Example 1. You've found that 2 is a primitive root of 13. Find all primitive roots.

Solution. Since 2 is a primitive root, all other primitive roots will have the form

These are

A. **Integral Polynomials.** We discuss the existence of primitive roots.

To this end, we work with polynomials.

An **integral polynomial** of **degree** d is a polynomial of form:

$M(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_2 x^2 + a_1 x + a_0$

where the coefficients are:

and the **leading coefficient**:

We call this polynomial **monic** iff the leading coefficient:

In algebra you will have learned long–division of polynomials.

For example, we divide monic polynomials $(x^4 - 3x - 5) \div (x^2 - x + 3)$.

which means:

This models the **Euclidean division algorithm** for monic integral polynomials.

The algorithm states division of monic integral polynomials $M(x) \div D(x)$ yields

As a special case, if c is a fixed integer, then $M(x) \div (x - c)$ yields

B. **Roots.** We discuss roots of polynomials.

Let n be a positive integer and $F(x)$ be an integral polynomial.

A **modulo n root** of $F(x)$ is an an **integer** solution to

For example we locate the roots of $x^2 + 3x + 1$ modulo 5.

$x^2 + 3x + 1 \equiv$

In this case, each root $x = c$ corresponded to a perhaps secret:

Theorem. Let $M(x)$ be a monic integral polynomial and n a positive integer.

Then integer $x = c$ is a modulo n root of $M(x)$ if and only if

for some monic integral polynomial $Q(x)$ such that

Proof. Apply the Euclidean division algorithm to $M(x) \div (x - c)$ to write

Evaluate at $x = c$ to obtain

Hence, $x = c$ is a root modulo n if and only if

which occurs if and only if

□

C. **Lagrange's Theorem.** We attempt to relate degree to the number of roots.

First we consider seemingly out–of–the–ordinary behavior.

Let us find all the roots of $x^2 - 1$ modulo 8.

$x^2 - 1 \equiv 0 \mod 8$

It appears the number of roots can exceed:

This strange behavior will be curbed when the modulus is prime.

Lagrange. Let p be prime $M(x)$ be a monic integral polynomial of degree d.
Then $M(x)$ has

Solution. We use induction on the degree d of the monic integral polynomial.

Base Case. If degree $d = 0$ then, as a monic polynomial of degree zero

Inductive Assumption. Let natural number d be given.

assume $\rightarrow$ degree d monic integral polynomials have:

Inductive Step. Assume monic integral polynomial $M(x)$ has degree $d + 1$.

goal $\rightarrow$

Case 1. If $M(x)$ has zero modulo p roots, then:

Case 2. Otherwise, $M(x)$ has a root, say:

By the theorem from the last page

□