

Mathematics of Coding and Cryptography Worksheet 2

1. A number is said to be rational if it is of the form a/b where a and b are integers and $b \neq 0$. The set of rational numbers is denoted \mathbb{Q} . A real number that is not rational is said to be irrational. Prove that $\sqrt{2}$ is irrational. Try to repeat the proof for $\sqrt{4}$. Why does the proof fail in the latter case?
2. McNuggets can be bought in quantities of 6, 9 or 20.
 - (a) It is impossible to buy precisely 43 McNuggets. Why?
 - (b) It is possible to buy precisely 44, 45, 46, 47, 48 or 49 McNuggets. How?
 - (c) Conclude that it is possible to buy precisely any number of McNuggets greater than 43. Why?
 - (d) If we are allowed to sell McNuggets back in quantities of 6, 9 or 20, then we can arrange to end up with any given number of McNuggets. How?
3. Let m , k and n be integers. Suppose $m|n$ and $m|(k+n)$. Prove that $m|k$.
4. Suppose p is an odd prime number. When p is divided by 4 it leaves a remainder of either 1 or 3. (For instance $13 = 3 * 4 + 1$ while $11 = 2 * 4 + 3$). A famous theorem asserts that if p leaves a remainder of 1 when divided by 4 then $p = a^2 + b^2$ for some integers a and b . (For instance, $13 = 3^2 + 2^2$). Verify this for all relevant primes < 100 . Can you prove it?
5. Review questions:
 - (a) Find $\int_0^3 x^3 e^{-x} dx$.
 - (b) Find the characteristic polynomial, eigenvalues and corresponding eigenspaces of the matrix
$$\begin{bmatrix} 4 & 2 & -2 & 2 \\ 1 & 3 & 1 & -1 \\ 0 & 0 & 2 & 0 \\ 1 & 1 & -3 & 5 \end{bmatrix}$$
 - (c) Suppose that \mathbf{A} is a 3×2 matrix and \mathbf{B} is a 2×3 matrix. Prove that $\det(\mathbf{AB}) = 0$. (Hint: try to prove it in the case that \mathbf{A} is a 3×1 matrix and \mathbf{B} is a 1×3 matrix. Generalize.)