Norwegian University of Science and Technology
Department of Mathematical Sciences

Department contact during exam:
Magnus Landstad (47259811)

Exam in MA1301 Number Theory

English
Friday December 7, 2012
Time: 09:00 – 13:00 (4 hours)
Grades due: January 4, 2013

Examination Aids
Code D (Simple calculator: HP30S, Citizen SR-270X eller Citizen SR-270X college)

Give reasons for all answers.

Problem 1 Find all solutions of the system

$$\begin{aligned} 2x &\equiv 4 \pmod{6} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 1 \pmod{11} \end{aligned}$$

Problem 2

If $n = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \ldots + a_k \cdot 10^k$ for integers $0 \le a_i \le 9$ the integer $T(n) = a_0 + a_1 + \ldots + a_k$ is called the crossum of n. Show that $m = 3$ and $m = 9$ are the only integers $m > 1$ such that $m|n$ if and only if $m|T(n)$.

Problem 3 How is Euler's ϕ-function defined? Find all n such that $\phi(n) = 8$.

Problem 4

a) Find all solutions of the congruence $13x \equiv 1 \pmod{60}$.

b) In a RSA-cryptosystem the secret decryptation key is $\{n, d\} = \{77, 13\}$. What is then the public decryptation key $\{n, e\}$?

c) Decode the message $N = 20$.

Problem 5

a) What is the definition of a primitive root modulo n?

b) Find one primitive root of 17 and explain how this can be used to find all primitive roots modulo 17.

c) Let p and q be prime nunbers such that $p = 2q + 1$. Show that 4 has order q modulo p.

Problem 6 Show that there are no integers m and n such that $m^5 - m = n^2 + 2$. (Hint: solve the equation modulo 5.)

Problem 7 Has the congruence $x^2 \equiv 311 \pmod{19}$ any solutions? Use this to determine whether the congruence $x^2 \equiv 19 \pmod{311}$ has solutions.