Polynomial Congruences

Suppose

\[ f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_sx^s \]

where the \( a_i \)'s are integers, and let \( b \) be an integer. Consider the *polynomial* congruence

(1) \[ f(x) \equiv b \pmod{m}. \]

An integer \( u \) is a *solution* to (1) means \( f(u) \equiv b \pmod{m} \).

Note that if \( u_0 \) is a solution to (1), then so is any \( u \), where \( u \equiv u_0 \pmod{m} \), because \( u \equiv u_0 \pmod{m} \) implies \( f(u) \equiv f(u_0) \pmod{m} \).

By the *number of solutions* to congruence (1) we mean the number of solutions from any complete residue system mod \( m \).

By a *complete set* of solutions to (1) we mean any set \( u_1, u_2, \ldots, u_t \) of solutions such that

(i) \( u_i \not\equiv u_j \pmod{m} \) for \( i \neq j \)

(ii) every solution to (1) is congruent mod \( m \) to one of the \( u_i \).

**Example 1.** \( x^2 + 1 \equiv 0 \pmod{5} \)

\( 2, 3 \) form a complete set of solutions
The number of solutions is 2.

**Example 2.** \( x^2 + 1 \equiv 0 \pmod{p} \), where \( p \) is prime.

See the \( x^2 + 1 \) worksheet.

**Example 3.** Solve \( x^2 \equiv 1 \pmod{8} \). This example shows that a quadratic equation can have more than two roots.

**Example 4.** Solve \( x^3 + x + 2 \equiv 0 \pmod{5} \).

**Example 5.** Solve \( x^5 + x^4 + 1 \equiv 0 \pmod{9} \).

**Example 6.** Solve \( x^2 + 5x + 24 \equiv 0 \pmod{36} \).