(1) Find a big \( O \)-estimate for the following functions
   (a) \( 5n^2 \log(n!) + (3n^3 + 5n + 1) \log n \);
   (b) \( n^2 \log(4n^2 + 2) + 3n^2 \);
   (c) \( n^2 \log(4n^2 + 2) + 3n^3 \);

(2) Find a big \( O \)-estimate for the number of operations (ignoring any counter arithmetic) in the following algorithms

Procedure 1 \textit{myfirstprogram} \((n : \text{integer})\)

\[
\begin{align*}
t &:= 0 \\
\text{for} \ i := 1 \ \text{to} \ n \\
& \quad \text{for} \ j := 1 \ \text{to} \ 7 \\
& \quad \quad \text{for} \ k = 1 \ \text{to} \ n \\
& \quad \quad \quad t := t + i + j + k^2 \\
\text{return} \ t.
\end{align*}
\]

Procedure 2 \textit{disjoint}(\(a_1, \ldots, a_n, b_1, \ldots, b_n : \text{elements}\))

\[
\begin{align*}
\text{answer} &:= \text{true} \\
\text{for} \ i := 1 \ \text{to} \ n \\
& \quad \text{for} \ j := 1 \ \text{to} \ n \\
& \quad \quad \text{if} \ a_i = b_j, \ \text{then} \ \text{answer} := \text{false} \\
\text{return} \ \text{answer}.
\end{align*}
\]

(3) Give a proof that
   (a) if \( a | b \) and \( b | c \), then \( a | c \);
   (b) if \( a | b \), then \( a^2 | b^2 \).

(4) Calculate the following
   (a) \( 141 \cdot 151 \mod 235 \);
   (b) if \( a \equiv 12 \mod 23 \) and \( b \equiv 7 \mod 23 \), find \((2a + 3b) \mod 23\);
   (c) \( 20124 \mod 4562 \) (show the intermediate calculations)

(5) Find the expansion in the given base
   (a) 130 in binary;
   (b) 2024 in ternary;
   (c) 2024 in hexadecimal.

(6) Find the decimal expansion of the following numbers
   (a) \( (1001001)_{2} \);
   (b) \( (AB01)_{16} \);
   (c) \( (432)_{5} \).

(7) Use the modular exponentiation algorithm to find
   (a) \( 3^{85} \mod 100 \);
   (b) \( 2^{39} \mod 41 \).

(8) Find the greatest common divisor of
   (a) \( 2^{13} \cdot 3^{11} \cdot 11^4 \cdot 17^2 \) and \( 2^{4} \cdot 3^{2} \cdot 5^{11} \cdot 17^2 \).
(b) 1435 and 2010.

(9) Find \( \gcd(70, 336) \) and its “Bézout form”, that is to say, write it as a linear combination of 70 and 336.

(10) Solve the congruence \( 121x \equiv 5 \mod 350 \).

(11) Use the Chinese Remainder Theorem to find a solution to the congruences \( x \equiv 3 \mod 5 \), \( x \equiv 2 \mod 7 \), and \( x \equiv 4 \mod 9 \).

(12) Use Fermat’s Little Theorem and modular exponentiation to find \( 10^{8010} \mod 401 \) (note that 401 is a prime).

(13) Using that 3 is a primitive root modulo 17, find \( \log_3(4) \).

(14) Is 100202345X a valid ISBN number? If not, what would the correct check digit have to be?

(15) Alice wants to communicate with Bob using RSA public key encryption, after he goes on a trip to China. For this she chooses two primes \( p = 41 \) and \( p = 43 \) and multiplies them together to get \( n = 1763 \). What is the decryption key \( d \) she has to give Bob before he leaves if she plans on using the encryption key \( e = 11 \)? When he’s abroad, she wants to send him the number 521 over an insecure channel using her encryption protocol. What will she send him?

(16) Alice and Bob want to create a common secret key using the Diffie-Hellman protocol. In a text message, they agree to use the prime 23 and primitive root 5. Alice selects secretly the exponent 3 and Bob chooses 7. What will they text to each other to figure out the common (secret) key, and what is this common key?