Department of Mathematical Sciences

Examination in **MA1301/6301 Number Theory**

For questions during the exam:
Tel:

Examination date: 7. December 2013
Time (from–to): 9.00–13.00
Aid code/Allowed aids: D
Specified calculator (Citizen SR-270X or HP 30S)
No other aids have been specified

Language: English
Number of pages: 2
Number of additional pages: 0

Kontrollert av:

Dato Sign

Note! Students will find their grades in "Studentweb". If you have questions regarding your grades, you must contact the department. The examination office cannot answer such questions.

Give reasons for all answers.

Problem 1

a) Compute the greatest common divisor of 161 and 217.

b) Determine all integers c for which

$$217x + 161y = c.$$

has integer solutions.

c) Find all solutions to the following Diophantine equation:

$$217x + 161y = 14.$$

Problem 2 Find all integer solutions of the system

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 12 \mod 7 \\ x &\equiv 20 \mod 13. \end{aligned}$$

Problem 3

a) Suppose n is a positive integer. Let a be an integer relatively prime to n. Define the following notions:

(i) the order of a modulo n;

(ii) a primitive root of n.

b) Determine the order of $1, 2, 3, 4, 5, 6$ modulo 7.

Problem 4

a) Suppose p is an odd prime and a such that $\gcd(a, p) = 1$. Define the following notions:

(i) a is a quadratic residue modulo p;

(ii) a is a quadratic nonresidue modulo p;

(iii) the Legendre symbol $\left(\frac{a}{p}\right)$.

b) Suppose p is an odd prime and a such that $\gcd(a, p) = 1$. Show that $x^2 \equiv a \mod p$ has either no solution or exactly two solutions x_0 and $p - x_0$.

c) State the Quadratic Reciprocity Theorem.

d) Compute $\left(\frac{281}{397}\right)$ and explain each step of the computation.

Problem 5

a) Define for an arithmetic function f the notion of multiplicativity.

b) Define Euler's φ-function. Give the expression of $\varphi(p_1^{k_1}p_2^{k_2}p_3^{k_3})$ for distinct primes p_1, p_2, p_3.

c) Compute $\varphi(60)$.

Problem 6 In a RSA-cryptosystem the public decryption key is $\{n, e\} = \{55, 3\}$.

a) What is the secret key $\{n, d\}$?

b) Encrypt the message $m = 18$.