UNIVERSITETET I TROMSØ
DET MATEMATISK
NATURVITENSKAPELIGE FAKULTET

Eksamen i:	MAT-1300, Diskret matematikk 2
Eksamensdag:	Fredag 28. september 2007
Tid for eksamen	09.00-13.00
Tillatte hjelpemiddel:	Godkjent kalkulator og 2 ark notater

Kontaktperson: Andrei Prasolov, tlf. 93675832

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

$$\begin{aligned} x &\equiv 1 \bmod 67 \\ x &\equiv 3 \bmod 19 \end{aligned}$$

b) La $n = 67 \cdot 19 = 1273$. Bruk Eulers teorem til å regne ut $2^{3567} \bmod n$.

Oppgave 2 *I Pollard Rho metoden skal man fortløpende beregne $x_k \bmod m$ etter rekursjonen*

$$\begin{aligned} x_1 &= a \text{ (velg selv)} \\ x_k &= f(x_{k-1}) \bmod m \end{aligned}$$

her er $f(x)$ et polynom, vanligvis er $f(x) = x^2 + 1$ et godt valg. Så beregnes $\gcd(x_{2k} - x_k, m)$ og man har funnet en faktor hvis denne er større enn 1.

a) Bruk Pollard Rho – metode til å faktorisere tallet 989.

b) Forklar hvorfor metoden virker.

Oppgave 3 *a) Vis at $r = 7$ er en primitiv rot modulo $p = 41$.*

b) Løs ligningen $x^6 \equiv 40 \bmod 41$ (Merk at $40 \equiv 7^{20} \bmod 41$.).

c) Hvor mange løsninger har ligningen $x^{15} \equiv 49 \bmod 41$?

Oppgave 4 *Output for en boolsk funksjon $F(x, y, z)$ 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 $F(x,y,z) = x\bar{z} + \bar{x}\ y$ ved å sammenligne output.

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

d) Vis at funksjonen $F(x,y,z)$ i a) og kan skrives $F(x,y,z) = x\bar{z} + \bar{x}\ y$ ved å bruke regnereglene for bolske algebraer. (Regnereglene står i tabell 2 under.)

Oppgave 5 *a) Det oppgis at* 991 *er et primtall. Beregn Legendre symbolet:* $\left(\frac{111}{991}\right)$

b) Bruk Kvadratisk resiprositet til å vise at hvis p er et odde primtall ($p \neq 3$), så er:

$$\left(\frac{3}{p}\right) = \begin{cases} 1 \text{ hvis } p \equiv \pm 1 \bmod 12 \\ -1 \text{ hvis } p \equiv \pm 5 \bmod 12 \end{cases}$$

c) Finn en tilsvarende kongruensbetingelse som i b) for nårtid 5 *er en kvadratisk rest modulo et odde primtall $p \neq 5$.*

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

	Tabell 2 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	$x\overline{x} = 0$