The Euclidean Algorithm: From Integers to Polynomials

Name: _____ Date: _____

1 Introduction

The Euclidean algorithm, dating back to ancient Greece (around 300 BCE), is one of the oldest and most elegant algorithms in mathematics. Named after the mathematician Euclid, this algorithm provides an efficient method for finding the greatest common divisor (GCD) of two integers.

What makes this algorithm truly remarkable is its universality—the same fundamental principles that work for integers can be extended to polynomials, allowing us to find the greatest common divisor of polynomial expressions. This connection demonstrates the beautiful unity of mathematical structures across different domains.

2 The Euclidean Algorithm for Integers

2.1 Essential Definitions

Before diving into the algorithm, let's establish our foundational concepts:

Definition (Divisibility): For integers a and b with $b \neq 0$, we say that b **divides** a (written $b \mid a$) if there exists an integer k such that $a = bk$.

Example: $3 \mid 12$ because $12 = 3 \cdot 4$.

Definition (Greatest Common Divisor): The **greatest common divisor** of two integers a and b (not both zero), denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b.

Example: $\gcd(12, 18) = 6$ because 6 is the largest integer that divides both 12 and 18.

Definition (Division Algorithm): For any integers a and b with $b > 0$, there exist unique integers q (quotient) and r (remainder) such that:

$$a = bq + r \quad \text{where } 0 \leq r < b$$

This is the foundation of "long division" and is crucial for understanding the Euclidean algorithm.

2.2 The Euclidean Algorithm Procedure

The Euclidean algorithm repeatedly applies the division algorithm:

Algorithm: To find $\gcd(a, b)$ where $a \geq b > 0$:

1. Apply the division algorithm: $a = bq_1 + r_1$ where $0 \leq r_1 < b$

2. If $r_1 = 0$, then $\gcd(a, b) = b$
3. Otherwise, apply the division algorithm to b and r_1: $b = r_1 q_2 + r_2$ where $0 \leq r_2 < r_1$
4. Continue this process until the remainder is 0
5. The last non-zero remainder is $\gcd(a, b)$

2.3 Example: Finding $\gcd(252, 105)$

Let's trace through the algorithm step by step:

$$252 = 105 \cdot 2 + 42 \tag{1}$$
$$105 = 42 \cdot 2 + 21 \tag{2}$$
$$42 = 21 \cdot 2 + 0 \tag{3}$$

Since the remainder is now 0, we have $\gcd(252, 105) = 21$.
Verification: $252 = 21 \cdot 12$ and $105 = 21 \cdot 5$, and $\gcd(12, 5) = 1$, confirming our answer.

2.4 Key Properties

Property 1: $\gcd(a, b) = \gcd(b, a \bmod b)$
This is why the algorithm works—the GCD doesn't change as we perform the division steps.

Property 2 (Bézout's Identity): For any integers a and b, there exist integers x and y such that:

$$\gcd(a, b) = ax + by$$

The Euclidean algorithm can be extended (called the Extended Euclidean Algorithm) to find these coefficients.

3 The Euclidean Algorithm for Polynomials

3.1 Polynomial Division Algorithm

Just as integers have a division algorithm, so do polynomials:

Polynomial Division Algorithm: For polynomials $f(x)$ and $g(x)$ with $g(x) \neq 0$, there exist unique polynomials $q(x)$ (quotient) and $r(x)$ (remainder) such that:

$$f(x) = g(x) \cdot q(x) + r(x)$$

where either $r(x) = 0$ or $\deg(r) < \deg(g)$.

Note: This is exactly polynomial long division that you've learned before!

3.2 Greatest Common Divisor of Polynomials

Definition: The **greatest common divisor** of two polynomials $f(x)$ and $g(x)$ (not both zero) is the monic polynomial of highest degree that divides both $f(x)$ and $g(x)$.

Note: We choose the monic polynomial (leading coefficient = 1) to ensure uniqueness.

3.3 Euclidean Algorithm for Polynomials

The algorithm is identical to the integer case:

Algorithm: To find $\gcd(f(x), g(x))$ where $\deg(f) \geq \deg(g)$ and $g(x) \neq 0$:

1. Divide $f(x)$ by $g(x)$: $f(x) = g(x) \cdot q_1(x) + r_1(x)$ where $\deg(r_1) < \deg(g)$ or $r_1 = 0$
2. If $r_1(x) = 0$, then $\gcd(f(x), g(x)) = g(x)$ (made monic)
3. Otherwise, divide $g(x)$ by $r_1(x)$: $g(x) = r_1(x) \cdot q_2(x) + r_2(x)$
4. Continue until the remainder is 0
5. The last non-zero remainder (made monic) is $\gcd(f(x), g(x))$

3.4 Example: Finding $\gcd(x^4 - 1, x^3 - 1)$

Step 1: Divide $x^4 - 1$ by $x^3 - 1$

$$x^4 - 1 = (x^3 - 1) \cdot x + (x - 1)$$

Step 2: Divide $x^3 - 1$ by $x - 1$

$$x^3 - 1 = (x - 1) \cdot (x^2 + x + 1) + 0$$

Since the remainder is 0, we have $\gcd(x^4 - 1, x^3 - 1) = x - 1$.

Verification: $x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1)$ and $x^3 - 1 = (x - 1)(x^2 + x + 1)$.

4 Practice Problems

Part A: Euclidean Algorithm for Integers

1. Use the Euclidean algorithm to find the following greatest common divisors:

(a) $\gcd(84, 36)$

(b) $\gcd(123, 45)$

(c) $\gcd(1001, 143)$

2. For the calculation $\gcd(84, 36)$ from problem 1(a), verify your answer by factoring both numbers into their prime factorizations and finding the GCD using the prime factorization method.

3. Use the Extended Euclidean Algorithm to find integers x and y such that $\gcd(123, 45) = 123x + 45y$.

Hint: Work backwards through your calculation from problem 1(b).

Part B: Polynomial Division Review

4. Perform the following polynomial divisions and express in the form $f(x) = g(x) \cdot q(x) + r(x)$:

(a) Divide $x^3 + 2x^2 - x + 3$ by $x^2 + 1$

(b) Divide $2x^4 - x^3 + 3x - 5$ by $x^2 - 2x + 1$

Part C: Euclidean Algorithm for Polynomials

5. Use the Euclidean algorithm to find the greatest common divisor of the following polynomial pairs:

(a) $\gcd(x^3 + x^2 - x - 1, x^2 + 2x + 1)$

(b) $\gcd(x^4 + x^3 - 3x^2 - 4x - 1, x^3 + x^2 - x - 1)$

6. Consider the polynomials $f(x) = x^3 - 6x^2 + 11x - 6$ and $g(x) = x^2 - 4x + 3$.

(a) Factor both polynomials completely.

(b) Use the factorizations to find $\gcd(f(x), g(x))$.

(c) Verify your answer by using the Euclidean algorithm.

7. Prove that for polynomials $f(x)$ and $g(x)$ with $g(x) \neq 0$:

$$\gcd(f(x), g(x)) = \gcd(g(x), r(x))$$

where $r(x)$ is the remainder when $f(x)$ is divided by $g(x)$.

This is the fundamental property that makes the Euclidean algorithm work for polynomials.