EKSAMENSOPPGAVE MAT-1300

Eksamen i	:	**MAT-1300 Diskret matematikk 2.**
Dato	:	**Fredag 10. juni 2005.**
Tid	:	**09.00 - 13.00.**
Sted:	:	**Aud. Max.**
Tillatte hjelpemidler	:	**Godkjent kalkulator og 2 ark notater.**

Oppgavesettet er på 6 sider eks. forside.

Kontaktperson: Professor Andrei Prasolov, mobil 48 12 50 27.

Begrunn svarene dine, vis fremgangsmåte ved oppgaveløsningen tydelig!

1 OPPGAVE

Vi minner om at $\tau(n)$ er antall ikke-negative divisorer til n, $\sigma(n)$ er summen av ikke-negative divisorer til n, og $\phi(n)$ er Eulers ϕ-funksjon.

La $n = 31 \cdot 37^2 = 42\,439$.

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

b) Regn ut $\sigma(n)$;

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

d) Regn ut

$$2^{4915\,089} \bmod n$$

ved hjelp av Eulers teorem.

2 OPPGAVE

a) La $n = 3 \cdot 5 \cdot 7 = 105$. Finn **alle** ikke-kongruente **løsninger** til kongruensen

$$x^3 \equiv 62 \,(\mathrm{mod}\, n)\,.$$

Hint: løs kongruensen modulo 3, 5 og 7, og bruk det kinesiske restteoremet.

b) La p være et primtall med

$$p \equiv 5 \,(\mathrm{mod}\, 6)\,,$$

og la

$$m = p^s, s \geq 1.$$

Vis at for hvert a, innbyrdes primisk med p, **eksisterer det** nøyaktig **én** ikke-kongruent **løsning** til kongruensen

$$x^3 \equiv a \,(\mathrm{mod}\, m)\,.$$

Hint: undersøk om det eksisterer en primitiv rot r modulo m, og beskriv a som

$$a \equiv r^k \,(\mathrm{mod}\, m)\,.$$

Søk deretter løsningene på formen $x \equiv r^y$.

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

$$p \equiv q \equiv -1 \,(\mathrm{mod}\, 6)$$

og $e = 3$.

Finn dekrypteringsnøkkelen d (betegn $p = 6s - 1$ og $q = 6t - 1$ og uttrykk d ved s og t).

Hvis det er vanskelig for deg å løse deloppgaven **generelt**, prøv å løse den for **konkrete** verdier $p = 1013$ og $q = 1019$.

3 OPPGAVE

La p være et primtall, $p \equiv 3(\mathrm{mod}\, 4)$, og la a være et heltall, innbyrdes primisk med p. Anta Legendre symbolet $\left(\frac{a}{p}\right)$ er lik 1.

a) Vis at kongruensen

$$x^2 \equiv a \,(\mathrm{mod}\, p)$$

har nøyaktig **to** ikke-kongruente **løsninger**:

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}.$$

b) Vis at **hver** av kongruensene

$$\begin{aligned} x^4 &\equiv a \pmod{p}, \\ x^8 &\equiv a \pmod{p}, \\ x^{16} &\equiv a \pmod{p} \end{aligned}$$

har **nøyaktig to** ikke-kongruente løsninger.

Hint: bruk deloppgave **a)** og Legendre symbolet $\left(\frac{-1}{p}\right)$.

c) Den riktige minimale kunnskapsprotokollen brukes for et produkt av **store** primtall. Vi skal modellere protokollen for relativt små tall. La $p = 103$, $q = 107$, og $n = p \cdot q = 11\,021$. 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 $x^4 \bmod n = 9793$ til Anne. Hennes oppgave er å finne $y = x^2 \bmod n$. Hun løser følgende kongruenser (ved hjelp av metoden fra deloppgave **a)**): $y^2 \equiv 9793 \pmod{103}$ og $y^2 \equiv 9793 \pmod{107}$. Resultatene er $\pm 9793^{26} \bmod 103 = \pm 27$: og $\pm 9793^{27} \bmod 107 = \pm 85$. Ved hjelp av det kinesiske restteoremet, løser Anne 4 kongruenser:

$$\begin{aligned} y &\equiv 27 \pmod{103} \\ y &\equiv 85 \pmod{107} \\ &\Longrightarrow y \equiv 4044 \pmod{n} \end{aligned}$$

$$\begin{aligned} y &\equiv 27 \pmod{103} \\ y &\equiv -85 \pmod{107} \\ &\Longrightarrow y \equiv 2911 \pmod{n} \end{aligned}$$

$$\begin{aligned} y &\equiv -27 \pmod{103} \\ y &\equiv 85 \pmod{107} \\ &\Longrightarrow y \equiv 8110 \pmod{n} \end{aligned}$$

$$\begin{aligned} y &\equiv -27 \,(\mathrm{mod}\, 103) \\ y &\equiv -85 \,(\mathrm{mod}\, 107) \\ &\Longrightarrow\ y \equiv 6977 \,(\mathrm{mod}\, n) \end{aligned}$$

Hvilken av de fire verdiene til y (4044, 2911, 8110, eller 6977) er **riktig**? Forklar fremgangsmåten.

4 OPPGAVE

En digital krets får som input ordnede par (x, y) av ikke-negative heltall $0 \leq x \leq 3$, $0 \leq y \leq 3$. Tallene kodes som 2-bit binære tall på vanlig måte:

$$\begin{aligned} 0 &\iff 00, \\ 1 &\iff 01, \\ 2 &\iff 10, \\ 3 &\iff 11. \end{aligned}$$

Vi skriver nå $x = a_1a_2$ og $y = b_1b_2$ binært. Kretsen utfører addisjonen av de to tallene, og produserer et 3-bit binært heltall. Vi betrakter den boolske funksjonen

$$c = f\,(a_1, a_2, b_1, b_2)$$

der c er er den første bit i summen av de to binære tall a_1a_2 og b_1b_2. Se eksemplene nedenfor (Tabell 1):

				Tabell 1:	
				Addisjon av 2-bit tall	
a_1	a_2	b_1	b_2	$c = f\,(a_1, a_2, b_1, b_2)$	Kommentar
0	1	1	0	0	$01 + 10 \rightarrow 1 + 2 = 3 \rightarrow \mathbf{0}11$
1	1	1	0	1	$11 + 10 \rightarrow 3 + 2 = 5 \rightarrow \mathbf{1}01$
0	1	1	1	1	$01 + 11 \rightarrow 1 + 3 = 4 \rightarrow \mathbf{1}00$
1	0	0	0	0	$10 + 00 \rightarrow 2 + 0 = 2 \rightarrow \mathbf{0}10$

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

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

$$\widetilde{a_1} \cdot \widetilde{a_2} \cdot \widetilde{b_1} \cdot \widetilde{b_2}$$

der

$$\begin{aligned} \widetilde{a_1} &= a_1 \text{ eller } \overline{a_1}, \\ \widetilde{a_2} &= a_2 \text{ eller } \overline{a_2}, \\ \widetilde{b_1} &= b_1 \text{ eller } \overline{b_1}, \\ \widetilde{b_2} &= b_2 \text{ eller } \overline{b_2}. \end{aligned}$$

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 2 nedenfor.

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

	Tabell 2		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 3. s_0, s_1, s_2 er sluttilstander (*final states*).

Tabell 3		
	f	
	Input	
Tilstand	0	1
$\mathbf{s}_0$	s_1	s_2
$\mathbf{s}_1$		s_3
$\mathbf{s}_2$	s_4	
s_3	s_1	
s_4	s_5	s_2, s_5
s_5		

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 1010100 **ikke** gjenkjennes av maskinen.

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

LYKKE TIL!