Polynomial Modular Arithmetic

Notation: We write $\mathbf{R}[x]$ for the set of polynomials with coefficients in the set $\mathbf{R}$, the real numbers.

Definition 1. If $a(x), b(x), m(x)$ are polynomials, we say that $a(x) \equiv b(x) \pmod{m(x)}$ ("are congruent mod $m(x)$") if $m(x)$ divides the polynomial $a(x) - b(x)$.

The polynomial $m(x)$ is called the *modulus*.

Examples:

Verify each of the following congruences.

- $x^2 + 1 \equiv 1 \pmod{x}$
- $x - 7 \equiv 5 \pmod{x}$
- $x^2 + 2x + 1 \equiv 2x + 1 \pmod{x^2}$
- $x^2 \equiv 2 \pmod{2x^2 - 4}$

Exercises

1. Reduce each polynomial to a congruent polynomial of lowest possible degree with respect to the given modulus.

   (a) $2x + 5 \bmod 2$ (b) $x - 2 \bmod x - 1$ (c) $x^3 + x^2 + x + 1 \bmod x^2 - x$ (d) $x^3 + 3x^2 + 1 \bmod x^2 - 7$

2. For each pair of polynomials $a(x), m(x)$ decide if there is an inverse modulo $m(x)$. An inverse is a polynomial $b(x)$ such that $a(x)b(x) \equiv 1 \pmod{m(x)}$.

   (a) $a(x) = x - 2$, $m(x) = x^2 - 4x + 4$ (b) $a(x) = x^2 - 4x + 4$, $m(x) = x - 2$ (c) $a(x) = x^3 - 7x^2 + x - 7$, $m(x) = x^4 - 1$ (d) $a(x) = x^3 - 6x^2 + 11x - 6$, $m(x) = x^4 - 9x^3 + 23x^2 - 15x$ (e) $a(x) = x^3 - 1$, $m(x) = x^4 + x^3 + 2x^2 + x + 1$