Discrete Mathematics - COMP0147

**2025 - Term 1**
**Prof. Elaine Pimentel**

**LIST OF EXERCISES**

PROOF TECHNIQUES, MODULAR ARITHMETIC
(ROSEN - CHAPTERS 1 AND 4)

---

**Required reading for this assignment:** *Discrete Mathematics and Its Applications* (Rosen, $7^{\text{th}}$ Edition):

- Chapter 1.7: *Introduction to Proofs*
- Chapter 4.1: *Divisibility and Modular Arithmetic*
- Chapter 4.3: *Primes and Greatest Common Divisors*

**Note:** The exercises are classified into difficulty levels: easy, medium, and hard. This classification, however, is only indicative. Different people may disagree about the difficulty level of the same exercise. Do not be discouraged if you see a difficult exercise–you may find that it is actually easy, by discovering a simpler way to solve it!

---

1. `[Medium]` (Rosen 1.7.5) Prove that if $m+n$ and $n+p$ are even integers, where $m$, $n$, and $p$ are integers, then $m+p$ is even. What type of proof did you use?
2. `[Medium]` (Rosen 1.7.6) Use a direct proof to show that the product of two odd numbers is odd.
3. `[Medium]` (Rosen 1.7.7) Use a direct proof to show that every odd integer is the difference of two squares.
4. `[Medium]` (Rosen 1.7.8) Prove that if $n$ is a perfect square, then $n+2$ is not a perfect square.
5. `[Medium]` (Rosen 1.7.9) Use a proof by contradiction to show that the sum of an irrational number and a rational number is irrational.
6. `[Easy]` (Rosen 1.7.11) Prove or refute that the product of two irrational numbers is irrational.
7. `[Hard]` (Rosen 1.8.10) Prove that $2 * 10^{500} + 15$ or $2 * 10^{500} + 16$ is not a perfect square. Is your proof constructive or non-constructive?
8. `[Medium]` (Rosen 1.8.12) Show that the product of two of the numbers $65^{1000} - 8^{2001} + 3^{177}$, $79^{1212} - 9^{2399} + 2^{2001}$, and $24^{4493} - 5^{8192} + 7^{1777}$ is non-negative. Is your proof constructive or non-constructive?
9. `[Easy]` (Rosen 1.8.14) Prove or refute that if $a$ and $b$ are rational numbers, then $a^b$ is also rational.
10. `[Easy]` (Rosen 1.8.29) Prove that there is no positive integer $n$ such that $n^2 + n^3 = 100$.
11. `[Medium]` Show that $min(a, b) \leq med(a, b) \leq max(a, b)$.
12. `[Hard]` Prove that between any two rational numbers there exists an infinite number of irrational numbers.
13. `[Easy]` Give an example of a relation that is:
    (a) symmetric, reflexive but not transitive.

(b) reflexive, transitive but not symmetric.

(c) symmetric, transitive but not reflexive.

14. `[Easy]` For $n \in \mathbb{N}, n \geq 1$, define

$$n! = n.(n-1).(n-2).\ldots.2.1$$

$n!$ is called the factorial of $n$. Let $k \in \mathbb{N}, k > 1$. Prove that the numbers

$$k! + 2, k! + 3, \ldots, k! + k$$

are composite. Conclude that no matter how large $m$ is, there always exist $m$ consecutive *composite* numbers.

15. `[Easy]` Find an odd prime factor of $5^{25} - 1$.

16. `[Medium]` Let $n$ be a positive composite integer and $p$ its smallest prime factor. It is known that:

    (a) $p \geq \sqrt{n}$;

    (b) $p - 4$ divides both $6n + 7$ and $3n + 2$.

    Determine all possible values of $n$.

17. `[Easy]` (Rosen 4.1.36) Show that if $a, b, c, m$ are integers with $m \geq 2$, $c > 0$, and

$$a \equiv b \pmod{m},$$

then

$$ac \equiv bc \pmod{mc}.$$

18. `[Medium]` (Rosen 4.1.36) Show that if $n$ is an integer, then

$$n^2 \equiv 0 \text{ or } 1 \pmod{4}.$$

Use this to show that if $m$ is a positive integer of the form $4k+3$ for some nonnegative integer $k$, then $m$ is not the sum of the squares of two integers.

19. `[Medium]` (Rosen 4.3.18) A positive integer is called *perfect* if it equals the sum of its positive divisors other than itself.

    (a) Show that 6 and 28 are perfect.

    (b) Show that $2^{p-1}(2^p - 1)$ is a perfect number when $2^p - 1$ is prime.

20. `[Medium]` (Rosen 4.3.22) The value of the Euler $\phi$-function at a positive integer $n$ is defined to be the number of positive integers less than or equal to $n$ that are relatively prime to $n$. [Note: $\phi$ is the Greek letter phi.]

    Show that $n$ is prime if and only if $\phi(n) = n - 1$.