Exam 2. juni 2015 **IR201712 Diskret Matematikk**
Duration 4 hours *English*

Calculators and other accessories are not permitted. Include **all intermediate calculations** necessary to justify your answer.

The English text is provided as an extra help, to aid with any problems with terminology. The Norwegian text remains the sole official version.

Problem 1 .... *(4%)*

(a) Calculate $\binom{6}{4}$.

(b) Calculate $\binom{640}{639}$.

Problem 2 .... *(7%)*

Calculate the following

(a) $(5+8) \mod 9 =$

(b) $(9 \cdot 6 + 3) \mod 19 =$

(c) $(x^2 + x + 1) \cdot (x + 1)$ over $\mathbb{Z}_2$.

Problem 3 .... *(5%)*

Solve the following congruences (modular equations)

(a) $2x \equiv 1 \pmod 3$

(b) $3x + 2 \equiv 1 \pmod 5$

Problem 4 .... *(4%)*

(a) Write the hexadecimal number 2C in decimal form.

(b) Write 20 (decimal) in hexadecimal form.

Problem 5 .... *(12%)*

Consider a computer system with usernames and passwords. Explain how to find the number of unique, possible passwords when

(a) ... the password consists of exactly six lower-case, Norwegian letters?

(b) ... the password consists of six to eight lower-case, Norwegian letters?

(c) ... the password consists of six to eight charachter where *the first one* is an upper-case Norwegian letter and the remainder can be either upper- or lower-case Norwegian letters?

It is sufficient to give formulæ and insert numbers. You **do not have to** complete the calculations. Explain what counting principles you use, and how you arrive at the answers.

Problem 6 .... *(6%)*

This problem considers logical arguments.

(a) Consider the two statements

1. Dersom det regnar, tek eg på regnjakke.
2. Det regnar.

What conclusion can you make using a direct proof (Modus Ponens)?

(b) Consider the argument

1. $s \Rightarrow t$
2. ??

$\therefore \neg s$

What statement must be insterted for the question marks to make a valid argument (Modus Tollens)? (The $\therefore$ symbol can be read as 'therefore' or as 'thus we can conclude that')

Problem 7 .... *(5%)*

Explain what we mean by a zero divisor, and list the zero divisors of $\mathbb{Z}_{12}$.

Problem 8 .... *(4%)*

Encrypt the message «godmorgen» with Cæsar's cipher. Show the details of the encryption using modular arithmetics over integers.

Problem 9 . . . . *(8%)*

(a) Let A and B be matrices over $\mathbb{Z}_2$:

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Calculate $A \cdot B =$

(b) Let C and D be matrices over $\mathbb{Z}_5$:

$$C = \begin{bmatrix} 1 & 2 \\ 0 & 3 \\ 0 & 4 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 4 \\ 3 & 2 \end{bmatrix}$$

Calculate $C \cdot D =$.

Problem 10 . . . . *(12%)*

Consider the relation $<$ (less than)

(a) What do we mean by a relation (in general)?

Answer the following three questions and give reasons for each answer:

(b) Is $<$ symmetric?

(c) Is $<$ reflexive?

(d) Is $<$ transitive?

Problem 11 . . . . *(12%)*

(a) Show step by step how to use the Euclidean algorithm to find $\text{hcf}(413, 273)$[1]?

(b) Show how to use the Extended Euclidean Algorithm to find the multiplicative inverse of 11 modulo 91.

(c) Given $\text{hcf}(a, b)$, how do we know whether a has a multiplicative inverse modulo b?

Problem 12 . . . . *(16%)*

RSA has the encryption function $e_{e,n}(x) = x^e \mod n$.

(a) Show step by step how to calculate $16^{14} \mod 21$ efficiently.

(b) Write pseudo code for an efficient algorithm to calculate $x^e \mod n$.

(c) Prove that the algorithm from (b) terminates in finite time.

(d) In the encryption function above, (e, n) is the public key. Explain how the secret (private) key is defined or how it is computed.

Problem 13 . . . . *(5%)*

Consider the recurrence

$$T(n) = 2 \cdot T(n-1) + 1,$$
$$T(0) = 1.$$

Use mathematical induction to prove that $T(n) = 2^{n+1} - 1$ for all $n \geq 0$.

[1] hcf stands for *Highest Common Factor*, also known as *greatest common divisor* (gcd).