IMO Training Session UCD April 26

T. J. LAFFEY

The theme of today's lecture is the use of polynomials in number theory.

A polynomial $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ has <u>degree</u> n if $a_0 \neq 0$. The numbers $a_0, a_1, \cdots, a_n$ are the <u>coefficients</u> of $f(x)$.

Polynomials can be added, multiplies by numbers (constants) and by one another.

One also has long division : given polynomials $f(x)$ and $g(x)$ with $g(x) \neq 0$, one can find polynomials $q(x)$, $r(x)$ with

$$f(x) = g(x)\,q(x) + r(x)$$

and $r(x)$ is either 0 or degree $r(x)$

$<$ degree $g(x)$.

<u>Example</u> $\underset{f(x)}{\underset{\uparrow}{x^6}} = \underset{g(x)}{\underset{\uparrow}{(x^2+x+1)}}\underset{q(x)}{\underset{\uparrow}{(x^4-x^3+x-1)}} \underset{r(x)}{\underset{\uparrow}{+1}}$.

A polynomial $f(x)$ of degree at least 1 has a root α (so $f(\alpha) = 0$) if and only if $x - \alpha$ divides $f(x)$ (without remainder).

A polynomial $f(x)$ of degree $n \geq 1$ has at most n distinct roots and if $f(x)$ has real or complex coefficients, then if

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

there are complex numbers $\alpha_1, \ldots, \alpha_n$ such that $f(x) = a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$.
[Fundamental Theorem of Algebra]. Even if $f(x)$ has real coefficients, the roots $\alpha_1, \ldots, \alpha_n$ need not necessarily be real.

Polynomials with rational or integer coefficients often arise in number theory.

Suppose $f(x)$ is a polynomial of degree $n \geq 1$ with rational coefficients. We say that $f(x)$ is irreducible over the rationals if one cannot factor $f(x) = g(x)\,h(x)$ where $g(x)$, $h(x)$ both have rational coefficients and both have degree less than n. ($\mathbb{Q}$ = field of rational numbers)

Example ① $x^2 - x + 1$ is irreducible over $\mathbb{Q}$

② $x^4 - 2$ is irreducible over $\mathbb{Q}$

③ $x^4 + 4$ is not irreducible over $\mathbb{Q}$.

① is clear since if $x^2 - x + 1$ were not irreducible over $\mathbb{Q}$, it would have to have a factor of degree 1, $ax - b$ with $a, b \in \mathbb{Q}$ and $x = b/a$ would be a root of $f(x) = 0$. But the roots of $f(x) = 0$ are $\frac{1 \pm i\sqrt{3}}{2}$ where $i = \sqrt{-1}$ and are not rational.

③ follows from the identity

$$x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2+2)^2 - (2x)^2$$
$$= (x^2 - 2x + 2)(x^2 + 2x + 2).$$

② $x^4 - 2$ has no factor of degree 1 over the rationals since $ax - b$ being a factor implies $x = b/a$ is a root and $x^4 - 2$ has no rational root. To show that $x^4 - 2$ is irreducible, we argue by contradiction. Suppose $f(x) = x^4 - 2 = g(x)\,h(x)$, where $g(x)$, $h(x)$ have rational coefficients and degree of each is less than 4. Then each must have degree 2, since $f(x)$ has no factors of degree 1 over the rationals. say

$$x^4 - 2 = (px^2 + ax + b)(qx^2 + cx + d)$$

where $p, q, a, b, c, d \in \mathbb{Q}$. Then $pq = 1$ and we can write

$$x^4 - 2 = (x^2 + a'x + b')(x^2 + c'x + d')$$

where $a', b', c', d' \in \mathbb{Q}$ — in fact $a' = a/p$, $b' = b/p$, $c' = c/q$, $d' = d/q$. Comparing coefficients, $b'd' = -2$, $a' + c' = 0$, and $a'c' + b' + d' = 0$. If $a'c' = 0$, then $b' + d' = 0$ and $d' = -b'$ and $b'd' = -b'^2 = -2$, so $b'^2 = 2$, which is impossible, since $\sqrt{2}$ is not rational. If $a'c' \neq 0$, then $c' = -a'$ and considering the coefficient of x, $a'd' + b'c' = 0$, so $d' - b' = 0$ and $b'^2 = -2$, which is also impossible. So $x^4 - 2$ is irreducible over the rationals.]

A polynomial $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ is called *monic* if $a_0 = 1$.

A famous result of Gauss, called Gauss's Lemma, states that if $f(x)$ is a polynomial of degree n with *integer* coefficients and $f(x) = g(x)h(x)$ where $g(x)$, $h(x)$ have *rational* coefficients, then there are rational numbers β, γ with $\beta\gamma = 1$ such that $g_1(x) = \beta g(x)$ and $h_1(x) = \gamma h(x)$ both have *integer* coefficients. This result is one of the most powerful results in this topic and allows very many different tools and tricks to be used in determining whether a polynomial with integer coefficients can be factored into two polynomials of lower degree and integer coefficients.

Application of Gauss's Lemma. Let $f(x) = x^3 - 3$. If $\sqrt[3]{3}$ were rational, we could write

$$f(x) = (x - \sqrt[3]{3})(x^2 + \sqrt[3]{3}\,x + (\sqrt[3]{3})^2)$$

using rational coefficients and then we can find rational numbers β, γ with $\beta\gamma = 1$ so that $\beta(x - \sqrt[3]{3})$ and $\gamma(x^2 + \sqrt[3]{3}\,x + (\sqrt[3]{3})^2)$ both have *integer* coefficients, so $\beta = \gamma = \pm 1$ and $\beta\sqrt[3]{3}$ is an integer, so $\sqrt[3]{3}$ is an integer. But $1 < \sqrt[3]{3} < 2$, so $\sqrt[3]{3}$ is certainly not an integer. Hence we conclude $\sqrt[3]{3}$ is not rational.

Example. Let $f(x) = x^4 - 10x^2 + 1$. If $f(x)$ is reducible over the rationals, then it has a factor of degree 1 or degree 2 over $\mathbb{Q}$ and by Gauss's Lemma, this says it has a factor of the same degree over the integers. If the degree is 1, this says $f(x) = 0$ has a factor $x - \alpha$ with α an integer, so $\alpha^4 = 10\alpha^2 - 1$, $\alpha^2 = 10 - \frac{1}{\alpha^2}$ and so $\frac{1}{\alpha^2}$ is an integer also, so $\alpha = \pm 1$ and ± 1 is not a root of $f(x) = 0$. Suppose $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ with a, b, c, d integers. Then $bd = 1$, so $b = d = \pm 1$. Also $a^2 + b + d = -10$ and $a^2 = -8$ or -12 so a is not rational. Hence $f(x)$ is irreducible over the rationals.

A general test for irreducibility was found by Eisenstein. It states:

Suppose $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$ where $a_1, a_2, \dots, a_n$ are integers and there exists a prime number p such that $p \mid a_1, p \mid a_2, \dots, p \mid a_n$, $p^2 \nmid a_n$. Then $f(x)$ is irreducible over the rational numbers.

P. 11

Example $x^4 - 2$ Take $p = 2$, $p \mid 2$, $p^2 \nmid 2$, so Eisenstein's result gives irreducibility.

x^4+8: IRR.

Note that with $f(x) = x^4 + 4$ and $p = 2$, $p \mid 4$, $p^2 \mid 4$ and Eisenstein's hypotheses are not valid for this polynomial. [6

—

Polynomials are often used in number Theory to keep track of information. For example, the following was an IMO problem in the 1980s. Suppose the set of natural number $\mathbb{N}$ is the disjoint union $S_1 \cup S_2 \cup \dots \cup S_k$ where $k > 1$ and S_i is an arithmetic progression with common difference d_i (so $S_i = \{a_i, a_i + d_i, a_i + 2d_i, a_i + 3d_i, \dots\}$ for some positive integers a_i, d_i) $(i = 1, 2, \dots, k)$. Then at least two of the differences d_i are equal.

Solution: Conside the series

$$f(z) = z + z^2 + z^3 + \dots$$

There is one term z^n for each $n \in \mathbb{N}$. But $n \in S_j$, so $n = a_j + m d_j$ for some $m \geq 0$ and some j, and $z^n = z^{a_j + m d_j}$.

Let $f_j(z) = z^{a_j} + z^{a_j + d_j} + z^{a_j + 2d_j} + \dots$

Then, since $\mathbb{N} = S_1 \cup S_2 \cup \dots \cup S_k$, disjoint union, $f(z) = f_1(z) + f_2(z) + \dots + f_k(z)$

For $|z| < 1$, $f(z) = \dfrac{z}{1-z}$ and $f_j(z) = \dfrac{z^{a_j}}{1 - z^{d_j}}$

and we have an identity

$$(*) \quad \frac{z}{1-z} = \frac{z^{a_1}}{1-z^{d_1}} + \circ \circ \circ + \frac{z^{a_k}}{1-z^{d_k}} \; ; \text{ for}$$

$|z| < 1$. Let $d = \max_{1 \le j \le k} d_j$ and suppose ~~that~~

$d = d_r$ and no other d_j. Then take

$$z = z_0 = r\left(\cos\frac{2\pi}{d} + i \sin\frac{2\pi}{d}\right) \quad (\text{so } z_0^{d_j} = r^{d_j}).$$

When $r = 1$, z_0 is a root of the equation $1 - z_0^{d_r} = 0$ but $1 - z_0^{d_j} \neq 0$ for any j with $d_j \neq d_r$. Also $z_0^{a_j} = r^{a_j}\left(\cos\frac{2\pi a_j}{d_j} + i \sin\frac{2\pi a_j}{d_j}\right)$.

with $|z_0^{a_j}| = r^{a_j}$

Think of what happens as we make r get close to (but less than 1). The denominator of the term $\frac{z_0^{a_r}}{1-z_0^{d_j}}$ gets close to zero and the numerator close to 1, so the absolute value of that term can be made as big as we wish. However, the denominator of any other term does not get close to 0 and the numerator gets close to 1 in absolute value, so we cannot make any other term arbitrarily large in absolute value in this way and the identity $(*)$ can then be violated. Hence we must have $d = d_r$ and also $d = d_s$ for some $s \neq r$ and the biggest d arises more than once. This solves the problem.

Another example. Suppose $A = \{a_1, a_2, \cdots, a_n\}$ is a set of n distinct positive integers $a_1, a_2, \cdots, a_n$ and we write

$A \oplus A$ for the list $(a_1+a_2, a_1+a_3, \cdots, a_1+a_n, a_2+a_3, \cdots, a_2+a_n, a_3+a_4, \cdots, a_{n-1}+a_n)$

$= (a_i + a_j : 1 \le i < j \le n)$

Suppose $B = \{b_1, b_2, \cdots, b_m\}$ is a set of m distinct positive integers and form $B \oplus B$.

Suppose the lists $A \oplus A$ and $B \oplus B$ contain exactly the same numbers (with the same multiplicities). Then we ask: must A equal B. First of all, the list for $A \oplus A$ has $\binom{n}{2}$ numbers and that for $B \oplus B$ has $\binom{m}{2}$ numbers, so $\binom{n}{2} = \binom{m}{2}$ and thus $m = n$.

However $A = \{2, 3, 4, 7\}$, $B = \{1, 4, 5, 6\}$, so $A \oplus A = (5, 6, 9, 7, 10, 11)$, $B \oplus B = \{5, 6, 7, 9, 10, 11)$, So $A \oplus A = B \oplus B$, but $A \neq B$. So is there anything else we can say about the sizes of A and B when $A \neq B$.

The following result is due to Erdös and Selfridge:

<u>Theorem</u>: Let A, B be sets of positive integers with n elements and suppose that $A \neq B$ and $A \oplus A = B \oplus B$. Then n is a power of 2.

<u>Proof</u>. Let $A = \{a_1, a_2, \dots, a_n\}$ and $B = \{b_1, b_2, \dots, b_n\}$. The trick is to form polynomials which determine A and B. Put $f(x) = x^{a_1} + x^{a_2} + \dots + x^{a_n}$, $g(x) = x^{b_1} + x^{b_2} + \dots + x^{b_n}$. Since $A \neq B$, $f(x) \neq g(x)$.

Next $f(x)^2 = (x^{a_1} + x^{a_2} + \dots + x^{a_n})(x^{a_1} + x^{a_2} + \dots + x^{a_n})$

$$= x^{2a_1} + x^{2a_2} + \dots + x^{2a_n} + 2\sum_{i<j} x^{a_i + a_j} \quad \dots (1)$$

Similarly $g(x)^2 = x^{2b_1} + x^{2b_2} + \dots + x^{2b_n} + 2\sum_{i<j} x^{b_i + b_j} \dots (2)$

The fact that $A \oplus A = B \oplus B$ means ~~that~~ the $\sum$ terms in $f(x)^2$ and $g(x)^2$ are the same.

Thus $f(x)^2 - g(x)^2 = (x^{2a_1} + x^{2a_2} + \dots + x^{2a_n}) - (x^{2b_1} + x^{2b_2} + \dots + x^{2b_n})$,

$(f(x) - g(x))(f(x) + g(x)) = f(x^2) - g(x^2) \; . \; . \; . \; (3)$

Let $h(x) = f(x) - g(x)$, so $f(x^2) - g(x^2) = h(x^2)$.

Note that $(f(1) - g(1))(f(1) + g(1)) = f(1) - g(1)$ and $f(1) + g(1) = 2n$, so $f(1) - g(1) = 0 = h(1)$.

So $x-1$ is a factor of $h(x)$. Let k be the positive integer such ~~that~~ $(x-1)^k$ divides $h(x)$ and $(x-1)^{k+1}$ does not divide $h(x)$. We then have $h(x) = (x-1)^k h_0(x)$, where $h_0(x)$ is a polynomial with integer coefficients and $h_0(1) \neq 0$.

Hence $h(x^2) = (x^2-1)^k h_0(x^2) = (x-1)^k(x+1)^k h_0(x^2)$.

Now equation ③ becomes

$$h(x)(f(x)+g(x)) = h(x^2),$$

$$(x-1)^k h_0(x)(f(x)+g(x)) = (x-1)^k(x+1)^k h_0(x^2),$$

and dividing by $(x-1)^k$ we get

$$h_0(x)(f(x)+g(x)) = (x+1)^k h_0(x^2)$$

and putting $x = 1$, we get

$$h_0(1)(f(1)+g(1)) = (1+1)^k h_0(1),$$

that is $h_0(1)(2n) = 2^k h_0(1)$,

so, since $h_0(1) \neq 0$, $2n = 2^k$ and

thus $n = 2^{k-1}$, as required.

Some more examples on irreducibility of polynomials.

(1) (Eisenstein) Let p be a prime. Then the polynomial $f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ is irreducible over the rationals.

[Outline solution: By Gauss's Lemma, we must show $f(x)$ is not the product of two monic polynomials of degree less than $p-1$ having integer coefficients. Suppose for the sake of contradiction, $f(x) = g(x)\,h(x)$, where $g(x)$, $h(x)$ are monic polynomials of degree less than $p-1$ having integer coefficients. Now

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$$
$$= (x-1)\,g(x)\,h(x).$$

The trick is to write $x = y+1$. Then

$$(y+1)^p - 1 = y\,g(y+1)\,h(y+1)$$

and $(y+1)^p = y^p + \binom{p}{1}y + \binom{p}{2}y^2 + \dots + \binom{p}{p-1}y + 1$

so $(y+1)^p - 1 = y\left(y^{p-1} + \binom{p}{1}y^{p-2} + \dots + \binom{p}{p-1}\right)$ and

thus $$y^{p-1} + \binom{p}{1}y^{p-2} + \dots + \binom{p}{p-1} = g(y+1)\,h(y+1). \circledast$$

However since p is prime, $p \mid \binom{p}{1}$, $p \mid \binom{p}{2}, \dots, p \mid \binom{p}{p-1}$ and also $p^2 \nmid \binom{p}{p-1} = p$. So $y^{p-1} + \binom{p}{1}y^{p-2} + \dots + \binom{p}{p-1}$ is irreducible over the rationals by Eisenstein's criterion. This contradicts $\circledast$, since $g(y+1)$ and $h(y+1)$ are both polynomials with integer coefficients and degree $< p-1$.

2. Prove that the polynomial

$$f(x) = (x-1)(x-2)(x-3)(x-4)(x-5)(x-6)+1$$

is irreducible over the rationals.

[Outline Solution: Suppose the result is false. By Gauss's Lemma, we have

$$f(x) = g(x)\,h(x) \quad \ldots \quad (1)$$

where $g(x)$, $h(x)$ are monic polynomials with integer coefficients and degree < 6.

Put $x=1$ in Equation (1). Then $1 = g(1)\,h(1)$. But $g(1)$ and $h(1)$ are integers, so either $g(1) = 1 = h(1)$ or $g(1) = -1 = h(1)$, so in any case $g(1) = h(1)$. Similarly $g(2) = h(2)$, $g(3) = h(3)$, $g(4) = h(4)$, $g(5) = h(5)$ and $g(6) = h(6)$. The polynomial $g(x) - h(x)$ has degree at most 5 and has at least six roots ($x = 1, 2, \ldots, 6$ are roots), so $g(x) - h(x) \equiv 0$ and $g(x) = h(x)$. From (1)

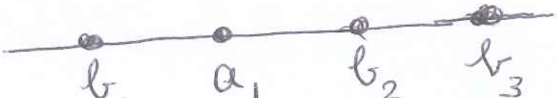
$$(x-1)(x-2)(x-3)(x-4)(x-5)(x-6) = g(x)^2 - 1$$
$$= (g(x)+1)(g(x)-1)$$

So $g(x) - 1$ is the product of some three of the factors $(x-1), (x-2), \ldots, (x-6)$ and $g(x)+1$ is the product of the other three. Write

$g(x) - 1 = (x-a_1)(x-a_2)(x-a_3)$ and

$g(x) + 1 = (x-b_1)(x-b_2)(x-b_3)$. So $a_1, a_2, a_3, b_1, b_2, b_3$ is a permutation of the numbers $1, 2, 3, 4, 5, 6$

Put $x = a_1$. Then $g(a_1) = 1$ and $g(a_1)+1 = 2$. So $2 = (a_1 - b_1)(a_1 - b_2)(a_1 - b_3)$. Hence two of the numbers $a_i - b_i$ are ± 1 and the third one is -2. So we can assume that $a_1 - b_1 = 1$, $a_1 - b_2 = -1$, $a_1 - b_3 = -2$



Next, put $x = a_2$ in $g(x)$. We get $g(a_2) = 1$ and $2 = (a_2 - b_1)(a_2 - b_2)(a_2 - b_3)$ and again the numbers $a_2 - b_1$, $a_2 - b_2$, $a_2 - b_3$ are $1, -1, -2$ in some order.

However $a_2 - b_2 \neq 1$, since $a_2 \neq a_1$.

Also $a_2 - b_2 \neq -1$, since $a_2 \neq b_3$.

so $a_2 - b_2 = -2$ and this implies that $a_2 = b_1$, which is false. This contradiction implies that $f(x)$ is irreducible over the rationals.

3. The polynomial $x^7 + 11x^4 + 1282$ is irreducible over the rationals.

[Outline solution: Arguing by contradiction, assume it is not irreducible. Using Gauss's Lemma) $f(x) = x^7 + 11x^4 + 1282 = g(x)h(x)$ for some monic polynomials $g(x)$, $h(x)$ with integer coefficients and degree < 7. Now $g(0)h(0) = 1282 = 2 \times 641$ and one checks that 641 is prime. So one of $|g(0)|, |h(0)| \leq 2$, say $|g(0)| \leq 2$. Since $|g(0)|$ = product of $|\lambda|$ as λ runs over the roots of $g(x) = 0$ in the complex numbers, $|\lambda| \leq 2$ for some such root. But $|\lambda|^7 + 11|\lambda|^4 \leq 128 + 176 < 1282$, so $f(\lambda) \neq 0$]

4. The polynomial $x^9 + 42x^5 - 84x^4 + 247$ is irreducible over the rationals.

[Outline Solution: Put $x = y+2$. Notice that $(y+2)^9 = y^9 + 2\binom{9}{1}y^8 + 2^2\binom{9}{2}y^7 + \cdots + 2^8\binom{9}{1}y + 2^9$ has all its coefficients except those of y^9 and y^0 divisible by 3. Also $42(y+2)^5 - 84(y+2)^4$ has all its coefficients divisible by 3 and its constant term is $42 \times 2^5 - 84 \times 2^4 = 0$. So if $f(x) = x^9 + 42x^5 - 84x^4 + 247$, then

$$f(y+2) = y^9 + a_1 y^8 + a_2 y^7 + \cdots + a_8 y + 2^9 + 247.$$

Now $2^9 + 247 = 759 = 3 \times 253$ and all the coefficients $a_1, a_2, a_3, \ldots, a_8$ are divisible by 3 and 3 divides 759 and 3^2 does not divide 759. So using Eisenstein's criterion with $p = 3$, $f(y+2)$ cannot be factored as the product of two polynomials with integer coefficients and degree less than 9. But if $f(x)$ is reducible, Gauss's Lemma yields $f(x) = g(x)h(x)$ for some polynomials $g(x)$, $h(x)$ with integer coefficients and degree less than 9. But then $f(y+2) = g(y+2)h(y+2)$, giving a contradiction. So $f(x)$ is irreducible over the rationals.