EKSAMENSOPPGAVE MAT-1300

Eksamen i	:	**MAT-1300 Diskret matematikk 2.**
Dato	:	**Onsdag 28. september 2005.**
Tid	:	**09.00 - 13.00.**
Sted:	:	**Aud. Max.**
Tillatte hjelpemidler	:	**Godkjent kalkulator og 2 ark notater.**

Oppgavesettet er på 5 sider eks. forside.

Kontaktperson: Professor Andrei Prasolov, mobil 93 67 58 32.

Begrunn svarene dine, vis fremgangsmåte ved oppgaveløsningen tydelig!

1 OPPGAVE

Vi minner om at $\phi(n)$ er Eulers ϕ-funksjon.
La $n = 1021 \cdot 1031 = 1052\,651$.

a) Regn ut $\phi(n)$;

b) Regn ut

$$x = 3^{1234\,454\,996} \bmod 1052\,651$$

og

$$y = 3^{-1234\,454\,996} \bmod 1052\,651$$

ved hjelp av Eulers teorem.

Hint: beregningene kan forenkles ved hjelp av kongruensen

$$x \cdot y \equiv 1 \,(\mathrm{mod}\, 1052\,651)$$

c) Et RSA-kryptosystem (n, e, d) baseres på heltallet n som er et produkt av to forskjellige primtall p og q:

$$n = p \cdot q, p \neq q.$$

En klartekst X (som er et heltall) krypteres ved hjelp av den offentlige krypteringsnøkkelen e på følgende måte:

$$Y = X^e \bmod n.$$

Den krypterte teksten Y dekrypteres ved hjelp av den hemmelige dekrypteringsnøkkelen d:

$$X = Y^d \bmod n.$$

La $n = 1021 \cdot 1031 = 1052\,651$ som i forrige deloppgaver. Hvilke av de fem verdiene e nedenfor som **ikke** kan brukes som krypteringsnøkler:

$$e = 2, 3, 5, 7, 11?$$

Forklar hvorfor.

d) I kryptosystemet fra deloppgave **c)** er krypteringsnøkkelen e lik 13. Finn dekrypteringsnøkkelen d.

2 OPPGAVE

La

$$n = 17^3 = 4913.$$

a) Vis at $r = 3$ er en primitiv rot modulo n.

b) Finn **alle** ikke-kongruente **løsninger** til kongruensen

$$x^4 \equiv 81 \pmod{4913}.$$

Hint: skriv x som

$$x \equiv r^s \bmod 4913.$$

c) La a være et heltall innbyrdes primisk med 4913:

$$\gcd(a, 4913) = 1.$$

Bevis setningen nedenfor:

Kongruensen

$$x^8 \equiv a \pmod{4913}$$

har minst én løsning hvis og bare hvis

$$a^{578} \equiv 1 \pmod{4913}.$$

Hint: skriv a som

$$a \equiv r^t \bmod 4913.$$

3 OPPGAVE

a) Finn alle kvadratrester modulo 7.

b) Finn alle kvadratrester modulo 23.

c) Den virkelige minimale kunnskapsprotokollen brukes for et produkt av **store** primtall. Vi skal modellere protokollen for små tall. La $p = 7$, $q = 23$, og $n = p \cdot q = 161$. Både Anne og Bjørn kjenner tallet n. Anne påstår at hun kan faktorisere n. For å sjekke dette, gjør Bjørn følgende: han velger et heltall x,

$$1 \leq x \leq n - 1,$$

og sender tallet $x^4 \bmod 161 = 128$ til Anne. Hennes oppgave er å finne $y = x^2 \bmod 161$. Hjelp Anne til å løse oppgaven, dvs. finn

$$y = x^2 \bmod 161.$$

Hint: løs kongruensene

$$\begin{aligned} y^2 &\equiv 128 \,(\mathrm{mod}\, 7)\,, \\ y^2 &\equiv 128 \,(\mathrm{mod}\, 23)\,. \end{aligned}$$

Bruk deretter deloppgavene **a)** og **b)** og Det Kinesiske Restteorem.

4 OPPGAVE

Gitt en boolsk funksjon

$$f(u, v, x, y) = (u + v) \cdot (v + x) \cdot (x + y)\,.$$

a) Finn den disjunktive normale formen (*sum of products*) til funksjonen f.

Hint: formelen skal være summen av **åtte** produkter. Hvert produkt skal ha formen

$$\widetilde{u} \cdot \widetilde{v} \cdot \widetilde{x} \cdot \widetilde{y}$$

der

$$\begin{aligned} \widetilde{u} &= u \text{ eller } \overline{u}, \\ \widetilde{v} &= v \text{ eller } \overline{v}, \\ \widetilde{x} &= x \text{ eller } \overline{x}, \\ \widetilde{y} &= y \text{ eller } \overline{y}. \end{aligned}$$

b) Forenkle formelen til f mest mulig. Du velger selv om du bruker Karnaugh metode, eller Quine-McCluskey metode, eller **beviser** den forenklede formelen ved hjelp av boolske identiteter i Tabell 1 nedenfor.

Hint: resulterende forenklede formelen skal være summen av **tre** produkter.

	Tabell 1		Boolske identiteter
1	$\overline{\overline{x}} = x$	11	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2	$x + x = x$	12	trengs ikke
3	$x \cdot x = x$	13	$x \cdot (y + z) = x \cdot y + x \cdot z$
4	$x + 0 = x$	14	$\overline{x \cdot y} = \overline{x} + \overline{y}$
5	$x \cdot 1 = x$	15	$\overline{x + y} = \overline{x} \cdot \overline{y}$
6	$x + 1 = 1$	16	$x + x \cdot y = x$
7	$x \cdot 0 = 0$	16a	$x + \overline{x} \cdot y = x + y$
8	$x + y = y + x$	17	trengs ikke
9	$x \cdot y = y \cdot x$	18	$x + \overline{x} = 1$
10	$x + (y + z) = (x + y) + z$	19	$x \cdot \overline{x} = 0$

5 OPPGAVE

En ikke-deterministisk endelig tilstandsmaskin

$$M = (S, I, f, s_0, F)$$

er gitt i tabell 2. s_0 og s_4 er sluttilstander (*final states*).

Tabell 2		
	f	
	Input	
Tilstand	0	1
$\mathbf{s_0}$	s_1	
s_1		s_0, s_2
s_2	s_3	
s_3	s_4	s_5
$\mathbf{s_4}$		
s_5	s_1, s_6	s_6
s_6		

a) Tegn tilstandsdiagram (rettet graf);

b) Finn språket $L(M)$ som gjenkjennes av maskinen M;

c) Finn en deterministisk maskin som gjenkjenner det samme språket $L(M)$. Tegn tilstandsdiagram.

d) Begrunn at ordet 0101001 **ikke** gjenkjennes av maskinen.

Hint: bruk den deterministiske maskinen fra deloppgave **c)**.

LYKKE TIL!