UNIVERSITETET I TROMSØ
DET MATEMATISK-NATURVITENSKAPELIGE FAKULTET

Eksamen i:	MAT-1300, Diskret matematikk 2
Dato:	Fredag 9. juni 2006
Tid for eksamen:	0900-1300
Tillatte hjelpemidler:	Godkjent kalkulator, 2 A4-ark (4 sider) med egne notater (enten håndskrevne eller trykte) og Rottmanns tabeller

Oppgavesettet er på 3 sider.

Kontaktperson: Loren Olson, tlf. 99701428

Begrunn alle svarene. Hver av de 6 oppgavene teller likt.

Oppgave 1

a.) Finn alle løsninger (kongruensklasser) som tilfredsstiller kongruensligningen $3x \equiv 5 \pmod 7$.

b.) Finn alle løsninger (kongruensklasser) som tilfredsstiller kongruensligningen $6x \equiv 8 \pmod{11}$.

c.) Bruk det kinesiske restteorem og svarene fra a.) og b.) til å finne alle løsninger (kongruensklasser) som tilfredsstiller kongruensligningen $17x \equiv 19 \pmod{77}$.

Oppgave 2

a.) La $n = 55$. La ϕ betegne Eulers phi-funksjon. Beregn $\phi(n)$.

b.) Bruk Eulers teorem til å finne det minste positive heltall kongruent med 3^{100000} modulo $n = 55$.

c.) Vi skal se på RSA i denne delen av oppgaven. Alice oppgir $n = 55$ og $e = 7$ som sin offentlig nøkkel. Bob sender $C = M^e = 2 \; mod \; n$ til Alice. Finn M.

Oppgave 3

a.) Er -1 en kvadratrest modulo $p = 1019$? Er 2 en kvadratrest modulo $q = 1013$?

b.) Er 21 en kvadratrest modulo $p = 1019$?

c.) Vis at 91 er et pseudoprimtall med hensyn til 2.

Oppgave 4

a.) Finn ordenen til 2 modulo 5.

b.) Vis at 5 er en primitiv rot modulo 6.

c.) Vis at 12 ikke har noen primitive røtter.

Oppgave 5

a.) La $L = \{\, 0^m 1^n \mid m \text{ og } n \text{ er heltall} \geq 0 \,\}$. La G være frasestrukturgrammatikken med vokabular $V = \{S, 0, 1\}$, terminaler $T = \{0, 1\}$ og produksjoner $S \to 0S$, $S \to 1S$ og $S \to \lambda$. (Husk at S er startsymbolet og at λ er den tomme strengen.) Vis at G genererer L.

b.) Lag tilstandsdiagrammet for den endelige tilstandsmaskinen M som er gitt ved følgende tilstandstabell:

	f		*g*	
	Input		***Input***	
State	***0***	***1***	***0***	***1***
s_0	s_1	s_0	1	0
s_1	s_3	s_0	1	1
s_2	s_1	s_2	0	1
s_3	s_2	s_1	0	0

Oppgave 6

a.) Lag en tabell som viser verdiene av den Boolske funksjonen $F(x, y, z) = \bar{x}y$.
b.) Finn sum av produkt utviklingen av $F(x, y) = \bar{y}$.
c.) Bruk et K-kart (="Karnaugh map") til å finne en minimal utvikling av $xy + x\bar{y} + \bar{x}y + \bar{x}\bar{y}$ som en Boolsk sum av Boolske produkter.

Boolean Identities.

Identity	*Name*
$\overline{\overline{x}} = x$	Law of the double complement
$x + x = x$ $x \cdot x = x$	Idempotent laws
$x + 0 = x$ $x \cdot 1 = x$	Identity laws
$x + 1 = 1$ $x \cdot 0 = 0$	Domination laws
$x + y = y + x$ $xy = yx$	Commutative laws
$x + (y + z) = (x + y) + z$ $x(yz) = (xy)x$	Associative laws
$x + yz = (x + y)(x + z)$ $x(y + z) = xy + xz$	Distributive laws
$\overline{(xy)} = \overline{x} + \overline{y}$ $\overline{(x + y)} = \overline{x}\,\overline{y}$	De Morgan's laws
$x + xy = x$ $x(x + y) = x$	Absorption laws
$x + \overline{x} = 1$	Unit property
$x\overline{x} = 0$	Zero property