Generalizing the Fundamental Theorem of Algebra: Lagrange’s Theorem

Recall

The Fundamental Theorem of Algebra If \( f(x) \) is a polynomial of degree \( n \) with complex coefficients, then \( f(x) \) has \( n \) complex roots. //

It is most often utilized in this alternate form:

The Fundamental Theorem of Algebra If \( f(x) \) is a polynomial of degree \( n \) with real coefficients, then \( f(x) \) has at most \( n \) real roots. //

Notice that in both cases, we are considering polynomials whose coefficients are drawn from a field (either \( \mathbb{C} \) or \( \mathbb{R} \)). We have seen that \( \mathbb{Z}_p \), the set of congruence classes modulo a prime \( p \), also forms a field. So does the Fundamental Theorem of Algebra hold in this setting?

Example: \( x^2 \equiv 1 \pmod{7} \). We have seen (as a result of Exercise 3.2.6(a)) that this congruence has exactly two solutions, \( x \equiv \pm 1 \pmod{7} \).

Example: \( x^2 \equiv -1 \pmod{7} \). By testing the possibilities \( x \equiv 0, 1, 2, 3, 4, 5, 6 \pmod{7} \), we find that this congruence has no solutions.
Example: $x^2 + 3x + 4 \equiv 0 \pmod{7}$. By Exercise 3.4.10, we note that since $\Delta = 3^2 - 4 \cdot 1 \cdot 4 \equiv 0 \pmod{7}$, the congruence has only one solution, corresponding to the solution of the linear congruence $2 \cdot 1x + 3 \equiv 0 \pmod{7}$. That is, $x \equiv 2 \pmod{7}$.

**Lagrange’s Theorem** If $f(x)$ is a polynomial of degree $n$ with integer coefficients so that at least one coefficient is not divisible by the prime $p$, then $f(x) \equiv 0 \pmod{p}$ has at most $n$ roots modulo $p$.

**Proof** Induction on $n$:

Base case: When $n = 1$, we have a linear congruence of the form $ax \equiv b \pmod{p}$. So either $(a, p) = 1$ and there is one solution to the congruence, or $(a, p) = p$, whence $p \nmid b$, and there are no solutions mod $p$.

Induction step: Assume that the theorem holds for polynomials of degree less than some fixed $n$; suppose that $f(x)$ is a polynomial of degree exactly $n$. If $f(x)$ has no roots mod $p$, then the theorem holds, so we can assume that there is at least one root: $x \equiv a \pmod{p}$. Division of $f(x)$ by $x - a$ produces a quotient polynomial $q(x)$ and a remainder, which must have degree smaller than the divisor, hence is an integer $r$. That is, $f(x) = (x - a) \cdot q(x) + r$. But $f(a) \equiv 0 \pmod{p}$ implies that $r \equiv 0 \pmod{p}$. Therefore, $f(x) \equiv (x - a) \cdot q(x) \pmod{p}$. 
Now if \( x \equiv b \pmod{p} \) is a distinct root of \( f(x) \), then
\[
0 \equiv f(b) \equiv (b - a) \cdot q(b) \pmod{p},
\]
and since \( b \not\equiv a \pmod{p} \), we can cancel the factor \( (b - a) \) above, proving that \( b \) is a root of \( q(x) \) as well. However, \( q(x) \) has degree less than \( n \) and has at least one coefficient not divisible by \( p \) (else all the coefficients of \( f(x) \) are divisible by \( p \)), so the induction hypothesis applies to \( q(x) \), allowing us to conclude that \( q(x) \) has at most \( n - 1 \) roots \( \pmod{p} \). Therefore, \( f(x) \equiv 0 \pmod{p} \) has at most \( n \) distinct roots modulo \( p \). \hfill //

It is significant that Lagrange’s Theorem applies only to prime moduli.

**Example:** \( x^2 \equiv 1 \pmod{8} \) has four solutions \( x \equiv 1, 3, 5, 7 \pmod{8} \).

**Corollary** Suppose \( p \) is a prime and \( n | p - 1 \). Then \( x^n \equiv 1 \pmod{p} \) has exactly \( d \) solutions \( \pmod{p} \).

**Proof** Recall (Exercise 2.1.29) that if \( p - 1 = mn \),
\[
(*) \quad x^{p-1} - 1 = (x^n - 1)(x^{n(m-1)} + x^{n(m-2)} + \cdots + x^n + 1)
\]

Lagrange’s Theorem says that the two polynomial factors on the right have at most \( n \) and at most
At most $n + n(m-1) = p - 1$ roots, while Fermat’s Little Theorem says that the polynomial on the left has exactly $p - 1$ roots mod $p$. Therefore both factors on the right have the maximum number of roots possible. In particular, $x^n - 1$ has $n$ roots mod $p$. //

**Corollary** If $p \equiv 1 \pmod{4}$, then $x^2 \equiv -1 \pmod{p}$ has a solution.

**Proof** Write $p = 4k + 1$. Then $n = 2k | p - 1$, and (*) becomes

$$x^{p-1} - 1 = (x^{2k} - 1)(x^{2k} + 1).$$

By Lagrange’s Theorem, the factors on the right have at most $2k$ roots each while by Fermat’s Little Theorem the polynomial on the left has exactly $4k = p - 1$ roots mod $p$. Thus, since neither of the factors on the right of (**) can have a common root, both have exactly $2k$ roots. In particular, $x^{2k} \equiv -1 \pmod{p}$ has $2k$ roots. If $x \equiv a \pmod{p}$ is one of these, then $(a^k)^2 \equiv -1 \pmod{p}$, whence $x \equiv a^k \pmod{p}$ is a solution to $x^2 \equiv -1 \pmod{p}$. //