Videregående Algoritmik, DIKU 2005/06
Mandag 9. januar
David Pisinger

Talteoretiske algoritmer, RSA kryptosystemet, Primtalstest

- Motivation
- Definitioner
- Euclids algoritme
- Udvidet Euclid
- RSA kryptosystemet
- Randomiserede algoritmer
- Rabin-Miller primtalstest
- Svært at faktorisere

Motivation

Internettet:

- Login til DIKU (med password)
- Handel med dankort
- Fortrolig besked
- Digital signatur

$\boxed{\text{Behov for kryptografi}}$

Sikkerhed i RSA beror på

- Det er svært at faktorisere et heltal
- Det er relativt let at finde primtal

Har ikke bevist: svært at faktorisere
Derfor: 1 mio $ til den der kan bryde systemet

Indtil for nylig: talteori smukt men ubrugeligt
Nu: vigtigt redskab i krytologi

Definitioner

d går op i a	$d \mid a$	$5 \mid 15$
d går ikke op i a	$d \nmid a$	$7 \nmid 15$
primtal		$2,3,5,7,11,13$
sammensat tal		$4,15,21,22$

Definition af modulo

Divisons theorem 31.1

$\boxed{\text{For ethvert } a \in \mathbb{Z} \text{ and } n \in \mathbb{Z}_+ \text{ er der unikke heltal } q, r \text{ med } 0 \leq r < n \text{ hvor } a = qn + r}$

$q = \lfloor \frac{a}{n} \rfloor$ kaldes kvotient $\qquad$ r kaldes rest (modulo n)
Skrivemåde $r = a \bmod n$

Ækvivalensklasse modulo n

Heltal med samme rest, opfattes som ækvivalensklasse

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

F.eks.

$$\mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\}$$

hvor

0 repræsenterer $\ldots, -14, -7, 0, 7, 14, \ldots$
1 repræsenterer $\ldots, -13, -6, 1, 8, 15, \ldots$
2 repræsenterer $\ldots, -12, -5, 2, 9, 16, \ldots$
3 repræsenterer $\ldots, -11, -4, 3, 10, 17, \ldots$

Største fælles divisior

fælles divisor $d = \text{cd}(a,b) \Leftrightarrow d \mid a$ og $d \mid b$.
største fælles divisor $d = \gcd(a,b)$

eksempel: $\gcd(21,35) = 7$

$$\begin{aligned}
\gcd(a,b) &= \gcd(b,a) \\
\gcd(a,b) &= \gcd(-a,b) \\
\gcd(a,b) &= \gcd(|a|,|b|) \\
\gcd(a,0) &= |a| \qquad \text{(definition)} \\
\gcd(a,ka) &= |a|, k \in \mathbb{Z}
\end{aligned}$$

Relativt primiske

a og b er relativt primiske hvis $\gcd(a,b) = 1$

eksempel: 21 og 25 er relativt primiske

Entydig primtalsfaktorisering

Ethvert positivt heltal a kan skrives entydigt på formen

$$a = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_r}^{e_r}$$

hvor $p_1, p_2, \ldots, p_r$ er primtal, og
$e_1, e_2, \ldots, e_r$ er de tilhørende potenser.

eksempel: $6000 = 2^4 \cdot 3 \cdot 5^3$

Regneregler

$$d \mid a \text{ og } d \mid b \;\Rightarrow\; d \mid (ax+by) \text{ for alle } x,y \in \mathbb{Z} \quad (31.4)$$

$$a \mid b \text{ og } b \mid a \;\Rightarrow\; a = \pm b \quad (31.5)$$

$$d \mid a \text{ og } d \mid b \;\Rightarrow\; d \mid \gcd(a,b) \quad \text{(korollar 31.3)}$$

eksempel:

$$7 \mid 14 \Rightarrow 7 \mid x \cdot 14$$
$$7 \mid 35 \Rightarrow 7 \mid y \cdot 35$$

eksempel:

$$a = 2^2 \cdot 3 \cdot 7 = 84$$
$$b = 2 \cdot 3 \cdot 5 = 30$$

Euclids algoritme

Theorem 31.9

$$x = \boxed{\gcd(a,b) = \gcd(b, a \bmod b)} = y$$

Når $x,y > 0$ har vi fra (31.5) at

$$x \mid y \text{ og } y \mid x \Rightarrow x = y$$

$\boxed{\textbf{viser } x \mid y}$

Lad $x = \gcd(a,b)$ så $x \mid a$ og $x \mid b$

$$(a \bmod b) = a - qb \text{ hvor } q = \lfloor \frac{a}{b} \rfloor$$

Bemærk at

$x \mid (a - qb)$ (da linearkombination af a,b)

Dermed $x \mid (a \bmod b)$. Fra korollar 31.3

$$x \mid b \text{ og } x \mid (a \bmod b) \Rightarrow x \mid \gcd(b, a \bmod b)$$

$\boxed{\textbf{viser } y \mid x}$

Lad $y = \gcd(b, a \bmod b)$ så $y \mid b$ og $y \mid (a \bmod b)$

$$a = qb + (a \bmod b) \text{ hvor } q = \lfloor \frac{a}{b} \rfloor$$

Bemærk at

$y \mid qb + (a \bmod b)$ (da linearkomb. af $b, (a \bmod b)$)

Dermed $y \mid a$. Fra korollar 31.3

$$y \mid a \text{ og } y \mid b \Rightarrow y \mid \gcd(a,b)$$

Euclids algoritme, (Elements of Euclid år 300 f.kr.)

Fra theorem 31.9 har vi rekursion

$$\gcd(a,b) := \gcd(b, a \bmod b)$$

Stopbetingelse $\gcd(a,0) = |a|$.

Rekursion må terminere da andet argument $(a \bmod b) < b$ er aftagende

```
EUCLID(a, b)
if b = 0
    then return a
    else return EUCLID(b, a mod b)
```

Eksempel

$$\begin{aligned} \text{EUCLID}(30,21) &= \text{EUCLID}(21,9) \\ &= \text{EUCLID}(9,3) \\ &= \text{EUCLID}(3,0) \\ &= 3 \end{aligned}$$

Euclids algoritme, tidskompleksitet

Fibonacci tal: $F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$
$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89 \ldots$

Øvre grænse

> Hvis $a > b \geq 1$ og EUCLID(a,b) udfører $k \geq 1$ rekursive kald, så er $a \geq F_{k+2}$ og $b \geq F_{k+1}$.

Hvis $a > b$ så i rekursive kald er $(b > a \bmod b)$

Induktion i k

$\boxed{k=1}$ $b \geq 1 = F_2$, $a > b$ så $a \geq 2 = F_3$

$\boxed{k>1}$ Lemma holder for $k-1$.

- Da $b > 0$ vil EUCLID(a,b) kalde EUCLID$(b, a \bmod b)$ som laver $k-1$ rekursive kald. Pga. induktionsantagelsen er $b \geq F_{k+1}$, og $(a \bmod b) \geq F_k$.
- Da $a > b > 0$ vil $\lfloor a/b \rfloor \geq 1$ så

  $$b + (a \bmod b) = b + (a - \lfloor a/b \rfloor b) \leq a$$

  Dermed

  $$a \geq b + (a \bmod b) \geq F_{k+1} + F_k = F_{k+2}$$

> Theorem 31.11: Antag $a > b \geq 1$ og $b < F_{k+1}$. Da vil EUCLID(a,b) udføre højst k rekursive kald

Nedre grænse

EUCLID laver præcist $k-1$ kald med input F_{k+1}, F_k.

Induktion i k

$\boxed{k=2}$ EUCLID(F_3, F_2) laver 1 kald

$\boxed{k>2}$ EUCLID$(F_{k+1}, F_k) =$ EUCLID(F_k, F_{k-1})

Fibonacci tal: $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89 \ldots$

Store-O

- $F_k \approx \phi^k/\sqrt{5}$
  hvor $\phi = (1+\sqrt{5})/2$ (golden ratio)
- $F_k = \Theta(2^k)$ så med input $b = F_k$ fås k iterationer
- EUCLID(a,b) kører i $O(\log b)$

Udvidet Euclids algoritme

Find $x, y \in \mathbb{Z}$ så

$$d = \gcd(a,b) = ax + by$$

(findes altid da giver konstruktiv algoritme)

```
(d, x, y) = EXTENDED-EUCLID(a, b)
if b = 0
    then return (a, 1, 0)
(d', x', y') ← EXTENDED-EUCLID(b, a mod b)
(d, x, y) ← (d', y', x' − ⌊a/b⌋y')
return (d, x, y)
```

Eksempel

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	–	3	1	0

Så vi har

$$\gcd(99, 78) = 3 = 99 \cdot (-11) + 78 \cdot 14$$

Udvidet Euclids algoritme

Returnerer $d = \gcd(a,b) = ax + by$ i hver iteration

- $\boxed{\text{hvis } b = 0}$
  returnerer $(d, x, y) = (a, 1, 0)$ som overholder
  $$d = a \cdot 1 + b \cdot 0 = ax + by$$
- $\boxed{\text{hvis } b \neq 0}$
  Har (d', x', y') hvor
  $$\begin{aligned} d' &= \gcd(b, a \bmod b) \\ d' &= bx' + (a \bmod b)y' \quad \text{(induktionsantagelse)} \end{aligned}$$
  Så vi har
  $$d = \gcd(a,b) = d' = \gcd(b, a \bmod b)$$
  For at finde x og y så $d = ax + by$
  $$\begin{aligned} d &= bx' + (a - \lfloor a/b \rfloor b)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor y') \end{aligned}$$
  Så hvis vi vælger $x = y'$ og $y = x' - \lfloor a/b \rfloor y'$ har vi
  $$d = ax + by$$

Køretid

Som EUCLID

Modulo regning

Modulo regning er som almindelig regning blot erstattes resultatet x med x modulo n.

Definition

$$a \oplus_n b := a + b \pmod{n}$$
$$a \odot_n b := a \cdot b \pmod{n}$$

Eksempel

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\odot_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Bemærk: ikke alle tal forekommer i sidste tabel

Additiv og multiplikativ gruppe

[*gruppe*: lukket, associativ, neutralt-element, alle har invers]

- $\mathbb{Z}_n$ er additiv gruppe modulo n
  $\{0,1,2,\ldots,n-1\}$
- $\mathbb{Z}_n^*$ er multiplikative gruppe modulo n
  tal der er relativt primiske med n, dvs:
  $\{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$

Eksempel: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$

Størrelse af multiplikativ gruppe $\mathbb{Z}_n^*$

Eulers phi-funktion

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

hvor p løber over alle primtal der går op i n (incl. n, hvis n er primtal).

Eksempel: $\mathbb{Z}_{15}^*$

$$\phi(15) = 15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$$

Multiplikativt inverse

Multiplikativt inverse (en slags “division” i gruppen $\mathbb{Z}_n^*$)

$$a \cdot a^{-1} = 1$$

Da $\mathbb{Z}_n^*$ er en gruppe findes inverse element altid

Eksempel

$\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$

a	1	2	4	7	8	11	13	14
a^{-1}	1	8	4	13	2	11	7	14

$\odot_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Løsning af ligninger modulo n

> For givne $a, n > 0$ og $b \geq 0$ find $x \in \mathbb{N}$ så
> $$ax \equiv b \pmod{n}$$

Da vi regner modulo kan der være 0 eller flere løsninger, f.eks.

$$\begin{array}{lll} 2x \equiv 3 \pmod{4} & \text{har løsning} & x \in \{\} \\ 2x \equiv 2 \pmod{4} & \text{har løsning} & x \in \{1,3,5,\ldots\} \end{array}$$

Nødvendig og tilstrækkelig betingelse for at findes løsning

$$b \in \langle a \rangle = \{ax \bmod n : x > 0\}$$

Theorem 31.23
Antag at $d = \gcd(a,n)$ og antag $d = ax' + ny'$ som bestemt af EXTENDED-EUCLID. Hvis $d \mid b$ så har

$$ax \equiv b \pmod{n}$$

en mulig løsning givet ved

$$x = x'(b/d) \bmod n$$

Bevis

$$\begin{aligned} ax &\equiv ax'(b/d) \pmod{n} \\ &\equiv d(b/d) \pmod{n} \\ &\equiv b \pmod{n} \end{aligned}$$

Korollar 31.26

Givet $n \in \mathbb{N}$, $n \geq 2$, hvis $\gcd(a,n) = 1$ for et $a \in \mathbb{Z}_n$ så har

$$ax \equiv 1 \pmod{n}$$

een unik løsning modulo n.
Denne kaldes den *multiplikativt inverse* a^{-1}.

$$\begin{aligned} &d = \gcd(a,n) = ax + ny \Leftrightarrow \\ &1 = ax + ny \Leftrightarrow \\ &1 \equiv ax \pmod{n} \end{aligned}$$

Husk:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$$

dvs alle elementer i $\mathbb{Z}_n^*$ har unik multiplikativt invers

Opsummering EXTENDED-EUCLID

- $\gcd(a,b)$
- $\gcd(a,b) = ax + by$
- $ax \equiv b \pmod{n}$
- a^{-1}

Kinesisk restklassesætning (Sun-Tsŭ år 100)

Find alle heltal x hvor

- $x \bmod 3 = 2$
- $x \bmod 5 = 3$
- $x \bmod 7 = 2$

Et sådant heltal er $x = 23$
Alle heltal på formen $x = 23 + 105k$

Bemærk: $105 = 3 \cdot 5 \cdot 7$

Theorem 31.27 (kinesisk restklassesætning)

Lad $n = n_1 \cdot n_2 \cdots n_k$ hvor n_i'erne er parvist primiske.
Hvis

$$a \leftrightarrow (a_1, \ldots, a_k), \qquad a \in \mathbb{Z}_n, a_i \in \mathbb{Z}_{n_i}$$
$$b \leftrightarrow (b_1, \ldots, b_k), \qquad b \in \mathbb{Z}_n, b_i \in \mathbb{Z}_{n_i}$$

hvor $a_i = a \bmod n_i$, så gælder regnereglerne

$$(a+b) \bmod n \leftrightarrow ((a_1+b_1) \bmod n_1, \ldots, (a_k+b_k) \bmod n_k)$$
$$(a-b) \bmod n \leftrightarrow ((a_1-b_1) \bmod n_1, \ldots, (a_k-b_k) \bmod n_k)$$
$$(ab) \bmod n \leftrightarrow ((a_1 b_1) \bmod n_1, \ldots, (a_k b_k) \bmod n_k)$$

Eksempel (figur 31.3)

Transformation $a \rightarrow (a_1, \ldots, a_k)$ **nem**   transformation $(a_1, \ldots, a_k) \rightarrow a$ **formel**

$n = n_1 n_2$
$65 = 5 \cdot 13$ ($n_1 = 5$ og $n_2 = 13$).

$$m_i = \frac{n}{n_i} = \frac{n_1 n_2}{n_i}$$
$$c_i = m_i (m_i^{-1} \bmod n_i)$$

$m_1 = \frac{n_1 n_2}{n_1} = n_2 = 13$
$m_2 = \frac{n_1 n_2}{n_2} = n_1 = 5$
$c_1 = 13(13^{-1} \bmod 5) = 26$
$c_2 = 5(5^{-1} \bmod 13) = 40.$

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	40	15	55	30	5	34	20	60	35	10	50	25
1	26	1	41	16	56	31	6	46	21	61	36	11	51
2	52	27	2	42	17	57	32	7	47	22	62	37	12
3	13	53	28	3	43	18	58	33	8	48	23	63	38
4	39	14	54	29	4	44	19	59	34	9	49	24	65

Ækvivalens

$$a \equiv (a_1 c_1 + a_2 c_2 + \cdots + a_k c_k) \pmod{n}$$

Eksempel

$$a \equiv (a_1 \cdot 26 + a_2 \cdot 40) \pmod{65}$$

Korollar 31.29 (bruges i korrekthed af RSA)

Hvis $n_1, n_2, \ldots, n_k$ er parvist primiske, og $n = n_1 n_2 \cdots n_k$ så gælder for alle heltal x og a at

$$x \equiv a \pmod{n_i} \text{ for } i = 1, 2, \ldots, k \qquad \Leftrightarrow$$
$$x \equiv a \pmod{n}$$

Eksempel $n_1 = 5, n_2 = 13$

$n = n_1 n_2 \qquad 65 = 5 \cdot 13 \qquad$ 5 og 13 primiske

$$\left.\begin{array}{l} 69 \equiv 4 \pmod{5} \\ 69 \equiv 4 \pmod{13} \end{array}\right\} \Leftrightarrow \quad 69 \equiv 4 \pmod{65}$$

Potens af element

Givet $n \in \mathbb{N}$ og $a \in \mathbb{Z}_n$, find

$$a^0, a^1, a^2, a^3, a^4, \ldots \text{ modulo } n$$

i	0	1	2	3	4	5	6	7	8	9	10	11	…
$3^i \bmod 7$	1	3	2	6	4	5	1	3	2	6	4	5	…

i	0	1	2	3	4	5	6	7	8	9	10	11	…
$2^i \bmod 7$	1	2	4	1	2	4	1	2	4	1	2	4	…

Theorem 31.30 (**Eulers theorem**) For ethvert heltal $n > 1$ gælder $a^{\phi(n)} \equiv 1 \pmod{n}$ for alle $a \in \mathbb{Z}_n^*$

Theorem 31.31 (**Fermats [lille] theorem**) Hvis p er et primtal så er $a^{p-1} \equiv 1 \pmod{p}$ for alle $a \in \mathbb{Z}_p^*$

Bemærk at $0 \notin \mathbb{Z}_p^*$ så $0^{p-1} \not\equiv 1 \pmod{p}$

Eksempel: $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\phi(7) = 7 \cdot (1 - \frac{1}{7}) = 6$
$a^{\phi(7)} \equiv 1 \pmod{7} \qquad$ for alle $a \in \mathbb{Z}_7^*$
$a^{7-1} \equiv 1 \pmod{7} \qquad$ for alle $a \in \mathbb{Z}_7^*$

Potensopløftning ved gentagen kvadrering

Udregn:

$$a^b \bmod n \qquad a, b \in \mathbb{N}_0, n \in \mathbb{N}$$

Udnytter at

$$a^{2c} \bmod n = (a^c)^2 \bmod n$$
$$a^{2c+1} \bmod n = a(a^c)^2 \bmod n$$

Algoritme

Lad $b = \langle b_k, b_{k-1}, \ldots, b_1, b_0 \rangle$ være binære kodning af b
Invariant: $c = \langle b_k, \ldots, b_i \rangle$, $d = a^c \bmod n$ i skridt i

```
MODULAR-EXPONENTIATION(a, b, n)
c ← 0
d ← 1
for i ← k downto 0 do
    c ← 2c
    d ← (d · d) mod n
    if b_i = 1 then
        c ← c + 1
        d ← (d · a) mod n
return d
```

Køretid
Antag: $a, b, n \leq 2^\beta$
Iterationer: $O(\beta)$. Multiplikation: $O(\beta^2)$ bitoperationer
Totalt: $O(\beta^3)$

Potensopløftning, eksempel

Udregn $11^{19} \bmod 21$
$a = 11$
$b = 19 = \langle 10011 \rangle$
$n = 21$

i	c	d
4	1	11
3	2	16
2	4	4
1	9	8
0	19	11