Exam 6. desember 2013
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 ..... *(7%)*

Write F and T for *true* and *false* respectively.

(a) Simplify the expression $s \wedge \neg s =$

(b) Simplify the expression $s \vee T =$

(c) 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 2 ..... *(12%)*

Consider each of the following arguments. Define predicate symbols and phrase the argument systematically on symbolic form. Decide whether the argument is valid and if it is, what argument technique is used.

(a)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Jula vert kvit og fin.
- Ergo er eg opplagd og inspirert når neste semester startar.

(b)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Det regnar heile jula.
- Ergo er eg sur og gretten når neste semester startar.

(c)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Eg er sur og gretten når neste semester startar.
- Ergo hadde me ikkje snø i jula.

Problem 3 ..... *(7%)*

Calculate the following

(a) $6 + 7 \mod 9 =$

(b) $4 \cdot 7 \mod 17 =$

(c) $(x^3 + x + 2) \cdot (x^4 + 2x^3 + 1)$ over $\mathbb{Z}_3$.

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

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

(a) ... the username consists of exactly six characters which are either lower-case, English letters or digits?

(b) ... the username consists of six to eight characters, which are either lower-case, English letters or digits?

(c) ... the username consists of six to eight characters where *the first one* is a lower-case English letter and the remainder can be either lower-case, English letters, digits, or one of the ten characters `.,-+:;_%$"`?

It is sufficient to give formulas 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 5 ..... *(8%)*

(a) Calculate $A \cdot B$ over $\mathbb{Z}_2$ where:

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

(b) Calculate $C \cdot D$ over $\mathbb{Z}_3$ where:

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

Problem 6 ..... *(4%)*

Let E be a matrix over $\mathbb{Z}_2$:

$$E = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{1}$$

Calculate E^{-1}.

Problem 7 ..... *(12%)*

(a) Give the formula (definition) for the binomial coefficient $\binom{n}{m}$

(b) Calculate $\binom{7}{3}$

(c) Explain how to construct a proof by mathematical induction.

(d) Use mathematical induction to prove the formula you found i part a. You can use the following well-known equation:

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}, \quad \text{when } n > m. \tag{2}$$

Problem 8 ..... *(6%)*

How many solutions with $0 \leq x \leq 14$ exist for the following equations:

(a) $3x \mod 15 = 3$?

(b) $3x \mod 15 = 1$?

Give reasons for your answer.

Problem 9 ..... *(10%)*

(a) Show how to use the Euclidean algorithm to find hcf$(90, 462)$[1]?

(b) Show how to use the Extended Euclidean Algorithm to find the multiplicative inverse of 13 modulo 73.

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

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

(a) Show step by step how to calculate $11^{17} \mod 21$ efficiently.

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

(c) How many multiplications are required to calculate $x^e \mod n$?

Problem 11 ..... *(10%)*

Consider the following recurrence, assuming that n is a power of two,

$$\begin{aligned} T(n) &= 2(T(n/2)) + n, \quad \text{when } n > 1, \\ T(1) &= 1. \end{aligned} \tag{3}$$

(a) Draw a recurrence tree for $T(n)$.

(b) Use the recurrence tree to find an exact solution for $T(n)$.

(c) Give a Big-Θ (best possible Big-O) bound on $T(n)$.

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