

1. Write 69 (base 10) in base 3.
2. Write 1001101 (base 2) in base 10.
3. Compute the sum $GILACXA + BCADAFH$ in base 26.
4. The following table gives a Boolean function f with 3-bit inputs and 1-bit outputs. Give an explicit formula for f , and simplify as much as possible.

$x_1x_2x_3$	$f(x_1x_2x_3)$
0 0 0	0
0 0 1	1
0 1 0	0
0 1 1	1
1 0 0	1
1 0 1	0
1 1 0	0
1 1 1	0

5. Show that $\mathcal{O}(n!) \subseteq \mathcal{O}(n^n)$.
6. Let $\mu(n) = n^2 + 16n$. Is $\mu(n) \in \mathcal{O}(n^3)$?
7. Show that if $\mu(n) \in \mathcal{O}(f(n))$, then $\mathcal{O}(\mu(n))$ is contained in $\mathcal{O}(f(n))$.
8. A linear feedback shift register uses constants $c_1 = 1$, $c_2 = 0$, $c_3 = 1$, and $c_4 = 0$, and has the output stream start with 0001. Use the output as a binary Vigenère key to decipher the cipher text 101100110110.
9. The plaint text of a binary Vigenère message is 1011011101 and the corresponding cipher text is 1101001100. The key is the output of a 4-bit linear feedback shift register. Determine the constants c_1, c_2, c_3 and c_4 used by the LFSR.
10. Let $f_k(x)$ be a Boolean function defined by

$$f_{k_1k_2}(x_1x_2) = (x_1 + k_1 \cdot x_2 \text{ MOD } 2)(k_2 + x_1 \cdot x_2 \text{ MOD } 2).$$

Suppose the output of the Feistel function $F_{10}(x)$ is 1001. What 4-bit input was x ?

11. A hash function $H(x)$ outputs 80-bit binary strings. Suppose that x_1, x_2, \dots, x_8 are eight distinct inputs chosen at random. Assume that H is constructed so that for inputs chosen at random, each output is equally likely. What is the probability that the hash values $H(x_1), H(x_2), \dots, H(x_8)$ are all different? (Do NOT attempt to simplify your answer.)