Algebra och talteori

MMGL31

Föreläsning 8

VT 2010

Samuel Bengmark

Repetition

- Primtal på formen a^n-1
- Mersenneprimtal
- Perfekta tal
- Samband mellan jämna perfekta tal och Mersenneprimtal

Idag

Hur beräkna $452^{929} \equiv_{1147}$?

- Multipliciera 928 gånger och reducera mod 1147 varje gång. Går men är jobbigt.

- Smartare med succesiv kvadrering. Visar med exempel

Beräkna $452^{929} \equiv_{1147}$?

1. Skapar listan

i	2^i	$452^{2^i} \bmod 1147$
0	1	452
1	2	138
2	4	692
3	8	565
4	16	359
5	32	417
6	64	692
7	128	565
8	256	359
9	512	417

2. Skriver 929 som summa av 2-potenser

$$929 = 512 + 256 + 128 + 32 + 1$$

3. Får multiplikation av 5 faktorer

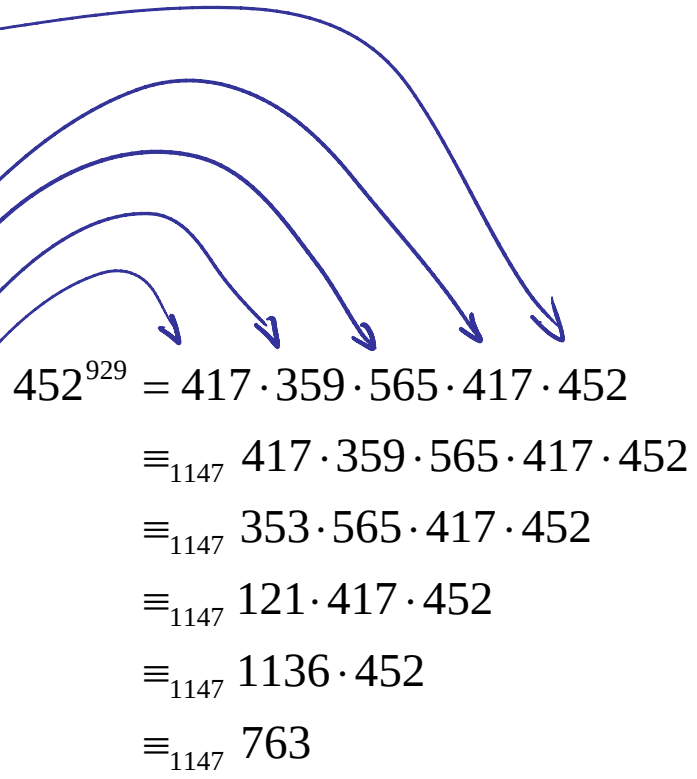
$$\begin{aligned} 452^{929} &= 452^{512} 452^{256} 452^{128} 452^{32} 452^{1} \\ &\equiv_{1147} 417 \cdot 359 \cdot 565 \cdot 417 \cdot 452 \\ &\equiv_{1147} 417 \cdot 359 \cdot 565 \cdot 417 \cdot 452 \\ &\equiv_{1147} 593 \cdot 565 \cdot 417 \cdot 452 \\ &\equiv_{1147} 121 \cdot 417 \cdot 452 \\ &\equiv_{1147} 1136 \cdot 452 \\ &\equiv_{1147} 763 \end{aligned}$$

4. Slutsats $452^{929} \equiv_{1147} 763$

Tänk gärna binärt!

$929 = 512 + 256 + 128 + 32 + 1$, dvs 929 på decimalform $= 1110100001$ på binär form

i	2^i	$452^{2^i} \bmod 1147$	929 på binär form
0	1	452	1
1	2	138	0
2	4	692	0
3	8	565	0
4	16	359	0
5	32	417	1
6	64	692	0
7	128	565	1
8	256	359	1
9	512	417	1



$$
\begin{aligned}
452^{929} &= 417 \cdot 359 \cdot 565 \cdot 417 \cdot 452 \\
&\equiv_{1147} 417 \cdot 359 \cdot 565 \cdot 417 \cdot 452 \\
&\equiv_{1147} 353 \cdot 565 \cdot 417 \cdot 452 \\
&\equiv_{1147} 121 \cdot 417 \cdot 452 \\
&\equiv_{1147} 1136 \cdot 452 \\
&\equiv_{1147} 763
\end{aligned}
$$

Succesiv kvadrering av a^k mod n

1. Reducera först exponenten till ett värde $r < \phi(n)$ med hjälp av Euler formel, dvs så att $a^r \equiv_n a^k$.
2. Beräkna alla värden a, a^2, a^4, … , a^{2^j}, en kvadrering för varje nytt värde tills $2^j<r$ och reducera i varje steg till ett värde mellan 0 och n.
3. Skriv r på binär form, dvs

$$r = c_j 2^j + c_{j-1} 2^{j-1} + ... + c_2 2^2 + c_1 2 + c_0, \quad c_i \in \{0,1\}$$

4. Får

$$a^k \equiv_n a^r \equiv_n a^{c_j 2^j + c_{j-1} 2^{j-1} + ... + c_2 2^2 + c_1 2 + c_0} \equiv_n (a^{2^j})^{c_j} (a^{2^{j-1}})^{c_{j-1}} ... (a^{2^2})^{c_2} (a^2)^{c_1} a^{c_0}$$

   Vilket är produkten av högst j tal i $\mathbb{Z}_n$.

Lösa ekvation $x^k \equiv_m b$

Använder Eulers formel och invers till k modulo $\phi(m)$.

1. Beräkna $\phi(m)$ och finn invers k^{-1} till k modulo $\phi(m)$ (den finns omm SGD(k,$\phi(m)$)=1)

2. Då är $b^{k^{-1}}$ en lösning eftersom

$$x^k=(b^{k^{-1}})^k=b^{k^{-1}k}=b^{1+r\phi(m)}\equiv_m b$$

Det siste steget gäller enligt Eulers formel om SGD(b,m)=1

Uppgift 17.1

Uppgift : Lös $x^{329} \equiv_{1147} 452$

Lösning:

1. Beräknar $\phi(1147)=\phi(31\cdot37)=\phi(31)\cdot\phi(37)=30\cdot36=1080$
2. Beräkna invers till 329 mod 1080, dvs

   $329\cdot x \equiv_{1080} 1 \Leftrightarrow x \equiv_{1080} 929$
3. Beräknar $452^{929} \equiv_{1147} 763$, mha succesiv kvadrering.
4. Då SGD(452,1147)=1 har vi inte fått en falsk lösning, men kontrollera gärna genom succ. kvad. att

   $763^{329} \equiv_{1147} 452$.
5. Slutsats $x \equiv_{1147} 763$ är en lösning

Förutsättningarna viktiga!

- Patologiskt exempel $x^3 \equiv_8 2$

RSA-krypto

Utgår ifrån att även för stora n är

- x^k är lätta att beräkna med hjälp av bara x, k och n, genom successiv kvadrering

Men

- $x^k \equiv_n a$ är mycket svår att beräkna utan att ha $\phi(n)$, vilken är svårt att beräkna utan att ha primtalsfaktorisering av n.

Exempel: ”då ba”

- Välj sätt att koda bokstäver som tal

a	b	c	d	e	f	g	h	i	j	k	l	m	n	…
11	12	13	14	15	16	17	18	19	20	21	22	23	24	…

- Välj två primtal p och q, i detta exempel p=11, q=13
- Beräkna m=pq=143
- Beräkna $\phi(m)=\phi(143)=\phi(11)\phi(13)=10\cdot 12=120$.
- Välj $k\in \mathbb{Z}\ \phi_{(m)}^{*}$, k=7 och beräknar $k^{-1} \equiv_{120} 103$.
- Publicerar m=143 samt k=7
- Håller $\phi(143)=120$ och $k^{-1} \equiv_{8} 103$ hemliga.

Kunden

- Text kodas till en sekvens siffror.

  då ab $\rightarrow$ 1438391112
- Sekvens delas upp i bitar så att ingen bit representerar ett tal $\geq$ 143, dvs s=(14,38,39,111,2)
- Varje bit b_i öpphöjs i 7 och får
- $(a_1,a_2, \ldots, a_n)=(14^7,38^7, 39^7,111^7,2^7) \equiv_{143}$ (53,25,52,45,128).
- Sekvensen (53,25,52,45,128) skickas till banken.

Banken

- Banken får

  $(a_1,a_2, \ldots, a_n) \equiv_{143} (53,25,52,45,128)$.

- Banken beräknar

  $(53^{103},25^{103}, 52^{103},45^{103},128^{103},25^{103}) \equiv_{143}$
  $(14,38,39,111,2)$

- Wow!!

Öppen nyckel

- Alla vet krypteringsnyckeln
  (m och k).

- Dekrypteringsnycklarna känner bara mottagaren till
  (k^{-1},$\phi(m)$).

- För att beräkna dekryperingsnycklarna utifrån krypteringsnycklarna måste man för stora m kunna faktorisera m i sina primtalsfaktorer.

- Om p och q har 200 siffror var tar det ca 75 år för världens idag snabbaste datorsystem att hitta faktorerna.

Krypto-ägaren, tex banken

- Välj sätt att koda bokstäver som tal, tex

a	b	c	d	e	f	g	h	i	j	k	l	m	n	…
11	12	13	14	15	16	17	18	19	20	21	22	23	24	…

Även blanksteg kan få sin egen siffra, låt säga 39.

- Välj två stora primtal p och q (minst 200 siffror var)
- Beräkna m=pq, samt $\phi(m)=(p-1)(q-1)$.
- Välj k så att SGD(k,$\phi(m)$)=1, och kan då även beräkna inversen k^{-1} till k modulo $\phi(m)$.
- Publicerar m, k (och valt sätt att koda bokstäver som siffror) (men publicerar absolut inte $\phi(m)$ och k^{-1}).

Kunden

- Text kodas till en sekvens siffror.
- Sekvens delas upp i bitar så att ingen bit representerar ett tal $\leq$ m, dvs $(b_1,b_2,\ldots,b_N)$ där $b_i \leq m$.
- Varje bit b_i öpphöjs i k mod m och
  $(a_1,a_2, \ldots, a_n)=(b_1^k,b_2^k, \ldots, b_n^k)$
  skickas till banken.

Banken

- Banken vill ta reda på b_i och löser därför ekvationen $x^k \equiv_m a_i$ genom beräkna $a_i^{k^{-1}}$
- Banken får då att

$$x \equiv_m a_i^{k^{-1}} \equiv_m b_i^{kk^{-1}} \equiv_m b_i^{1+r\phi(m)} \equiv_m b_i$$

FLS som primtalstest?

Vi vet att för primtal p gäller att för $\forall a \not\equiv_p 0$ gäller $a^{p-1} \equiv_p 1$.

Definition

Att tal $a \not\equiv_m 0$ sådant att $a^{m-1} \not\equiv_m 1$ 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

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

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.