda sammansatt tal n är ett Carmichael-tal omm för var primtalsfaktor p i n gäller att

1. $p^2 \nmid n$
2. $p-1 \mid n-1$

Rabin-Millers följdsats till FLS

Sats

Låt p vara ett udda primtal och $p-1=2^k q$, q udda.

För varje $a \not\equiv_p 0$ gäller då att

$a^q \equiv_p 1$ eller

$a^q \equiv_p -1$ eller $a^{2q} \equiv_p -1$ eller $a^{4q} \equiv_p -1$ eller … eller $a^{2^{k-1}q} \equiv_p -1$

Bevis: Enligt FLS är $a^{p-1} \equiv_p 1$. Titta på sekvensen av succesiva kvadrater: a^q, a^{2q}, a^{4q},…, $a^{2^{k-1}q}$, $a^{2^k q}$. Eftersom det sista talet är 1 finns två möjligheter

1. a^q (och alla andra i sekvensen) är 1
2. något tal i sekvensen är ej 1 men när det kvadreras blir det 1. Då måste talet vara -1.
   (Vi är i en kropp)

Rabin-Miller test

Definition

Låt n vara ett udda tal och $n-1=2^k q$, q udda.

Ett tal a kallas ett Rabin-Miller vittne för n om

$a^q \not\equiv_n \pm 1$ och $a^{2q} \not\equiv_n -1$ och $a^{4q} \not\equiv_n -1$ och … och $a^{2^{k-1}q} \not\equiv_n -1$

Sats

Varje udda sammansatt tal har gott om Rabin-Miller vittnen. Minst 75% av alla mellan 1 och n-1 är Rabin-Miller vittnen.

Har man inte hittat ett vittne efter att ha provat drygt 25% av talen vet man att det är primt.

Uppgift 19.7

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 $n=p_1^{k1}\ldots p_r^{kr}$. Då får vi att

$F(n) = F(p_1^{k1}\ldots p_r^{kr}) =$

$= F(p_1^{k1})\ldots F(p_r^{kr}) =$

$= p_1^{k1}\ldots p_r^{kr} =$

$= n$