MFK-M310 Introduction to number theory and its applications,

Exam 18.12.2023

Solve all tasks. Remember to justify your claims and write down your calculations. You can use a calculator as support, but not for solving equations or calculating congruences directly. Your calculations should be written so that it is be believable that the calculations could have been done by hand.

1. (a) Determine the greatest common divisor of numbers 315 and 141 by using the Euclidian algorithm.
   (b) Calculate $\varphi(250)$
   (c) Let n be a positive integer. What is the definition of congruence modulo n?

2. Solve the system of congruence equations

$$\begin{cases} x \equiv 3 \pmod{11}, \\ x \equiv 5 \pmod{12}. \end{cases}$$

3. RSA is used with primes $p = 7$ and $q = 11$.
   (a) How many possible encryption exponents e are there, when $1 \leq e \leq \varphi(pq)$? (3p)
   (b) Let us use encryption exponent $e = 53$. Determine the decryption exponent d and decipher message 5. (9p)

4. Prove that $n^7 - n$ is divisible by 14 for all integers n.

5. (a) Is number 5 a primitive root modulo 23?
   (b) Show that $\ln 2$ is irrational. (Here ln is the natural logarithm.) You can assume known that Euler's number (or Napier's constant) e is transcendental.