NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **MA1301/MA6301 Tallteori**

Faglig kontakt under eksamen: Richard Williamson

Tlf: (735) 90154

Eksamensdato: Torsdag 4. desember 2014

Eksamenstid (fra–til): 09:00 – 13:00

Hjelpemiddelkode/Tillatte hjelpemidler: D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Tillatte kalkulatorer: Hewlett Packard HP30S, Citizen SR-270X, Citizen SR-270X College, Casio fx-82ES PLUS.

Annen informasjon:
Besvar alle de seks oppgavene. Begrunn svarene dine. Hver oppgave er verdt fem poeng. Mulige poeng for hver del angis i parentes. Det er ikke nødvendig å løse oppgavene i rekkefølge.

Hvis du ikke kan løse en del av en oppgave etter å ha prøvd en stund, gå videre og kom heller tilbake til den: ikke bruk for mye tid på hver del. Skriv ned så mye du kan om hvordan du ville løse oppgaver du ikke får til.

Benytt gjerne et utsagn i en del av en oppgave i resten av oppgaven, selv om du ikke har vist at det er sant.

Benytt gjerne følgende resultater fra kurset når de passer.

(I) La p og q være primtall 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 kongruensene 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) La p være et 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: bokmål

Antall sider: 4

Antall sider vedlegg: 0

Kontrollert av:

Dato Sign

Oppgave 1 Sekvensen av Fibonaccitall u_1, u_2, u_3, ... er definert ved rekursjon som følger:

(1) $u_1 = 1$;

(2) $u_2 = 1$;

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

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

a) Beregn u_4 og u_5. [0.5 poeng]

b) Ved å referere til definisjonen av en kongruens, forklar hvorfor

$$u_4 \equiv u_1 \pmod 2$$

og

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

[1 poeng]

c) La n være et naturlig tall. Bevis at

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

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

d) Er u_{371} et oddetall eller et partall? [1 poeng]

Oppgave 2

a) Finn et heltall 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 ikke finnes et heltall x slik at:

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

[1.5 poeng]

Oppgave 3

a) Vis uten å regne ut at

$$2 \cdot 3^{472} \equiv 3 \pmod{53}.$$

[2.5 poeng]

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

Oppgave 4

a) Finn en løsning til følgende kvadratisk kongruens.

$$12x^2 - 21x + 8 \equiv 0 \pmod{61}.$$

Tips: Benytt at

$$39^2 \equiv 57 \pmod{61}.$$

[1.5 poeng]

b) Hvor mange heltall x slik at $0 \leq x < 43789$ finnes det slik at x er en løsning til følgende kvadratisk kongruens?

$$13x^2 + 238x + 269 \equiv 0 \pmod{43789}$$

Du kan benytte uten begrunnelse at 43789 er et primtall, og at

$$42656 = 2^5 \cdot 31 \cdot 43.$$

[3.5 poeng]

Oppgave 5

Person B har fått en melding fra person A som har blitt krypert av RSA-algoritmen. Tabellen vedlagt med eksamen har blitt benyttet for å oversette fra symboler til heltall. Det første heltallet i den krypterte meldingen er 25. Den offentlige nøkkelen til person B er $(187, 53)$. Knekk koden til det første symbolet i meldingen. *Tips*: Du kommer til å trenge å regne ut noe som er for stort for kalkulatoren din. Benytt da at

$$25^7 \equiv -2 \pmod{187}.$$

[5 poeng]

Oppgave 6

a) Skriv de første fem primtallene p slik at $p \equiv 2 \pmod 3$. [1 poeng]

b) La n være et naturlig tall. Bevis at det finnes et primtall p slik at $p > n$ og $p \equiv 2 \pmod 3$. Med andre ord, bevis at det finnes uendelig mange primtall p slik at $p \equiv 2 \pmod 3$. *Tips*: La q være produktet av alle primtallene som er mindre enn eller like n, og som er kongruent til 2 modulo 3. Benytt primtallsfaktoriseringen til $3q - 1$. [3 poeng]

c) Hvilket primtall p får vi fra argumentet ditt når $n = 14$? [1 poeng]

Symbol	Tilsvarende heltall
	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: Hvordan oversette mellom symboler og heltall