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

> *Angling may be said to be so like the mathematics that it can never be fully learnt.*
>
> —Izaak Walton, *The Complete Angler* (1653)

## The Art of Angling

1. In $\triangle ABC$, $AB = AC$ and $\angle A = 40^\circ$. The bisector from $\angle B$ intersects $AC$ at point $D$. What is $\angle BDC$?

2. Let $ABCD$ be a square with side length 24. Let $P$ be a point on side $AB$ with $AP = 8$, and let $AC$ and $DP$ intersect at $Q$. Determine the area of triangle $CQD$ — AIMO 2019/3

3. Let $ABC$ be a triangle and $D$ be a point on $\overline{BC}$ so that $\overline{AD}$ is the internal angle bisector of $\angle BAC$. Show that — Angle Bisector theorem

$$\frac{AB}{AC} = \frac{DB}{DC}.$$

4. In $\triangle ABC$ let $I$ be the center of the inscribed circle, and let the bisector of $\angle ACB$ intersect $AB$ at $L$. The line through $C$ and $L$ intersects the circumscribed circle of $\triangle ABC$ at the two points $C$ and $D$. If $LI = 2$ and $LD = 3$, then find $IC$. — AIME 2016/6

5. Let $ABC$ be an acute triangle inscribed in circle $\Omega$. Let $X$ be the midpoint of the arc $\widehat{BC}$ not containing $A$ and define $Y$, $Z$ similarly. Show that the orthocenter of $XYZ$ is the incenter $I$ of $ABC$.

*The great masters of modern analysis are Lagrange, Laplace, and Gauss…*

—W. W. R. Ball, *A Short Account of the History of Mathematics* (1888)

**Lagrange's Theorem**

Linear congruences share many properties with linear equations; what about polynomials in general?

Consider the polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where all of $a_0, a_1, \ldots, a_n$ are integers. The Fundamental Theorem of Algebra asserts that $f$ has exactly $n$ complex roots (as long as the polynomial is not constant, of course). But if we consider the congruence

$$f(x) \equiv 0 \pmod{m}$$

for some modulus $m$, does the same theorem hold? That is, does $f$ have $n$ incongruent roots modulo $m$?

It is $n$ complex roots counted with multiplicities, which means repeated roots are counted separately. For example, the polynomial $(x-1)^2$ has only one distinct root, but two roots counted with multiplicities.

Simple experimeintation precludes the idea. For example, it is easy to show that the congruence

$$x^4 - 2 \equiv 0 \pmod{16}$$

has no solution. Run $x$ through a complete set of residues, say $0, 1, \ldots, 15$, and if there are any solutions this finite process would find it. In fact, the same brute-force method works for finding solutions to any polynomial congruence; and therein lies one of the beauties of modular arithmetic. A second example: by running $x$ through the values $0, 1, \ldots, 7$ we find that the congruence

$$x^2 - 1 \equiv 0 \pmod{8}$$

has four solutions, namely $x \equiv 1, 3, 5, 7$. In this case the number of solutions is greater than the degree of the congruence, but in the first example the number of solutions is less than the degree of the congruence. Clearly something different is at play here.

Mathematicians are not easily discouraged, and we are no exception. Instead of considering all moduli, consider congruences to prime moduli only; we hope that this heuristic, a familiar one in number theory, leads to progress. And indeed it does—after similar experimentations to the ones we did above, we notice that sometimes the number of roots is less than the degree of the congruence, sometimes it is equal to the degree, but it is never greater than the degree. This apparently weaker analogue of the Fundamental Theorem of Algebra is known as *Lagrange's Theorem*.

Guess who was the first to prove the Fundamental Theorem of Algebra?

More concretely, Lagrange's Theorem states that the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most $\deg f$ incongruent solutions. From here on, we make one further restriction on the coefficients of $f$; we have already stated they must be integers, but when considering $f$ to a prime modulus, the leading coefficient must not be a multiple of $p$, or else it would vanish. Such an inconvenience does not exist in normal polynomial equations.

Our proof consists of two parts; first we show that if $f$ has a root, then $f$ can be factorised into a linear factor and a polynomial of degree

$\deg f - 1$. The second part is to show that repeating this process leads us to either exactly $\deg f$ or fewer roots; in either case the number roots does not exceed the degree. To ease the notation, let $d = \deg f$.

We begin by assuming that $f$ has a root, for otherwise our proof is already complete; 0 is definitely less than or equal to $d$. Let this root be $x \equiv r$. Hence

$$f(r) \equiv 0 \pmod{p}$$

and so

$$f(x) \equiv f(x) - f(r) \pmod{p}.$$

Expanding the RHS, we have

$$f(x) - f(r) = \sum_{k=0}^{d} a_k x^k - \sum_{k=0}^{d} a_k r^k.$$

These summation signs look scary, but they really aren't. They are just a compact way of expressing the general form of polynomials, which is written in expanded form on the previous page.

The only difference between $f(x)$ and $f(r)$ is that $x$ is replaced by $r$; the coefficients remain the same. Therefore we can group the terms with the same power together and factorise out the coefficients, leaving us with

$$f(x) - f(r) = \sum_{k=0}^{d} a_k (x^k - r^k).$$

More explicity, we can write the expression as

$$f(x) - f(r) = a_d(x^d - r^d) + a_{d-1}(x^{d-1} - r^{d-1}) + \cdots + a_1(x - r). \quad (1)$$

(The constant terms simply vanish.) From here, we note that $(x - r)$ is a factor of the polynomial $x^k - r^k$ for $k > 0$. So we pull out a factor of $(x - r)$ from each of the terms in the above expansion of $f(x) - f(r)$ to obtain

$$f(x) - f(r) = (x - r)(b_{d-1}x^{d-1} + b_{d-2}x^{d-2} + \cdots + b_1 x + b_0)$$

where all of $b_0, b_1, \ldots, b_{d-1}$ are integers that depend on $a_0, a_1, \ldots, a_d$. It doesn't matter what the coefficients of the factored polynomial actually are; the only thing that matters is that it must have degree of $d - 1$, because when we pulled out a factor of $(x - r)$ from each of the terms of Equation (1) the highest power of $x$ that remained was $x^{d-1}$.

Therefore, we have shown that

$$f(x) - f(r) = (x - r)g(x),$$

where $g$ is a polynomial of degree $d - 1$. But recall that $f(x) \equiv f(x) - f(r)$, and so we actually have

$$f(x) \equiv (x - r)g(x) \pmod{p}.$$

The first part of our plan is complete. Now the game is just to repeat the process, because any root of $g$ is also a root of $f$. If $g(x)$ has no roots modulo $p$, we are done; otherwise we apply exactly the same reasoning to factor $g(x)$ as a product of a linear factor and another polynomial with degree of $\deg g - 1$. The degree of the original polynomial $f$ is $d$, and so we can play the game a maximum of $d$ times. If we encounter a polynomial that has no roots before we completely factorise $f$ as a product of linear factors, then $f$ itself has fewer than $d$ roots. If $f$ can be factorised all the way, it has exactly $d$ roots. In either case the number of roots cannot exceed $d$. This completes the proof of Lagrange's Theorem.

A more succint way of saying it is that each time we find a root of $f$ modulo $p$, we can pull out another linear factor. But we can only pull out a linear factor a maximum of $d$ times; hence there cannot be more than $d$ roots modulo $p$.

The discerning reader notices a glaring hole in our proof: we have not used the assumption that $p$ is prime! In fact, we have, but in a subtle way that is easy to overlook. Exactly where we have implicitly relied on the primality of $p$ is left as the object of the first exercise.

**Problems**

1. In the above proof, where did we use the assumption that $p$ is prime?

2. Prove Lagrange's Theorem by contradiction. Assume that a polynomial $f$ with degree $d$ has $d+1$ roots

   $$r_1, r_2, \ldots, r_{d+1}$$

   modulo some prime $p$. Further assume that this is the polynomial with smallest degree with this property. Show that this leads to a contradiction.

   Hint: use the same method as the proof shown above.

3. In this problem consider the congruence

   $$x^d - 1 \equiv 0 \pmod{p}$$

   where $d$ is a factor of $p-1$.

   (a) Let $p - 1 = dd'$ and $y = x^d$. Show that

   $$x^{p-1} - 1 \equiv (y-1)(y^{d'-1} + y^{d'-2} + \cdots + 1) \pmod{p}.$$

   (b) What is the degree of the polynomial

   $$y^{d'-1} + y^{d'-2} + \cdots + 1$$

   in terms of $p$ and $d$?

   (c) Fermat's Little Theorem tells us that the congruence

   $$x^{p-1} - 1 \equiv 0 \pmod{p}$$

   has exactly $p-1$ solutions, as any value of $x$ except 0 is a solution. Use this to show that the congruence

   $$x^d - 1 \equiv 0 \pmod{p}$$

   has exactly $d$ solutions.

   Don't forget to use Lagrange's Theorem too!