UCD Mathematical Enrichment Programme 2017.

April 8

Polynomials, power series, number theory.

T. J. Laffey.

If we are given a polynomial $f(x)$ with rational coefficients, we may not be able to factor it as $f(x) = g(x)\,h(x)$ where both $g(x)$ and $h(x)$ have smaller degree than the degree of $f(x)$, if we insist that $g(x)$ and $h(x)$ have rational coefficients. For example, $f(x) = x^2+4$ factors using complex numbers as $(x+2i)(x-2i)$, where $i = \sqrt{-1}$. However, it cannot be factored using just real numbers as $(x-a)(x-b)$ since then $a^2 = -4$ and $b^2 = -4$, while squares of real numbers cannot be negative.

In the case of the polynomial $f(x) = x^2-2$, using real numbers, we can factor $f(x) = (x-\sqrt{2})(x+\sqrt{2})$, as $\sqrt{2}$ is a real number, but $\sqrt{2}$ is not a rational number, while if $x-q$ is a factor of x^2-2, $q^2-2=0$ and q must be $\pm\sqrt{2}$. So x^2-2 cannot be factored into the product of two polynomials of lower degree using only rational numbers.

Definition. A polynomial $g(x)$ with rational coefficients and degree at least 1 is called irreducible over the rationals if $g(x)$ cannot be factored into the product $u(x)\,v(x)$ of polynomials $u(x)$, $v(x)$ with rational coefficients and each having degree less than the degree of $g(x)$.

For example, every polynomial $g(x)$ of degree 1 is irreducible.

x^2-2 and x^2-3 are examples of polynomial of degree 2 which are irreducibl over the rationals.

Testing whether a given polynomial $g(x)$ with rational coefficients is irreducible over the rationals can be quite difficult. The following major result of Gauss helps:

3

<u>Gauss's Lemma</u>. Let $g(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ where $a_0, a_1, \cdots, a_n$ are <u>integers</u> and $a_0 \neq 0$. Suppose that $g(x) = u(x)\, v(x)$ where
$$u(x) = b_0x^r + b_1x^{r-1} + \cdots + b_r,$$
$$v(x) = c_0x^s + c_1x^{s-1} + \cdots + c_s,$$
where $1 \leq r, s < n$ and all the coefficients $b_0, b_1, \cdots, b_r, c_0, c_1, \cdots, c_s$ are <u>rational</u> numbers. Then $g(x) = u_1(x)\, v_1(x)$ where
$$u_1(x) = p_0x^r + p_1x^{r-1} + \cdots + p_r = \frac{p_0\, u(x)}{b_0},$$
$$v_1(x) = q_0x^s + q_1x^{s-1} + \cdots + q_s = \frac{q_0\, v(x)}{c_0},$$
where $p_0, p_1, \cdots, p_r, q_0, q_1, \cdots, q_s$ are all integers. Note the same r, s occurs in the second factorization

The proof is not especially difficult, but, due to time constraints, we will not present it here. However, it is very important that if a student wants to apply it in solving an IrMO or IMO problem, he or she must quote it in full with absolute accuracy, otherwise one gets an automatic gloo.
The need for absolute accuracy applies to the use of any result which is not proved in the solution to a problem.
If you Google Gauss's Lemma, you will be offered several proofs and applications.

<u>Example</u>. Consider the polynomial x^3-3. Suppose we can factor

① : $x^3-3 = (b_0x+b_1)(c_0x^2+c_1x+c_2)$

where b_0, b_1, c_0, c_1, c_2 are all integers. Then $b_0c_0=1$ on looking at the coefficients of x^3.

So $b_0 = c_0 = 1$ or $b_0 = c_0 = -1$, since b_0, c_0 are integers.

Case 1 $b_0 = c_0 = 1$. Comparing the coefficient of x^0, the constant term, we get $b_1 c_2 = -3$, and because b_1 and c_2 are integers, the only possibilities are $(b_1, c_2) = (1,-3), (-1,3), (3,-1), (-3,1)$.

Comparing the coefficient of x^2, we get $b_0 c_1 + b_1 c_0 = 0$, so $c_1 + b_1 = 0$.

Comparing the coefficient of x, we get

$$b_0 c_2 + b_1 c_1 = 0.$$

So $c_2 = -b_1 c_1 = b_1^2$ (since $c_1 + b_1 = 0$).

It follows that $c_2 = 1$, since $c_2 \in \{1, -1, 3, -3\}$ and $b_1 = -3$, giving a contradiction.

Case 2 $b_0 = c_0 = -1$ leads to a contradiction in the same way.

Hence no factorization of the form (1) is possible... (2)

But suppose that $\alpha = \sqrt[3]{3}$ is a rational number. Then $\alpha^3 = 3$

and

$$x^3 - 3 = x^3 - \alpha^3 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$$

and both factors $x - \alpha$ and $x^2 + \alpha x + \alpha^2$ have rational coefficients.

Applying Gauss's Lemma (Here $r = 1$, $s = 2$) we deduce that a factorization of the form (1) must exist, contradicting (2). Hence the assumption that α is a rational number is false.

So $\sqrt[3]{3}$ is not rational.

Gauss's Lemma is one of the most powerful tools in proving the irrationality of numbers.

<u>Example</u>. Prove that $\alpha = \sqrt{2} + \sqrt[3]{3}$ is not a rational number.

<u>Solution</u>. While $\sqrt{2}$ and $\sqrt[3]{3}$ are not rational numbers, it does not follow that $\sqrt{2} + \sqrt[3]{3}$ is not rational (as depending on the numbers involved, the sum of two irrational numbers can be rational or irrational. (Note however that the sum of two rational numbers is always a rational number.

To solve the problem, we note that $\alpha - \sqrt{2} = \sqrt[3]{3}$ and cubing gives

$$(\alpha - \sqrt{2})^3 = 3,$$

that is

$$\alpha^3 - 3\alpha^2\sqrt{2} + 6\alpha - 2\sqrt{2} = 3 .$$

Hence

$$\alpha^3 + 6\alpha - 3 = \sqrt{2}\,(3\alpha^2 + 2).$$

Squaring yields

$$(\alpha^3 + 6\alpha - 3)^2 = 2\,(3\alpha^2 + 2)^2.$$

Expanding we get

$$\alpha^6 + 12\alpha^4 - 6\alpha^3 + 36\alpha^2 - 36\alpha + 9 = 18\alpha^4 + 24\alpha^2 + 8,$$

that is

$$\alpha^6 - 6\alpha^4 - 6\alpha^3 + 12\alpha^2 - 36\alpha + 1 = 0.$$

Let $f(x) = x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$. Then α is a root of $f(x) = 0$. Suppose that α is rational. Then $x - \alpha$ is a factor of $f(x)$ and $f(x) = (x-\alpha)(x^5 + h_1 x^4 + h_2 x^3 + h_3 x^2 + h_4 x + h_5)$.

The formulas $x^6 - \alpha^6 = (x-\alpha)(x^5 + \alpha x^4 + \alpha^2 x^3 + \alpha^3 x^2 + \alpha^4 x + \alpha^5)$,
$x^4 - \alpha^4 = (x-\alpha)(x^3 + \alpha x^2 + \alpha^2 x + \alpha^3)$, $x^3 - \alpha^3 = (x-\alpha)(x^2 + \alpha x + \alpha^2)$ and $x^2 - \alpha^2 = (x-\alpha)(x+\alpha)$ and the rationality of α imply that the coefficients h_1, h_2, h_3, h_4, h_5 are all rational. Let $u(x) = x - \alpha$,

$$v(x) = x^5 + h_1 x^4 + h_2 x^3 + h_3 x^2 + h_4 x + h_5.$$

Now $f(x) = u(x)v(x)$ and $f(x)$ has integer coefficients, while $u(x)$ and $v(x)$ have rational coefficients. So we can apply Gauss's Lemma to get

$$f(x) = u_1(x)\, v_1(x), \text{ where } u_1(x) = a_0 x + a_1,$$

$v_1(x) = b_0 x^5 + b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5$, where

$a_0, a_1, b_0, b_1, \cdots, b_5$ are all integers and $u_1(x) = a_0(x-\alpha)$. Comparing the coefficient of x^6 yields $a_0 b_0 = 1$, so $a_0 = b_0 = \pm 1$, since a_0, b_0 are integers. Comparing the constant term, we get $a_1 b_5 = 1$, and thus $a_1 = \pm 1$, since a_1 and b_5 are integers. Hence $\alpha = -\dfrac{a_1}{a_0} = \pm 1$. Since $\alpha = \sqrt{2} + \sqrt[3]{3}$, $\alpha > 1$, so we have a contradiction. The contradiction arose from assuming α is rational. Hence α is not rational.

<u>Exercise</u>. Prove that the following numbers are not rational: $\sqrt{2}+\sqrt{3}$, $\sqrt{5}+\sqrt[3]{5}$.

<u>Note</u>. The number e and Napier's number e are not rationals, but the proof is more difficult. It is not known whether $e+\pi$ is rational or not.

Testing whether a polynomial with rational coefficients is irreducible over the rationals by hand often depends on finding the right trick. However, there is one famous criterion for irreducibility.

Eisenstein's Irreducibility Criterion.

Suppose that $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, where $a_0 \neq 0, a_1, \ldots, a_n$ are integers. Suppose there is a prime number p such that

(i) p does not divide a_0

(ii) p divides $a_1, a_2, \ldots, a_n$ and

(iii) p^2 does not divide a_n.

Then $f(x)$ is irreducible over the rationals.

Examples ① $x^3 - 3$; take $p = 3$

② $x^4 + 5x^3 + 10x^2 + 10x + 5$, take $p = 5$.

③ $x^4 + x^3 + x^2 + x + 1$.

[If this polynomial, $g(x)$ is not irreducible then $g(x) = u(x)v(x)$, where $u(x)$, $v(x)$ are polynomials with rational coefficients of degree less than 4. Now replace x by $x+1$ and show you contradict ②.]

(4) Prove that $x^n - 3x + 5$, is irreducible over the rationals. [11]

<u>Solution</u> Suppose that $f(x) = x^n - 3x + 5$ is reducible ($=$ not irreducible) over the rationals. Then $n > 1$ and using Gauss's Lemma (which applies since $f(x)$ has integer coefficients),

$$f(x) = u(x)\, v(x)$$

for some polynomials $u(x)$, $v(x)$ with <u>integer</u> coefficients and degree $u(x) = r$, degree $v(x) = s$, for some r, s with $1 \le r, s < n$ and $n = r + s$.

By the fundamental theorem of algebra,

$$u(x) = a(x - \alpha_1) \cdots (x - \alpha_r),$$
$$v(x) = b(x - \beta_1) \cdots (x - \beta_s),$$

where a, b are integers and $\alpha_1, \ldots, \alpha_r$, $\beta_1, \ldots, \beta_s$ are complex numbers.

Comparing the coeffients of x^n on both sides of the equation $f(x) = u(x) v(x)$, we obtain $ab = 1$, so $a = b = \pm 1$.

Note that $f(0) = u(0) v(0)$ and $u(0)$, $v(0)$ are integers, since $u(x)$, $v(x)$ have integer coefficients.

But $f(0) = 5$, so one of $u(0)$, $v(0)$ is ± 1 and the other ± 5. Say $u(0) = \pm 1$.

So $a(-1)^r \alpha_1 \alpha_2 \cdots \alpha_r = \pm 1$ and taking absolute values and the fact that $a = \pm 1$ also, we get

$$|\alpha_1 \alpha_2 \cdots \alpha_r| = 1,$$

and hence

$$|\alpha_1||\alpha_2| \cdots |\alpha_r| = 1.$$

Hence for some j with $1 \leq j \leq r$, we must have $|\alpha_j| \leq 1$.

Since $f(x) = u(x)\, v(x)$, $f(\alpha_j) = 0$, that is $\alpha_j^n - 3\alpha_j + 5 = 0$.

Hence, $5 = -\alpha_j^n + 3\alpha_j$ and taking absolute values

$$\begin{aligned} 5 = |5| &= |-\alpha_j^n + 3\alpha_j| \\ &\leq |-\alpha_j^n| + |3\alpha_j| \\ &= |\alpha_j|^n + 3|\alpha_j| \\ &\leq 1 + 3 = 4, \text{ since } |\alpha_j| \leq 1, \end{aligned}$$

implying $5 \leq 4$, which is false. This contradiction arose from assuming that $f(x)$ is reducible. Hence $f(x)$ is irreducible as claimed.

<u>Example 5.</u> x^4+2 is irreducible over the rationals. (Eisenstein with $p=2$)

<u>Example 6.</u> $x^4+4 = x^4+4x^2+4 - 4x^2$

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

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

<u>Example 7.</u> x^4+8 is irreducible over the rationals.

<u>Solution</u>: Suppose that it is reducible over the rationals. Using Gauss's Lemma, we can write $f(x) = x^4+8$ as a product $u(x)v(x)$ of polynomials with integer coefficients and degree less than 8. Since $u(0)v(0) = f(0) = 8$, $u(0) = \pm 1$, ± 2, ± 4 or ± 8.

<u>Claim 1.</u> $u(0) \neq \pm 1$. Using the argument of the solution to (4) on page 10, there would be a root α of $u(x)$ with $|\alpha| \leq 1$. But $\alpha^4+8 = 0$, so $|\alpha|^4 = |-8| = 8$ and this is impossible.

Claim 2. $u(0) \neq \pm 2$.

For suppose $u(0) = \pm 2$. As in (4) on page 10, $u(x) = a(x-\alpha_1)\cdots(x-\alpha_r)$, for $a = \pm 1$, some integer r with $1 \leq r < 8$ and roots $\alpha_1, \cdots, \alpha_r$ in $\mathbb{C}$, the {complex numbers}.

So $|u(0)| = |\alpha_1||\alpha_2|\cdots|\alpha_r|$.

We now calculate $|\alpha_j|$.

The roots of $z^4+1=0$ also satisfy the equation $z^8-1=0$, since $z^8-1=(z^4-1)(z^4+1)$.

We know that the roots of $z^8-1=0$ are of the form $\cos\frac{2k\pi}{8} + i\sin\frac{2k\pi}{8}$ and $0 \leq k < 8$, so each root has absolute value $\sqrt{\cos^2\frac{2k\pi}{8} + \sin^2\frac{2k\pi}{8}} = 1$.

So if $\lambda^8+1=0$, $|\lambda| = 1$. If $\mu^4+8=0$, then $\left(\frac{\mu}{\sqrt[4]{8}}\right)^4+1=0$, and $\left|\frac{\mu}{\sqrt[4]{8}}\right| = 1$ and $|\mu| = \sqrt[4]{8}$

Since $\alpha_j^4+8=0$, $|\alpha_j| = \sqrt[4]{8}$.

Hence $|u(0)| = 8^{r/4}$. Thus $8^{r/4}=2$ and $2^{3r} = 8^r = 2^4$, implying $r = 4/3$, which is impossible

Claim 3 $|u(0)| \neq 4$.

As in the case dealt with in Claim 2, we get $u(0) = 8^{r/4}$ and $2^{3r} = 4^4 = 2^8$ and $3r = 8$, which is impossible.

So we must have $|u(0)| = 8$ and as in Claim 2, $8^{r/4} = 8$ and $r = 4$. But this implies that $u(x)$ has degree 4, contradicting our initial assumption that $u(x), v(x)$ both have degree less than 4. Hence $x^4 + 8$ is irreducible over the rationals.

[The solution is written in a very lengthy form. It is instructive to study it to see why the argument does not work for $x^4 + 4$, as we know it must. Note that the Eisenstein criterion does not apply to x^4+4, x^4+8 as the only possible prime p would be $p=2$ and p^2 divides 4 and p^2 divides 8 in this case]

Sequences.

Suppose we are given the first few terms of a sequence and a recurrence relation expressing the n^{th} term in terms of earlier terms. We would like to find an explicit formula for the nth term. The best known example is probably the Fibonacci sequence $\{F_n\}$ defined by $F_0 = F_1 = 1$, $F_{n+2} = F_n + F_{n+1}$, for $n = 0, 1, 2, \ldots$, and we want an explicit formula for F_n.

One method is to write down several terms and view the pattern and try and guess the formula and then try to prove the guess correct by induction. That is often the simplest way, but here I want to describe a more systematic way which sometimes works. We illustrate the method using the Fibonacci sequence.

Let $f(x) = F_0 + F_1 x + F_2 x^2 + \cdots + F_n x^n + F_{n+1} x^{n+1} + F_{n+2} x^{n+2} + \cdots$

Then

$$x f(x) = F_0 x + F_1 x^2 + \cdots + F_n x^{n+1} + F_{n+1} x^{n+2} + \cdots$$

$$x^2 f(x) = F_0 x^2 + F_1 x^3 + \cdots + F_n x^{n+2} + \cdots$$

Note here that when we add $x f(x)$ and $x^2 f(x)$ and collect terms with the same power of x, and use the recurrence relation $F_{n+2} = F_n + F_{n+1}$, (so $F_3 = F_1 + F_2$, $F_4 = F_2 + F_3$, ...), we get

$$(x^2 + x) f(x) = F_0 x + F_2 x^2 + F_3 x^3 + \cdots + F_{n+2} x^{n+2} + \cdots$$
$$= f(x) - 1 \quad (\text{using } F_0 = F_1 = 1).$$

Hence $f(x)(1 - x - x^2) = 1$.

The roots of the polynomial $y^2 - y - 1 = 0$ are $y = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$ and putting $\alpha = \frac{1+\sqrt5}{2}$, $\beta = \frac{1-\sqrt5}{2}$, we get

$$1 - x - x^2 = (1 - \alpha x)(1 - \beta x).$$

Next, $f(x) = \dfrac{1}{(1-\alpha x)(1-\beta x)}$ and we try to break this into two parts. Suppose

$$\frac{1}{(1-\alpha x)(1-\beta x)} \equiv \frac{A}{1-\alpha x} + \frac{B}{1-\beta x}.$$

Then $1 = A(1-\beta x) + B(1-\alpha x)$
$= A + B - x(\beta A + \alpha B)$.

Solve $A + B = 1$, $\beta A + \alpha B = 0$ to get

$$\left.\begin{array}{l} \alpha A + \alpha B = \alpha \\ \beta A + \alpha B = 0 \end{array}\right] \Rightarrow A = \frac{\alpha}{\alpha - \beta}, \; B = \frac{-\beta}{\alpha - \beta}.$$

Consider the geometric progression

$$1 + \alpha x + \alpha^2 x^2 + \cdots = \frac{1}{1 - \alpha x} \quad \left(\text{for } |x| < \frac{1}{\alpha}\right)$$

$$1 + \beta x + \beta^2 x^2 + \cdots = \frac{1}{1 - \beta x} \quad \left(\text{for } |x| < \frac{1}{|\beta|}\right)$$

Hence $f(x)$ can be written

$$\frac{1}{\alpha - \beta}\left[\alpha(1 + \alpha x + \alpha^2 x^2 + \cdots) - \beta(1 + \beta x + \beta^2 x^2 + \cdots)\right]$$

$$= \frac{1}{\alpha-\beta}\left[(\alpha - \beta) + (\alpha^2 - \beta^2)x + (\alpha^3 - \beta^3)x^2 + \cdots + (\alpha^{n+1} - \beta^{n+1})x^n + \cdots\right.$$

$$= 1 + \left(\frac{\alpha^2 - \beta^2}{\alpha - \beta}\right)x + \left(\frac{\alpha^3 - \beta^3}{\alpha - \beta}\right)x^2 + \cdots + \frac{(\alpha^{n+1} - \beta^{n+1})}{\alpha - \beta}x^{n+1} + \cdots$$

Hence
$$F_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}, \text{ where}$$
$\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$, so $\alpha - \beta = \sqrt{5}$.

One consequence of this and the fact that α is approx. 1.6 while $|\beta|$ is approximately 0.6, is that
$$\frac{F_{n+1}}{F_n} = \frac{\alpha^{n+2} - \beta^{n+2}}{\alpha^{n+1} - \beta^{n+1}} = \alpha \frac{1 - \left(\frac{\beta}{\alpha}\right)^{n+2}}{1 - \left(\frac{\beta}{\alpha}\right)^{n+1}} \to \alpha$$
as $n \to \infty$. The number $\alpha = \frac{1+\sqrt{5}}{2}$ is called the <u>Golden mean</u>, and in ancient Greek as well as modern architecture, it is considered the most pleasing ratio to the eye for proportions of windows etc. Also, it is the ratio of breadth versus height you see in the screens of old TVs.

In general, if we are given a sequence $\{s_n\}$ where $s_0 = a$, $s_1 = b$ are given and $s_{n+2} = p s_n + q s_{n+1}$, we put $f(x) = s_0 + s_1 x + s_2 x^2 + \dots + s_n x^n + \dots$

and then add $px^2 f(x)$ and $qx f(x)$ and using $ps_n + qs_{n+1} = s_{n+2}$ obtain

$$(1 - px - qx^2) f(x) = s_0 + (s_1 - qs_0)x$$

and $$f(x) = \frac{s_0 + (s_1 - qs_0)x}{1 - px - qx^2}.$$

One can then factorize $1 - px - qx^2$
$= (1 - \gamma x)(1 - \delta x)$ and proceed as for Fibonacci to get a formula for the term s_n.

In general, the method works for linear recurrences – the nth term t_n of the sequence satisfies (for all n)

$$t_{n+k} = c_0 t_n + c_1 t_{n+1} + \dots + c_{k-1} t_{n+k-1},$$

where k and $c_0, c_1, \dots, c_{k-1}$ are fixed numbers.

Also, noticing that with $f(x)$ as at top of this page, $\frac{df}{dx}$ has ns_n as the coefficient of x^{n-1}, using ingenuity, it has wide uses.

Binomial Coefficients.

Binomial coefficients arise in many parts of Mathematics and it is easy to construct very tricky questions about them.

The binomial theory states that

$$(1+x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n!}{r!\,(n-r)!}.$$

Here $0! = 1$ and for n a positive integer, $n! = n(n-1)\cdots 2.1$, so $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $\ldots$.

$\binom{n}{r}$ is the number of ways of choosing a team of r players from n players, when n and r are positive integers. So $\binom{n}{r}$ is a positive integer when n, r are positive integers and $r \le n$.
[If $r > n$, $\binom{n}{r} = 0$ here].

<u>Exercise</u>. The Catalan numbers C_n are defined as follows: $C_1 = 1$, and, for $n \geq 1$,

$$(n+2)\,C_{n+1} = 2(2n+1)\,C_n.$$

Prove, by induction, that $C_n = \frac{1}{n+1}\binom{2n}{n}$.

Prove that

$$C_n = \sum_{k=0}^{n-1} C_k C_{n-k-1}.$$

Deduce that C_n is a positive integer.

This exercise is typical of questions about binomial coefficients. It is not at all clear from the definition, or the formula, that C_n is an integer.

The number $\binom{2n}{n}$ occurs in many questions. For example, if one tosses a (fair) coin $2n$ times, the probability that one gets exactly k heads is $\binom{2n}{k}\left(\frac{1}{2}\right)^{2k}$. Hence $\binom{2n}{n}\frac{1}{2^{2n}}$ is the probability that one gets exactly n heads and n tails. A natural question is: how big is this number for large n.

To answer this, one needs to know Stirling's formula which states that $\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ is a good approximation for $n!$ for large n. [Here $e = 2.718281828\ldots$ is Napier's number, the base for $\ln$].

Using this, one gets that $\binom{2n}{n}\frac{1}{2^{2n}}$ is approximately $\frac{1}{\sqrt{\pi n}}$ for n large. So, for example, if $n = 100$, the probability is approximately $\frac{1}{\sqrt{100\pi}}$, which is close to $\frac{1}{18}$, which is bigger than one might expect.

Suppose p is a prime number $< 2n$. Then p divides $(2n)!$. If $p > n$, then p does not divide $(n!)^2$ [Note that if a prime divides the product of two integers, it must divide at least one of them and $n! = n(n-1)\cdots 2\cdot 1$ has all its factors $n-i < p$]

Hence, since $\binom{2n}{n}$ is an integer, if $n < p < 2n$, p must divide $\binom{2n}{n}$.

Hence $\binom{2n}{n}$ is at least as big as the product of all prime numbers p with $n < p < 2n$.

So, if there are k prime number p_i with $1 \leq n < p_i < 2n$, then

$$\binom{2n}{n} \geq p_1 p_2 \cdots p_k \geq (n+1)^k$$

and taking logs,

$$k \leq \frac{\ln \binom{2n}{n}}{\ln (n+1)} \leq \frac{\log \binom{2n}{n}}{\log (n)} \quad \cdots (1)$$

Exercise : Check that if $1 \leq k \leq n$, then $\binom{2n}{k} \leq \binom{2n}{n}$.

By the binomial theorem $(1+1)^{2n} = \sum_{j=0}^{2n} \binom{2n}{j}$,

so, in particular, $\binom{2n}{n} < 2^{2n}$

So (1) gives $k < \dfrac{2n \log 2}{\log n}$.

[Ex.. Use the exercise to get a slightly better bound].

These examples illustrate a few ways of how binomial coefficients can give rise to nice questions. Look at IMO type questions on the net to find many more]

Solution to the Exercises on page 26 of the March 25 Lecture (S1)

1. $1/z = \cos\theta - i\sin\theta$, since $(\cos\theta + i\sin\theta)(\cos\theta - i\sin\theta)$
$= \cos^2\theta + \sin^2\theta = 1.$

So $z + \frac{1}{z} = (\cos\theta + i\sin\theta) + (\cos\theta - i\sin\theta)$
$= 2\cos\theta$ and
$z - \frac{1}{z} = (\cos\theta + i\sin\theta) - (\cos\theta - i\sin\theta)$
$= 2i\sin\theta.$

By DeMoivre's Theorem, $z^m = (\cos\theta + i\sin\theta)^m$
$= \cos m\theta + i\sin m\theta$, and $\frac{1}{z^m} = \cos m\theta - i\sin m\theta$,
so $(\cos\theta - i\sin\theta)^m = \cos m\theta - i\sin m\theta$, for all positive integers m.

Suppose $n = 2k$, where k is a positive integer. Then $\left(z + \frac{1}{z}\right)^n = (2\cos\theta)^n = 2^n\cos^n\theta$.

Expanding $\left(z + \frac{1}{z}\right)^n = \left(z + \frac{1}{z}\right)^{2k}$ by the binomial theorem, we obtain

$$2^n\cos^n\theta = z^{2k} + \binom{2k}{1} z^{2k-1}\left(\frac{1}{z}\right) + \binom{2k}{2} z^{2k-2}\left(\frac{1}{z}\right)^2 + \cdots$$
$$+ \binom{2k}{r} z^{2k-r}\left(\frac{1}{z}\right)^r + \cdots + \binom{2k}{k} z^{2k-k}\left(\frac{1}{z}\right)^k + \cdots$$
$$+ \binom{2k}{2k-r} z^{2k-(2k-r)}\left(\frac{1}{z}\right)^{2k-r} + \cdots$$
$$+ \binom{2k}{2k-1} z\left(\frac{1}{z}\right)^{2k-1} + \binom{2k}{2k}\left(\frac{1}{z}\right)^{2k}.$$

Using the fact that for binomial coefficients $\binom{m}{s} = \binom{m}{m-s}$ and combining the term with z^t with the term with $\left(\frac{1}{z}\right)^t$ and using the formula

CS2

$$z^t + \left(\frac{1}{z}\right)^t = 2\cos t\theta, \quad \text{for } t = 0, 1, \dots, k-1,$$

we obtain

$$2^n \cos^n\theta = 2\cos 2k\theta + \binom{2k}{1} 2\cos(2k-2)\theta + \binom{2k}{2} 2\cos(2k-4)\theta + \dots + \binom{2k}{k-1} 2\cos(2k-2(k-1))\theta + \binom{2k}{k}.$$

Dividing by 2 yields

$$2^{n-1}\cos^n\theta = \cos n\theta + \binom{n}{1}\cos(n-1)\theta + \binom{n}{2}\cos(n-2)\theta + \dots + \binom{n}{k-1}\cos 2\theta + \frac{1}{2}\binom{n}{k}.$$

When $n = 2k+1$, the argument is the same except that rather than have one term $\binom{2k}{k}$ without a multiple of $2\cos$, we get two terms

$$\binom{2k+1}{k} z + \binom{2k+1}{k+1} z^{-1} = \binom{2k+1}{k} 2\cos\theta.$$

So the formula is:

$$2^{2k}\cos^{2k+1}\theta = \cos(2k+1)\theta + \binom{2k+1}{1}\cos(2k-1)\theta + \binom{2k+1}{2}\cos(2k-3)\theta + \dots + \binom{2k+1}{k}\cos\theta.$$

S3

To get corresponding formulae for $\sin n\theta$, one can use $\left(z-\frac{1}{z}\right)^n$ instead of $\left(z+\frac{1}{z}\right)^n$, or alternatively, differentiate the formula for $\cos n\theta$ with respect to θ.

2. This problem with $\cos\frac{\pi}{7}$ etc is supposed to remind you of roots of unity.
The 14th roots of unity are $\cos\frac{2k\pi}{14}+i\sin\frac{2k\pi}{14}$, $k=0,1,2,\dots,13$. Since $z^{14}-1=(z^7-1)(z^7+1)$, the seven 7th roots of unity are included in that list – those are the ones with k even. Hence the roots of $z^7+1=0$ are $\cos\frac{2\pi}{14}+i\sin\frac{2\pi}{14}$, $\cos\frac{6\pi}{14}+i\sin\frac{6\pi}{14}$, $\cos\frac{10\pi}{14}+i\sin\frac{10\pi}{14}$, $\cos\frac{14\pi}{14}+i\sin\frac{14\pi}{14}$, $\cos\frac{18\pi}{14}+i\sin\frac{18\pi}{14}$, $\cos\frac{22\pi}{14}+i\sin\frac{22\pi}{14}$, $\cos\frac{26\pi}{14}+i\sin\frac{26\pi}{14}$, that is:

$\cos\frac{\pi}{7}+i\sin\frac{\pi}{7}$, $\cos\frac{3\pi}{7}+i\sin\frac{3\pi}{7}$, $\cos\frac{5\pi}{7}+i\sin\frac{5\pi}{7}$,
$\cos\pi+i\sin\pi=-1$, $\cos\frac{9\pi}{7}+i\sin\frac{9\pi}{7}$,
$\cos\frac{11\pi}{7}+i\sin\frac{11\pi}{7}$, $\cos\frac{13\pi}{7}+i\sin\frac{13\pi}{7}$.

Note that $\cos\frac{13\pi}{7} + i\sin\frac{13\pi}{7} = \cos\left(2\pi - \frac{\pi}{7}\right)$
$+ i\sin\left(2\pi - \frac{\pi}{7}\right) = \cos\frac{\pi}{7} - i\sin\frac{\pi}{7}$,

$\cos\frac{11\pi}{7} + i\sin\frac{11\pi}{7} = \cos\left(2\pi - \frac{3\pi}{7}\right) + i\sin\left(2\pi - \frac{3\pi}{7}\right)$
$= \cos\frac{3\pi}{7} - i\sin\frac{3\pi}{7}$ and $\cos\frac{9\pi}{7} + i\sin\frac{9\pi}{7}$
$= \cos\frac{5\pi}{7} - i\sin\frac{5\pi}{7}$.

Hence the sum of all the roots of the equation $z^7 + 1 = 0$ are
$2\cos\frac{\pi}{7} + 2\cos\frac{3\pi}{7} + 2\cos\frac{5\pi}{7} - 1$.

[Note that if $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$ is a polynomial with roots $\alpha_1, \dots, \alpha_n$, so that
$$f(x) = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n),$$
then $-\sum_{j=1}^{n} \alpha_j = a_1$, $\sum_{j<k} \alpha_j \alpha_k = a_2$,
$-\sum_{j<k<l} \alpha_j \alpha_k \alpha_l = a_3, \dots, (-1)^n \alpha_1\alpha_2 \dots \alpha_n = a_n$]

Since the coefficient of z^6 in z^7+1 is 0,
we get $2\cos\frac{\pi}{7} + 2\cos\frac{3\pi}{7} + 2\cos\frac{5\pi}{7} = -1$.
Now $\cos\frac{5\pi}{7} = \cos\left(\pi - \frac{2\pi}{7}\right) = -\cos\frac{2\pi}{7}$.
Hence $\cos\frac{\pi}{7} - \cos\frac{2\pi}{7} + \cos\frac{3\pi}{7} = 1/2$,
as claimed.

[This solution is systematic and avoids any hard calculation. A slicker version is to note that

$$z^7+1=(z+1)(z^6-z^5+z^4-z^3+z^2-z+1)$$

and that

$$\frac{1}{z^3}(z^6-z^5+z^4-z^3+z^2-z+1)$$

$$=\left(z^3+\frac{1}{z^3}\right)-\left(z^2+\frac{1}{z^2}\right)+\left(z+\frac{1}{z}\right)-1$$

and putting $z=\cos\frac{\pi}{7}+i\sin\frac{\pi}{7}$, we get

$$2\cos\frac{3\pi}{7}-2\cos\frac{2\pi}{7}+2\cos\frac{\pi}{7}-1.$$

This must be zero since $z^7=\cos\pi+i\sin\pi=-1$ so $z^7+1=0$ and $z+1\neq 0$.]

3. The result is obvious for $p\le n$, since then p divides $n!$, for $p=2017$, a prime. Suppose $p>n$ and that p does not divide a_0. Consider $f(x)$ ~~mod~~ p — ~~that~~ is, we regard each coefficient a_i mod p as $r_i\in\mathbb{Z}_p=\{0,1,2,\dots,p-1\}$, where a_i leaves remainder r_i on division by p. Now setting $x=j$ $(0\le j<p)$, $f(j)$ is divisible by p and this says that over $\mathbb{Z}_p$, $f(j)=0$. But $\mathbb{Z}_p$ is a field, so $x-j$ is a factor of $f(x)$ over $\mathbb{Z}_p$. Now, since $a_0\neq 0$ in $\mathbb{Z}_p$, $f(x)$ over $\mathbb{Z}_p$ has degree n and has p roots $(0,1,2,\dots,p-1)$

But over a field, $f(x)$ cannot have more roots than its degree. Since $n < p$, we have a contradiction.
So p divides a_0. If any coefficient a_j is not divisible by p, let j_0 be the least j for which a_0 is not divisible by p and then mod p, $f(x) = a_{j_0}x^{n-j_0}$ $+ a_{j_1}x^{n-j_0-1} + \cdots + a_n$ (read mod p), and we get that p divides a_{j_0}, as we did for a_0. Hence if $n < p$, all coefficients of $f(x)$ are divisible by p.

[Note. For x a positive integer, the binomial coefficient $\binom{x}{n}$ is an integer as it is the number of ways to pick a team of n players from x players (So $\binom{x}{n} = 0$ if x is a positive integer less than n). Check that $\binom{x}{n}$ is an integer for every integer x (where $\binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!}$].

4. Suppose first $p=2$. Then $a_1=1$, $a_2=3$ and $a_1+a_3=4$. So only one sum has the desired property.

Suppose $p>2$.

The numbers $a_1, a_2, \ldots, a_k$ are the integers between 1 and p^2 not divisible by p.

The come in sequence of length $p-1$

$$a_1=1,\ a_2=2,\ \ldots,\ a_{p-1}=p-1,$$
$$a_p=p+1,\ a_{p+1}=p+2,\ \ldots a_{2(p-1)}=2p-1,$$
$$a_{2(p-1)+1}=2p+1,\ a_{2p}=2p+2,\ \ldots,\ a_{3(p-1)}=3p-1,$$
$$a_{3(p-1)+1}=3p+1,\ \ldots\ldots\ a_{p(p-1)}=p^2-1,$$

$k=p^2-p$ and

The sum of the integers $1, 2, \ldots, l$ is $\frac{l(l+1)}{2}$ and if $1 \le l < p-1$, this sum is not divisible by p, while for $l=p-1$, the sum is $\frac{p(p-1)}{2}$ which is divisible by p since p is odd.

In order that $a_1+\cdots+a_r$ be divisible by p^2, it must be divisible by p and since the sum of the numbers in each sequence of length $p-1$ is divisible by p

and, for $1 \le l \le p-1$, the sum of [58]

$pa+1, pa+2, \ldots, pa+l$ is

not divisible by p, if a is an integer. Hence r must be $m(p-1)$ for some integer m with $2 \le m \le p$.

To sum all the terms in the first m sequences, one observes that the sum $1+2+\cdots+p-1$ occurs m times, giving $\frac{m\,p(p-1)}{2}$. The rest comes from the multiples of p attaches to each a_i. In the first sequence, there are zero. In the second there are $p-1$, in the third $2(p-1)$, $\ldots$, in the mth: $(m-1)(p-1)$. The contribution of those is $p(p-1)(1+2+\cdots+(m-1))$

$$= p(p-1)\frac{m(m-1)}{2}.$$

So $a_1 + \cdots + a_{m(p-1)} = \frac{mp(p-1)}{2} + \frac{p(p-1)m(m-1)}{2}.$

For this to be divisible by p^2, we require that p divide m^2. But $m \le p$. Hence $m = p$ and their is only one such r.