

UNIVERSITETET I TROMSØ
DET MATEMATISK
NATURVITENSKAPELIGE FAKULTET

Utsatt eksamen i: MAT-1300, Diskret matematikk 2
Eksamensdag: 20. sept., 2004
Tid for eksamen: 09.00-13.00
Tillatte hjelpemiddel: Godkjent kalkulator og 2 ark notater

Oppgavesettet er på 3 sider.

Kontaktperson:

Oppgave 1 Bruk kinesisk restteorem til å finne det minste positive tall x slik at

$$x \equiv 5 \pmod{13}$$

$$x \equiv 3 \pmod{23}$$

Oppgave 2 La $n = 667 = 23 \cdot 29$. Bruk Eulers teorem til å regne ut $2^{184804} \pmod{n}$.

Oppgave 3 RSA offentlig nøkkel kryptografi kan beskrives slik. En klartekst P (som er et tall) krypteres til $C \equiv P^e \pmod{n}$, hvor n er et produkt av 2 store primtall. Både e og n er offentlige. Et tall P kalles et fikspunkt hvis $P^e \equiv P \pmod{n}$.

La $n = 667$ og vi røper med en gang at faktoriseringen er $n = 23 \cdot 29$. Vi lar også $e = 237$.

a) En klartekst P er kryptert med n og e som ovenfor og den krypterte teksten er $C = 285$. Finn P . Forklar hvordan du går frem.

b) Finn alle R slik at $R^{237} \equiv R \pmod{23}$ og alle S slik at $S^{237} \equiv S \pmod{29}$.

c) Finn et P slik at $P^{237} \equiv P \pmod{n}$. Denne P skal ikke være kongruent med $0 \pmod{n}$ og heller ikke $\pm 1 \pmod{n}$.

Oppgave 4 Et tall $a \pmod{n}$, innbyrdes prim med n , kalles en kvadratisk rest modulo n hvis det finnes en x slik at $a \equiv x^2 \pmod{n}$. Hvis $a \equiv x^2 \pmod{n}$ ikke er løslar kalles a for en ikke-rest.

a) La r være en primitiv rot modulo 23 og forklar hvorfor alle like potenser $r^{2t} \pmod{23}$, $t = 0, 1, 2, 3, \dots, 10$ er forskjellige kvadratrester modulo 23.

b) Avgjør om 23 er en kvadratrete modulo 173 eller ikke. Forklar fremgangsmåten.

c) Finn en primitiv rot r modulo 23 og en primitiv rot modulo 23^2 . Forklar fremgangsmåten.

Oppgave 5 Det følgende beskriver en minimal kunnskapsprotokoll hvor en person A vil overbevise B om at hun vet faktoriseringen ($n = p \cdot q$) av et stort sammensatt heltall n . Her er p og q begge primtall kongruent med 3 mod 4. Protokollen går i tre trinn.

i) B , som kjenner n , men ikke p og q velger et heltall x tilfeldig, beregner $y = x^4 \bmod n$ og sender y til A .

ii) Når A mottar y beregner hun kvadratroten av y . Det er fire slike, men hun velger den som er kongruent med x^2 modulo n , og sender den til B .

iii) B sjekker det han mottar mot $x^2 \bmod n$, som han allerede har regnet ut.

a) I ii), forklar hvordan A går frem for å regne ut en kvadratroten av y modulo n ?

b) Hvis A gjør feil i ii) og beregner feil kvadratroten, forklar hvordan B (og alle andre som har snappet opp meldingene) kan beregne p og q og dermed vite faktoriseringen av n .

c) Forklar hvordan en slik minimal kunnskapsprotokoll kan brukes til å erstatte passord for tilgang til datamaskiner.

Oppgave 6 Output for en boolsk funksjon i tre variabler er gitt i tabell 1.

a) Finn sum av produkt utviklingen til en boolsk funksjon $F(x, y, z)$ som har dette output.

b) Bruk Karnaugh maps til å finne et enklere uttrykk for funksjonen $F(x, y, z)$ i a).

c) Bruk regnereglene for boolsk algebra til å vise at

$$xyz + \overline{x}yz + \overline{xy}z + \overline{xy}\overline{z} + \overline{x}\overline{y}\overline{z} + \overline{x}\overline{y}z = z + \overline{x}\overline{z}.$$

(Regnereglene står i tabell 3 under.)

Oppgave 7 En ikke-deterministisk tilstandsmaskin $M = (S, I, f, s_0, F)$ er gitt i tabell 2. s_0 og s_3 er slutttilstander.

a) Tegn tilstandsdiagram (rettet graf).

b) Finn språket som gjenkjennes av maskinen M .

c) Finn en deterministisk maskin som gjenkjenner det samme språket. Tegn tilstandsdiagram.

Tabell 2

Tilstand	f Input	
	0	1
s_0	s_3	s_1
s_1		s_2, s_4
s_2		s_3
s_3	s_4	
s_4		s_3

Tabell 1			
x	y	z	$F(x, y, z)$
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	0

	Tabell 3 Bolske identiteter
1	$\overline{\overline{x}} = x$
2	$x + x = x$
3	$x \cdot x = x$
4	$x + 0 = x$
5	$x \cdot 1 = x$
6	$x + 1 = 1$
7	$x \cdot 0 = 0$
8	$x + y = y + x$
9	$xy = yx$
10	$x + (y + z) = (x + y) + z$
11	$x(yz) = (xy)z$
12	$x + yz = (x + y)(x + z)$
13	$x(y + z) = xy + xz$
14	$\overline{(xy)} = \overline{x} + \overline{y}$
15	$\overline{(x + y)} = \overline{x} \overline{y}$
16	$x + xy = x$
17	$x(x + y) = x$
18	$x + \overline{x} = 1$
19	$x\overline{x} = 0$