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

Exam 3, Module 7, Codes 201400483 & 201800141

Discrete Structures & Efficient Algorithms

Friday, April 5, 2019, 13:45 - 15:45

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

There are FIVE exercises.

This third exam of Module 7 consists of the **Algebra part** only, and is a **2h exam**. The total is 50 points. The grade is:

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

Algebra

1. (a) (5 points) Compute the order of each element in $U(18)$.

   (b) (4 points) Prove that $U(18)$ is isomorphic to $U(14)$.

2. (a) (4 points) Prove that the ring R defined by

$$R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

   is an integral domain.

   (b) (3 points) Is the ring S defined by

$$S = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

   an integral domain?

   (c) (2 points) Is the ring T defined by

$$T = \{a + b\sqrt{2} \mid a, b \in \mathbb{R}\}$$

   an integral domain?

3. We want to paint the edges of a square made of iron wire using red and blue. We want to use Burnside's theorem to determine the number of different colorings.

   (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) (4 points) Determine the number of orbits in S under G.

   (c) (4 points) Determine for each element in S the corresponding orbit.

4. Consider $p(x) \in \mathbb{Z}_3[x]$ defined by $p(x) = x^2 + 1$ and let $\mathbb{F}$ be defined as

$$\mathbb{F} = \mathbb{Z}_3[x] / < p(x) > .$$

   (a) (3 points) Argue that $\mathbb{F}$ is a field.

PTO

(b) (3 points) Describe the elements of $\mathbb{F}$.

(c) (2 points) How many elements does $\mathbb{F}$ have.

(d) (3 points) Prove that the multiplicative group $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is cyclic.

5. (a) (8 points) Consider the RSA method, and assume that Alice has published the modulus $n = 65$ and the exponent $e = 11$. Bob emails the cipher text $C = 2$ 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.

   (b) (2 points) By making use of a well-known theorem, show that $15^{17} = 15 \pmod{17}$, without actually doing much of calculations.