Kenmerk: EWI2019/TW/DMMP/MU/Mod7/Exam3

Re-Exam 3, Module 7, Codes 201400483 & 201800141

Discrete Structures & Efficient Algorithms

Thursday, April 18, 08:45 - 10:45

All answers need to be motivated. No calculators. You are allowed to use a handwritten cheat sheet (A4, both sides).

This third re-exam of Module 7 consists of the **Algebra part** only, and is a **2h exam**. The total is 50 points. Your exam grade is 1 plus your total number of points multiplied by $0.18(= 9/50)$, rounded to one digit, that is:

$$1 + \frac{9P}{50}.$$

Algebra

1. (7 points) Investigate whether or not $U(20)$ and $U(30)$ are isomorphic.

2. Let the ring R be given by
$$\{a + b\sqrt{6} \mid a, b \in \mathbb{Z}_7\}$$
   (a) (4 points) Prove that R has no zero divisors.
   (b) (3 points) Argue that R is a field.
   (c) (3 points) Calculate $(1 + \sqrt{6})^{-1}$.

3. We want to paint the edges of an equilateral triangle made of copper wire using red, yellow and blue. We want to use Burnside's theorem to determine the number of different colorings. Each coloring should contain at least two different colors.
   (a) (3 points) What, in the terminology of Burnside's theorem, is the set S and what is the group of permutations G acting on S.
   (b) (3 points) Determine the number of orbits in S under G.
   (c) (4 points) Determine for each element in S the corresponding orbit.
   (d) (2 points) How can you check the consistency of your answers to 3a, 3b and 3c?

4. Consider $p_1(x), p_2(x) \in \mathbb{Z}_2[x]$ defined by $p_1(x) = x^3 + x + 1$, $p_2(x) = x^3 + x^2 + 1$. and let $\mathbb{F}_i$ be defined as
$$\mathbb{F}_i = \mathbb{Z}_2[x]/ < p_i(x) >, \quad i = 1, 2.$$
   (a) (3 points) Argue that $\mathbb{F}_i$ are fields.
   (b) (3 points) Describe the elements of $\mathbb{F}_i$.
   (c) (2 points) How many elements do $\mathbb{F}_i$ have.
   (d) (3 points) Prove that the multiplicative groups $\mathbb{F}_i^* = \mathbb{F}_i \setminus \{0\}$ are isomorphic.

PTO

5. (a) (8 points) Consider the RSA method, and assume that Alice has published the modulus $n = 143$ and the exponent $e = 7$. Bob emails the cipher text $C = 4$ to Alice. Compute everything that an eavesdropper Eve needs to break Alice's code in order to reconstruct Bob's original message M. Also compute M.

   (Hints for calculus: $16^2 = 113$ (mod 143), $113^2 = 42$ (mod 143), $42^2 = 48$ (mod 143), and $48^2 = 16$ (mod 143).)

   (b) (2 points) Prove by making use of a theorem and without using modular exponentiation, that

$$25^{29} = 25 \text{ (mod } 29)$$