Kunnskap for ei betre verd

Institutt for matematiske fag

Eksamensoppgåve i **MA1301/MA6301 Talteori**

Fagleg kontakt under eksamen: Richard Williamson

Tlf: (735) 90154

Eksamensdato: Torsdag 4. desember 2014

Eksamenstid (frå–til): 09:00 – 13:00

Hjelpemiddelkode/Tillatne hjelpemiddel: D: Ingen prenta eller handskrive hjelpemiddel tillatne. Bestemt, enkel kalkulator tillaten. Tillatne kalkulatorer: Hewlett Packard HP30S, Citizen SR-270X, Citizen SR-270X College, Casio fx-82ES PLUS.

Annan informasjon:
Svar på alle dei seks oppgåvene. Alle svar skal grunngjevast. Kvar oppgåve er verd fem poeng. Moglege poeng for kvar del angjes i parentes. Det er ikkje naudsynt å løyse oppgåvene i rekkjefylgje.

Hvis du ikkje kan løyse ein del av ein oppgåve etter å ha prøvd ei stund, gå vidare og kom heller tilbake til den: ikkje bruk for mykje tid på kvar del. Skriv ned så mykje du kan om korleis du ville løyse oppgåver du ikkje får til.

Nytt gjerne eit utsagn i ein del av ein oppgåve i resten av oppgåven, selv om du ikkje har vist at det er sant.

Nytt gjerne fylgjande resultater frå kurset når det høver.

(I) Lat p og q vere primtal slik at $p > 2$, $q > 2$, og $p \neq q$. Dersom $p \equiv 1 \pmod 4$ eller $q \equiv 1 \pmod 4$, eller begge disse kongruensane er sanne, er $\mathbb{L}_q^p = \mathbb{L}_p^q$. Dersom $p \equiv 3 \pmod 4$ og $q \equiv 3 \pmod 4$, er $\mathbb{L}_q^p = -\mathbb{L}_p^q$.

(II) Lat p være eit primtall slik at $p > 2$. Dersom $p \equiv 1 \pmod 8$ eller $p \equiv 7 \pmod 8$ er $\mathbb{L}_p^2 = 1$. Ellers er $\mathbb{L}_p^2 = -1$.

Lykke til!

Målform/språk: nynorsk

Sidetal: 3

Sidetal vedlegg: 0

Kontrollert av:

Dato Sign

Oppgåve 1 Sekvensen av Fibonaccitall u_1, u_2, u_3, … er definert ved rekursjon som fylgjer:

(1) $u_1 = 1$;

(2) $u_2 = 1$;

(3) Anta at $u_1, u_2, \ldots, u_m$ har blitt definert, kor $m \geq 2$. Da definerer vi:

$$u_{m+1} = u_m + u_{m-1}.$$

a) Rekn ut u_4 og u_5. [0.5 poeng]

b) Ved å referere til definisjonen av ein kongruens, forklar kvifor

$$u_4 \equiv u_1 \pmod 2$$

og

$$u_5 \equiv u_2 \pmod 2.$$

[1 poeng]

c) Lat n være eit naturleg tal. Bevis at

$$u_{n+3} \equiv u_n \pmod 2.$$

Tips: Nytt induksjon og b). [2.5 poeng]

d) Er u_{371} eit oddetal eller eit partal? [1 poeng]

Oppgåve 2

a) Finn eit heiltal x slik at:

(1) $0 \leq x < 1292$;
(2) $x \equiv 3 \pmod 4$;
(3) $x \equiv 2 \pmod{17}$;
(4) $x \equiv 3 \pmod{19}$.

[3.5 poeng]

b) Vis at det ikkje fins eit heiltal x slik at:

(1) $x \equiv 4 \pmod 6$;
(2) $x \equiv 11 \pmod{15}$.

[1.5 poeng]

Oppgåve 3

a) Vis utan å rekne ut at
$$2 \cdot 3^{472} \equiv 3 \pmod{53}.$$
[2.5 poeng]

b) Vis utan å rekne ut at $36 \cdot (49!) - 4 \cdot 3^{472}$ er deleleg med 53. [2.5 poeng]

Oppgåve 4

a) Finn ei løysing til fylgjande kvadratiske kongruens.
$$12x^2 - 21x + 8 \equiv 0 \pmod{61}.$$
Tips: Nytt at
$$39^2 \equiv 57 \pmod{61}.$$
[1.5 poeng]

b) Kor mange heiltal x slik at $0 \leq x < 43789$ finnes det slik at x er ei løysing til fylgjande kvadratiske kongruens?
$$13x^2 + 238x + 269 \equiv 0 \pmod{43789}$$
Du kan nytte utan grunngjeving at 43789 er eit primtal, og at
$$42656 = 2^5 \cdot 31 \cdot 43.$$
[3.5 poeng]

Oppgåve 5

Person B har fått ei melding fra person A som har blitt krypert av RSA-algoritmen. Tabellen vedlagt med eksamen har blitt nytta for å omsetja frå symboler til heiltal. Det fyrste heiltalet i den krypterte meldinga er 25. Den offentlege nykelen til person B er $(187, 53)$. Knekk koden til det fyrste symbolet i meldinga. *Tips*: Du kjem til å trenge å rekne ut noko som er for stort for kalkulatoren din. Nytt da at
$$25^7 \equiv -2 \pmod{187}.$$
[5 poeng]

Oppgåve 6

a) Skriv dei fyrste fem primtala p slik at $p \equiv 2 \pmod{3}$. [1 poeng]

b) Lat n være eit naturleg tal. Bevis at det finnes eit primtal p slik at $p > n$ og $p \equiv 2 \pmod{3}$. Med andre ord, bevis at det finnes uendeleg mange primtall p slik at $p \equiv 2 \pmod{3}$. *Tips*: Lat q være produktet av alle primtala som er mindre enn eller lik n, og som er kongruent til 2 modulo 3. Nytt primtallsfaktoriseringa til $3q - 1$. [3 poeng]

c) Kva primtal p får vi frå argumentet ditt når $n = 14$? [1 poeng]

Symbol	Tilsvarande heiltal
	0
A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8
I	9
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26
Æ	27
Ø	28
Å	29
0	30
1	31
2	32
3	33
4	34
5	35
6	36
7	37
8	38
9	39
.	40
,	41
!	42
:	43
–	44
?	45

Tabell 1: Korleis omsette mellom symboler og heiltal