UNIVERSITETET I TROMSØ
DET MATEMATISK
NATURVITENSKAPELIGE FAKULTET

Eksamen i:	MAT-1300, Diskret matematikk 2
Eksamensdag:	Fredag 11. juni 2004
Tid for eksamen	09.00-13.00
Tillatte hjelpemiddel:	Godkjent kalkulator og 2 ark notater

Oppgavesettet er på 3 sider.

Kontaktperson: Ragnar Soleng, tlf. 77644014

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

$$\begin{aligned} x &\equiv 1 \bmod 11 \\ x &\equiv 3 \bmod 23 \end{aligned}$$

Oppgave 2 *La $n = 551 = 19 \cdot 29$. Bruk Eulers teorem til å regne ut $2^{1008509} \bmod n$.*

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

La $n = 253$ og vi røper med en gang at faktoriseringen er $n = 11 \cdot 23$. Vi lar også $e = 67$.

a) Finn alle R slik at $R^{67} \equiv R \bmod 11$ og alle S slik at $S^{67} \equiv S \bmod 23$.

b) Finn et P slik at $P^{67} \equiv P \bmod n$. Denne P skal ikke være kongruent med $0 \bmod n$ og heller ikke $\pm 1 \bmod n$.

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

a) Bruk at 2 er en primitiv rot modulo 11 til å finne alle kvadratrester modulo 11.

b) Vis at produktet av en kvadratiske rest og en ikke-rest igjen er en ikke-rest.

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 $3 \bmod 4$. 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), hvordan går A frem for å finne den riktige kvadratrot av y? Dvs. den som er kongruent med $x^2 \bmod n$*.*

b) Hvordan kan hun være så sikker på at hun ikke røper noe om faktoriseringen av n?

c) Hvorfor blir B ved å gjenta protokollen flere ganger overbevist om at A kjenner p og q?

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) Vis at funksjonen $F(x, y, z)$ *i a) og kan skrives* $F(x, y, z) = z + x\overline{y}$ *ved å sammenligne output.*

c) Vis at funksjonen $F(x, y, z)$ *i a) og kan skrives* $F(x, y, z) = z + x\overline{y}$ *ved å bruke Karnaugh maps.*

d) Vis at funksjonen $F(x, y, z)$ *i a) og kan skrives* $F(x, y, z) = z + x\overline{y}$ *ved å bruke regnereglene for bolske algebraer. (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 sluttilstander.*

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

	f	
	Input	
Tilstand	0	1
s_0	s_0	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	1
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	$\overline{(x + y)} = \overline{xy}$
16	$x + xy = x$
17	$x(x + y) = x$
18	$x + \overline{x} = 1$
19	$x\overline{x} = 0$