Exam 2. desember 2014 **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 $\binom{5}{3}$.

(b) Calculate $\binom{520}{519}$.

Problem 2 .... *(6%)*

Write F and T for *True* and *False* respectively.

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

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

(c) Write down a truth table for the expression $p \Rightarrow q$.

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

Calculate the following

(a) $12 + 3 \mod 13$

(b) $6 \cdot 5 \mod 10$

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

Solve the following congruences (modular equations)

(a) $2x \equiv 1 \pmod 5$

(b) $4x + 2 \equiv 1 \pmod 9$

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

Class 5A have to elect student representatives. There are twelve girls and seven boys in the class. Answer the following, and explain what counting principles you use for each question.

(a) In how many ways can they elect one representative of each gender?

(b) In how many ways can they elect one representative and one deputy?

(c) In how many ways can they elect one representative and one deputy, where the two of them have different gender?

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

(a) Write the hexadecimal number 1E in decimal form.

(b) Write 33 (decimal) in hexadecimal form.

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

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

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \tag{11}$$

Calculate $A \cdot B =$

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

$$C = \begin{bmatrix} 1 & 1 \\ 6 & 1 \\ 2 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 3 & 2 \\ 3 & 0 \end{bmatrix} \tag{13}$$

Calculate $C \cdot D =$.

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

Consider the statement

if m is odd, then m^2 is odd

(a) Formalise the statement using logical symbols.

(b) Prove the statement.

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

Consider equivalence relations.

(a) What do we mean by a relation?

(b) What does it mean when we say that relation is an equivalence (relation)?

(c) Show that $a \equiv b \pmod{n}$ is an equivalence. (Remember that $a \equiv b \pmod{n}$ means the same as $a \mod n = b \mod n$.)

Problem 10 .... *(3%)*

List the zero divisors of $\mathbb{Z}_{15}$.

Problem 11 .... *(16%)*

(a) Show step by step how to use the Euclidean algorithm to find $\text{hcf}(365, 189)$[1]?

(b) Show how to use the Extended Euclidean Algorithm to find the multiplicative inverse of 15 modulo 83.

(c) Give pseudo code for the Euclidean algorithm.

(d) Explain how we can guarantee that the Euclidean algorithm completes in finite time.

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

(a) Explain what we mean by a public key cipher (asymmetric cipher).

(b) Give one example of a public key cipher in common, contemporary use.

(c) What advantages do public key ciphers have compared to symmetric ciphers?

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

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

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

Problem 13 .... *(9%)*

Consider the expression $3^{69} \mod 19$.

1. Show how you can use Fermat's little theorem to simplify the expression.
2. Explain what other arithmetic rules you can use to calculate such expressions ($x^y \mod n$) as easily as possible.
3. Calculate $3^{69} \mod 19$. Show how you make the computation.

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