Exam 1. desember 2015
Duration 4 hours

IR201712 Diskret Matematikk
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 $\binom{5}{3}$.

(b) Calculate $\binom{777}{776}$.

Problem 2 . . . . *(4%)*

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

(b) Write 63 (decimal) in hexadecimal form.

Problem 3 . . . . *(4%)*

Calculate the following

(a) $(17 + 12) \mod 9 =$

(b) $(4 \cdot 12 + 3) \mod 16 =$

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

Let $a \oplus b$ denote XOR of a and b. Use a truth table to show that $a \oplus b$ is equivalent to $(a \wedge \neg b) \vee (\neg a \wedge b)$. (Remember that $a \oplus b$ is false when a and b have the same truth value and true when a and b have different truth values.)

Problem 5 . . . . *(4%)*

Solve the following congruences (modular equations)

(a) $3x \equiv 2 \pmod 5$

(b) $4x - 2 \equiv 4 \pmod 9$

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

A poker hand is five random cards from a standard 52-card deck.

(a) How many distinct poker hands exist?

(b) How many distinct poker hands include four of a kind? (There are thirteen kinds: $2, 3, \ldots, 10$ samt Knave, Queen, King, Ace. The fifth card can be anything.)

Problem 7 .... *(8%)*

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

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

Calculate $A \cdot B =$

(b) Let C and D be matrices over $\mathbb{Z}_7$:

$$C = \begin{bmatrix} 1 & 2 \\ 3 & 3 \\ 0 & 2 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 5 \\ 6 & 2 \end{bmatrix}$$

Calculate $C \cdot D =$

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

Let s and t be two statements. Consider the following three arguments:

a)
$$\begin{array}{c} s \Rightarrow t \\ t \\ \hline \therefore s \\ \hline \end{array}$$

b)
$$\begin{array}{c} s \Rightarrow t \\ s \\ \hline \therefore t \\ \hline \end{array}$$

c)
$$\begin{array}{c} s \Rightarrow t \\ \neg t \\ \hline \therefore \neg s \\ \hline \end{array}$$

For each of the three arguments, decide whether it is valid or not.

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

Consider the following statement from NRK's web pages:

Må legge ned Aukrustsenteret hvis Caprino vinner rettsaken

Let's call this statement u.

(a) Define to statements, s og t, such that the statement u can be written as $u = (s \Rightarrow t)$.

(b) Write the contrapositive statement of u on symbolic form (as an expression in s and t).

(c) Write the contrapositive statement of u in natural language.

Problem 10 .... *(15%)*

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

(a) Explain what we mean when we say that RSA is an asymmetric cipher.

(b) What advantages do asymmetric ciphers have compared to symmetric ciphers?

(c) Give one example of a symmetric cipher in common, contemporary use.

(d) What advantages do symmetric ciphers have compared to public keys?

(e) How are practical systems (e.g. SSL) designed to get the best out of symmetric and asymmetric ciphers?

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

This problem considers relations between two sets.

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

(b) An equivalence is a relation which satisfies three particular properties. Name and define each of these three properties.

(c) Recall that we write $x \equiv y \pmod{n}$ if $x \mod n = y \mod n$. This is a relation which we call congruence modulo n. Is congruence modulo n an equivalence? Give reasons for your answer.

Problem 12 .... *(4%)*

Encrypt the message «godaften» with a transposition cipher. The key is the permutation $(4, 2, 1, 3)$.

Problem 13 .... *(6%)*

We are going to assess the running time of four different sorting algorithms when sorting very large arrays.Let n be the number of elements to be sorted. The following table shows how many times each algorithms has to swap to elements in the worst case, and this is expected to be the most time consuming operation.

Algoritme 1	$\frac{n(n-1)}{2}$
Algoritme 2	n^2
Algoritme 3	$n(1 + \log n)$
Algoritme 4	$2^n - n^{20} + n^{10}$

(a) Give a Big-Θ expression (best possible Big-O expression) for the number of swaps needed by each algorithm. Make the expression as simple as possible.

(b) Sort the four algorithms from fastest to slowest based on the running time for large arrays (when n tends to infinity). Indicate any ties in the list.

Problem 14 .... *(8%)*

(a) Show step by step how to use the Euclidean algorithm to find $\text{hcf}(525, 1295)$[1]?

(b) Show how to use the Extended Euclidean Algorithm to find the multiplicative inverse of 13 modulo 81.

Problem 15 .... *(8%)*

Consider two polynomials over $\mathbb{Z}_2$:

$$f(x) = x^4 + x^3 + x^2 + 1,$$
$$g(x) = x^3 + 1.$$

Calculate the following

(a) $f(x) \mod g(x) =$

(b) $\text{hcf}(f(x), g(x)) =$

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