NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **MA1301/MA6301 Number theory**

Academic contact during examination: Richard Williamson

Phone: (735) 90154

Examination date: Thursday 4th December 2014

Examination time (from–to): 09:00 – 13:00

Permitted examination support material: D: No printed or hand-written support material is allowed. Permitted calculators: Hewlett Packard HP30S, Citizen SR-270X, Citizen SR-270X College, Casio fx-82ES PLUS.

Other information:
Answer all four problems. Justify your answers. Each problem is worth 5 marks. The possible marks for each part is given in brackets. It is not necessary to solve the problems in order.

If you cannot solve a part of a problem after having tried a while, move on and come back later to it instead: don't spend too much time on each part. Write down as much as you can regarding how you would like to solve a problem that you are unable to answer.

You can appeal to an assertion in a part of a problem in the rest of the problem, even if you have not shown that the assertion is true.

You can make use of the following results from the course where it is possible to do so.

(I) Let p and q be prime numbers such that $p > 2$, $q > 2$, and $p \neq q$. If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, or both of these congruences hold, then $\mathbb{L}_q^p = \mathbb{L}_p^q$. If $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, then $\mathbb{L}_q^p = -\mathbb{L}_p^q$.

(II) Let p be a prime number such that $p > 2$. If $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$, then $\mathbb{L}_p^2 = 1$. Otherwise we have that $\mathbb{L}_p^2 = -1$.

Good luck!

Language: English

Number of pages: 4

Number pages enclosed: 0

Checked by:

Date Signature

Problem 1 The sequence of Fibonacci numbers u_1, u_2, u_3, ... is defined by recursion as follows:

(1) $u_1 = 1$;

(2) $u_2 = 1$;

(3) Assume that $u_1, u_2, \ldots, u_m$ has been defined, where $m \geq 2$. We then define:

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

a) Calculate u_4 and u_5. [0.5 marks]

b) Referring to the definition of a congruence, explain why

$$u_4 \equiv u_1 \pmod 2$$

and

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

[1 mark]

c) Let n be a natural number. Prove that

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

Hint: Use induction and b). [2.5 marks]

d) Is u_{371} an odd number or an even number? [1 mark]

Problem 2

a) Find an integer x such that:

(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 marks]

b) Show that there does not exist an integer x such that:

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

[1.5 marks]

Problem 3

a) Show without calculating that

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

[2.5 marks]

b) Show without calculating that $36 \cdot (49!) - 4 \cdot 3^{472}$ is divisible by 53. [2.5 marks]

Problem 4

a) Find a solution to the following quadratic congruence.

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

Hint: Use that

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

[1.5 marks]

b) How many integers x such that $0 \leq x < 43789$ are there such that x is a solution to the following quadratic congruence?

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

You can use without justification that 43789 is a prime number, and that

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

[3.5 marks]

Problem 5

Person B has received a message from Person A which has been encrypted by means of the RSA algorithm. The table included with the exam has been used to translate from symbols to integers. The first integer in the encrypted message is 25. Person B's public key is $(187, 53)$. Break the code of the first symbol in the message. *Hint*: You will need to calculate something which is too large for your calculator. Use then that

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

[5 marks]

Problem 6

a) Write down the first five prime numbers p such that $p \equiv 2 \pmod 3$. [1 mark]

b) Let n be a natural number. Prove that there exists a prime number p such that $p > n$ and $p \equiv 2 \pmod 3$. In other words, prove that there exists infinitely many prime numbers p such that $p \equiv 2 \pmod 3$. *Hint*: Let q be the product of all prime numbers which are less than or equal to n, and which are congruent to 2 modulo 3. Use the prime factorisation of $3q - 1$. [3 marks]

c) Which prime number p do we obtain from your argument when $n = 14$? [1 mark]

Symbol	Corresponding integer
	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

Table 1: How to translate between symbols and integers