Melbourne High School
Maths Extension Group 2023
Term 2 Week 7 Handout Solutioins

Lagrange's Theorem

1. In the proof, we reasoned that this factorisation process eventually results in all the roots; this reasoning assumes that if

$$f(x) \equiv g(x)h(x) \pmod p$$

and $f(r) \equiv 0$ then $g(r) \equiv 0$ or $h(r) \equiv 0$. This is only true when the modulus is prime; the idea is the same as that of Euclid's Lemma. Recall that Euclid's Lemma states if a prime divides a product of two numbers, the prime must divide at least one of the two numbers. In the notation of modular arithmetic, it states that if $ab \equiv 0 \pmod p$ then $a \equiv 0$ or $b \equiv 0$. Note that this is not true when the modulus is composite. A simple example: 6 divides $12 = 3 \times 4$, but it divides neither 3 nor 4. So if the modulus was not prime in our proof of Lagrange's Theorem, at the point where we have

$$f(x) \equiv (x - r)g(x) \pmod p,$$

if p was a composite number, there might be a root of f that is neither a root of $x - r$ or $g(x)$, which means we have failed to count it.

When the modulus is prime, it is guaranteed that any further root of f that is not r is a root of g, and hence the factorisation argument correctly leads to a maximum of d roots.

2. Since $x \equiv r_1$ is a root, write

$$f(x) \equiv (x - r_1)g(x) \pmod p$$

where $g(x)$ is some polynomial of degree $d - 1$. Since all of the roots $r_1, r_2, \dots, r_{d+1}$ are distinct, all of $r_2, \dots, r_{d+1}$ must be roots of g (here is where we use the assumption that p is prime). This is a contradiction because it means that g) has d roots but its degree is $d - 1$, and we have assumed that f is the polynomial with smallest degree that has more roots that its degree. This contradiction completes the proof.

3. (a) Since $p - 1 = dd'$ we have

$$x^{p-1} - 1 = x^{dd'} - 1 = y^{d'} - 1.$$

It is handy to know that a polynomial of this form, $y^{d'} - 1$, can be factorised as

$$y^{d'} - 1 = (y - 1)(y^{d'-1} + y^{d'-2} + \cdots + 1).$$

The factorisation follows at once from the geometric series formula

$$1 + a + a^2 + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}$$

by multiplying both sides by $a - 1$.

(b) The degree of $y - 1 = x^d - 1$ is d, and the degree of $x^{p-1} - 1$ is $p - 1$, so the degree we're looking for is $p - 1 - d$.

(c) Let
$$f(x) = y^{d'-1} + y^{d'-2} + \cdots + 1.$$
By Lagrange's Theorem, $x^d - 1 \equiv 0$ has at most d solutions while f has at most $p-1-d$ solutions. Since $x^{p-1} - 1 \equiv 0$ has exactly $p-1$ solutions, $x^d - 1$ must have at least $p - 1 - (p - 1 - d) = d$ solutions. Hence
$$x^d - 1 \equiv 0 \pmod{p}$$
must have exactly d solutions.