Polynomials

Rohan Goyal

February 27, 2021

§0

Introduction

In this handout, I hope to cover most of what can come up in polynomials in olympiads and introduce various ideas. As we will go over a comprehensive set of things, there are a few minor prerequisites[1]-

- What a polynomial is
- Knowing what complex numbers are and basic things like conjugates of complex numbers.
- Vieta's formulas
- Triangle Inequality
- Differentiation(Being able to differentiate polynomials and know some rules like Product Rule)
- Intermediate Value Theorem
- Mean Value Theorem
- For section on Integer polynomials, we will also assume comfort with modular arithmetic and working in $\mathbb{F}_p$.

In case you are not familiar with what any of these mean or what they are, I encourage you to just google them and then come back to the document.

We will also assume fundamental theorem of algebra without proof.

Theorem (Fundamental Theorem of Algebra)
Every single-variate polynomial with complex coeffiecients has atleast 1 complex root.

Corollary
Every single-variate complex polynomial of degree n has exactly n roots when counted with multiplicity.

[1] Hopefully nothing outside standard school syllabus

Notation

- Throughout the handout, "polynomial" refers to a single variable polynomial unless stated otherwise.
- $\exists$ stands for "there exists" or "exists".
- $\in$ refers to "in".
- $\forall$ stands for "for all".
- $\mathbb{N}$ refers to the set of naturals.
- $\mathbb{N}_0$ refers to the set of whole numbers.
- $\mathbb{Z}$ refers to the set of integers.
- $\mathbb{Q}$ refers to the set of rationals.
- $\mathbb{R}$ refers to the set of reals.
- $\mathbb{C}$ refers to the set of complex numbers.
- $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ refer to the set of single variate polynomials with integer, rational, real and complex coefficients respectively.
- $a|b$ means a divides b.
- $\mathbb{F}_p$ refers to the field mod p(prime), i.e. the residue class $\{0, 1, 2, \cdots p-1\} \pmod p$
- WLOG stands for "Without loss of generality"
- FTSOC stands for "For the sake of contradiction"

Contents

§1 Intro to Real Polynomials

A lot of the problems we face in olympiads about polynomials revolve around real polynomials so we start with them!

§1.1 Factorization and Complex Conjugates

By the fundamental theorem of arithmetic, we have the very powerful tool that lets us pick roots for any complex polynomial but we can talk slightly more about what these roots are for real polynomials.

Theorem 1.1

If α is a complex root with non trivial imaginary part of $P \in \mathbb{R}[x]$ then so is $\overline{\alpha}$ and $\alpha, \overline{\alpha}$ have the same multiplicity.

Proof. We know that $\overline{P(\alpha)} = P(\overline{\alpha})$ but if α is a root then $\overline{0} = 0 \implies P(\overline{\alpha}) = 0$. But $(x-\alpha)^k(x-\overline{\alpha})^k$ is a real polynomial $\forall k \in \mathbb{N}$. Now, if $\alpha, \overline{\alpha}$ have different multiplicities then let $P(x) = (x-\alpha)^{k_1}(x-\overline{\alpha})^{k_2}Q(x)$ and $Q(x) \in \mathbb{R}[x]$ where $Q(\alpha) \neq 0$ and WLOG $k_1 > k_2$.
Observe that $R = \frac{P}{(x-\alpha)^{k_2}(x-\overline{\alpha})^{k_2}}$ is a real polynomial with root α but not $\overline{\alpha}$. Contradiction!

Thus, α and $\overline{\alpha}$ have equal multiplicities. □

The following two immediate corollaries are left as exercises.

Corollary 1.2

If P is a real polynomial with odd degree then it has atleast 1 real root.

Corollary 1.3

Every real polyomial can be written as a product of real linear and quadratic factors.

Now, equipped with this knowledge let's try a problem.

Example 1.4 (Putnam)

$P(x) \geq 0 \forall x \in \mathbb{R}$, P.T., $\exists g, h$ such that $P = g^2 + h^2$ where $P, g, h \in \mathbb{R}[x]$

Sketch. First observe that no real factor of P occurs with odd multiplicity. Now, let $p = Q^2R$ where R has no real roots.
Now, remember that by 1.3, $R = q_1q_2 \cdots q_k$ where q_i are all quadratic real factors. Now, we can write each $q_i = a_i^2 + b_i^2$ and by using the identity that $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$, we can write R as a sum of two squares. Let $R = r_1^2 + r_2^2$. Now, $g = r_1Q$ and $h = r_2Q$ works.

□

Exercise 1.5 (USAMO 1975/3)**.** If $P(x)$ denotes a polynomial of degree n such that $P(k) = \frac{k}{k+1}$ for $k = 0, 1, 2, \ldots, n$, determine $P(n+1)$.

§1.2 Size of Roots

Now, we move onto another very important consideration which is the size of factors and/or the size of the output.

Example 1.6 (Taiwan)
Find all polynomials P such that $P(x)P(x+2) = P(x^2)$

The structure here is such that it directly motivates us to look at roots as we are able to generate new roots from existing roots. i.e if α is a root of $P(x)$, then $P(\alpha^2) = 0$ and thus α^2 is also a root and similarly, $(\alpha-2)^2$ is also a root.

Now, if we consider any root of P other than 1. Now, if $|\alpha| \leq 1$ then $|\alpha - 2|^2 > 1 \geq |\alpha|$ and if $|\alpha| > 1 \implies |\alpha|^2 > |\alpha| > 1$. Thus, for any root other than 1, we can generate a root with modulus larger than itself and 1.
So, this suggests that we should be able to generately arbitrarily large roots and in fact we can. As there must be finitely many roots of P other than 1, now consider the one with the largest modulus among these roots. But by our previous claim, we can generate another root with larger modulus and we get a contradiction! Thus, if P is not the 0 polynomial then it can only have root 1. Thus, we can let $P = k(x-1)^n$.

Now, $P(x)P(x+2) = k^2(x^2-1)^n = k(x^2-1)^n \iff k \in \{0,1\}$. Thus, $\boxed{P(x) \equiv (x-1)^n}$ and $\boxed{P(x) \equiv 0}$ are the only solutions. You can easily recheck them as well. □

For a problem of a similar taste, try the following problem-

Problem 1.7 (INMO 2018)**.** Find all polynomials with real coefficients $P(x)$ such that $P(x^2+x+1)$ divides $P(x^3-1)$.

For solution check 9

§1.3 Differentiation and Double Roots

This idea revolves around one key theorem that makes differentiation a very powerful idea for working with polynomials.

Theorem 1.8
For $P \in \mathbb{C}[x]$, α is a double root of P iff α is a root of $P'(x)$ and $P(x)$.

Try proving it on your own!

With this, we try the following problems.

Example 1.9 (Putnam 1956)
Let $P, Q \in \mathbb{C}[x]$ such that P and Q have the same set of roots with possibly different multiplicities. Suppose that $P+1, Q+1$ also have the same set of roots with possibly different multiplicities. Prove that $P = Q$.

First begin by noting that

WLOG, $\deg P \geq \deg Q$.

Let the two sets of roots be S_1, S_2 and S_1, S_2 are disjoint.

If α is a root of P with multipicity m then it is a root with multiplicity $m-1$ of P'. Similarly, we get for $P+1$. Thus, P' has degree atleast

$$2\deg P - |S_1| - |S_2| \leq \deg P' = \deg P - 1 \implies \deg P + 1 \leq |S_1| + |S_2| \implies |S_1| + |S_2| > \deg P$$

.
But, S_1, S_2 are also the set of roots of $P-Q$ which has degree $\leq \deg P$ which is a contradiction unless $P-Q$ is the zero polynomial. Thus, $P=Q$.

This is a very simple yet instructive example on the power of differentiation on polynomials and the control over repeated roots it gives us.

Now, try the following slightly harder problem!

Exercise 1.10 (LMAO Senior 2020/2)**.** P is a degree m complex polynomial such that $P(0) \neq 0$. Prove that there exists a rational number c, such that for all positive integers k, there are precisely $\lceil cm^k \rceil$ distinct complex roots of the polynomial $\underbrace{P(P(\cdots P(x)\cdots))}_{k \text{ times}}$.

You can find the official solution in the selected solutions at 9

§1.4 Symmetric Polynomials

We first introduce symmetric polynomials.

Definition 1.11. Let $P(x_1, x_2, \cdots x_n)$ be a polynomial in n variables. We say P is symmetric if $\forall \tau \in S_n$[2]

$$P(x_1, x_2, \cdots x_n) = P(x_{\tau(1)}, x_{\tau(2)}, \cdots, x_{\tau(n)})$$

i.e. A symmetric polynomial is a polynomial that is not influenced by the ordering of the variables and is thus symmetric in all its variables.

Now, we move onto the main dish. Let $x_1, x_2, \cdots x_n$ be numbers and let σ_i be the sum of the products of these terms taken i at a time. For example,

$$\sigma_1 = \sum_{1 \leq i \leq n} x_i$$

$$\sigma_2 = \sum_{1 \leq i < j \leq n} x_i x_j$$

and so on till $\sigma_n = x_1 x_2 \cdots x_n$.
Now, we have the very strong fundamental theorem of symmetric polynomials!

Theorem 1.12 (Fundamental Theorem of Symmetric Polynomials)
Any symmetric polynomial $P(x_1, x_2 \cdots, x_n)$ can be written as

$$P(x_1, x_2, \cdots x_n) = Q(\sigma_1, \sigma_2, \cdots \sigma_n)$$

where Q is unique. in fact if P has integer, rational or real coefficients then so does Q.

Try proving this on your own!

[2] S_n is the set of all permutations of $\{1, 2, \cdots n\}$.

Example 1.13

Let α be a root of a monic integer polynomial P and β be a root of a monic integer polynomial Q. Prove that-

- $\alpha\beta$ is also a root of some monic integer polynomial.
- $\alpha+\beta$ is also a root of some monic integer polynomial.

Also prove the result for rational polynomials instead of integer.

We are not going into much depth into symmetric polynomials but if you want to see some important results, you can read up on *Brilliant* or *Wikipedia*.

§1.5 Lagrange Interpolation

Lagrange Interpolation is a very strong result that gives us a method to create polynomials according to some conditions we wish to satisfy. It's extremely powerful and will often also come up in future sections.

Theorem 1.14 (Lagrange Interpolation)

If $x_1 < x_2 < \cdots x_{n+1}$ are complex numbers and $a_1, a_2, \cdots a_{n+1}$ are some other complex numbers then there exists a unique polynomial P of degree atmost n such that $P(x_i) = a_i$.

In fact, we will find an explicit formula for P and prove uniqueness afterwards
First observe, that if we can instead define, $n+1$ polynomials P_i such that

$$P_i(x_j) = \begin{cases} 0, & i \neq j \\ a_i, & i = j \end{cases}$$

then $P = \sum_{i=1}^{n+1} P_i$ works.

But, we can let $P_i = a_i \dfrac{\prod_{1\leq j\leq n, i\neq j}(x-a_j)}{\prod_{1\leq j\leq n+1, i\neq j}(a_i-a_j)}$ and this works.

Now, we prove uniqueness, let Q be another polynomial that works. Then, $P-Q \neq 0$ has $n+1$ roots but degree atmost n which is impossible.

Remark 1.15. This type of construction where you set up each part individually and then sum over all is actually quite commonplace as it's the same construction we often use for Chinese Remainder Theorem and similar construction ideas will come up again throughout the handout.

§1.6 Problem set for real polynomials

[3]

Problem 1.16. Prove all above given theorems and corollaries which do not have proof attached.

Problem 1.17. Try the exercises.

Problem 1.18. A polynomial of degree n takes rationals to rationals on $n+1$ points. Prove that it is a rational polynomial. Soln: 9

Problem 1.19 (USAMO 2002/3)**.** Prove that any monic polynomial (a polynomial with leading coefficient 1) of degree n with real coefficients is the average of two monic polynomials of degree n with n real roots.

Problem 1.20 (Putnam 1968)**.** For each positive integer $n \geq 1$, determine all monic polynomials of degree n whose roots are all real, for which every coefficient is either 1 or -1.

Problem 1.21. If $p, q \in \mathbb{R}[x]$ satisfy $p(p(x)) = q(x)^2$, does it follow that $p(x) = r(x)^2$ for some $r \in \mathbb{R}[x]$?

Problem 1.22 (ISL 2019 A5)**.** Let $x_1, x_2, \ldots, x_n$ be different real numbers. Prove that

$$\sum_{1 \leqslant i \leqslant n} \prod_{j \neq i} \frac{1 - x_i x_j}{x_i - x_j} = \begin{cases} 0, & \text{if } n \text{ is even;} \\ 1, & \text{if } n \text{ is odd.} \end{cases}$$

Problem 1.23 (RMM 2018/2)**.** Determine whether there exist non-constant polynomials $P(x)$ and $Q(x)$ with real coefficients satisfying

$$P(x)^{10} + P(x)^9 = Q(x)^{21} + Q(x)^{20}.$$

Soln: 9

Problem 1.24 (USAMO 2019/6)**.** Find all polynomials P with real coefficients such that

$$\frac{P(x)}{yz} + \frac{P(y)}{zx} + \frac{P(z)}{xy} = P(x-y) + P(y-z) + P(z-x)$$

holds for all nonzero real numbers x, y, z satisfying $2xyz = x + y + z$.

Problem 1.25 (Iran Round 3 A3)**.** We are given a natural number d. Find all open intervals of maximum length $I \subseteq R$ such that for all real numbers $a_0, a_1, \cdots a_{2d-1}$ inside interval I, we have the polynomial $P(x) = x^{2d} + a_{2d-1}x^{2d-1} + \cdots a_0$ has no real roots.

Problem 1.26 (RMMSL 2018 A1)**.** Let m and n be integers greater than 2, and let A and B be non-constant polynomials with complex coefficients, at least one of which has a degree greater than 1. Prove that if the degree of the polynomial $A^m - B^n$ is less than $\min(m, n)$, then $A^m = B^n$.

[3] If anyone could tell me the sources of the problems for which I have not mentioned source, I will update them so please let me know.

§2 Integer and Polynomials

Now, we move on to integer and rational polynomials!
The first idea we see in integer polynomials is already quite powerful and motivates a lot of the ideas we use.

§2.1 $a-b|P(a)-P(b)$

Theorem 2.1
If $P \in \mathbb{Z}[x]$, and $a \neq b \in \mathbb{Z}$ then $a-b|P(a)-P(b)$

This proof is actually quite direct and you should try on your own as you can just consider individual terms and conclude.

Proof. Let $P = a_n x^n + a_{n-1}x^{n-1} + \cdots$.
First observe that $\forall i \in \mathbb{N}, a-b|a^i-b^i \implies a-b|a_i(a^i-b^i) \implies$
$a-b|\sum_{i=1}^{n} a_i(a^i-b^i) \implies a-b|\sum_{i=1}^{n} a_i a^i + a_0 - \sum_{i=1}^{n} a_i b^i - a_0 \implies a-b|P(a)-P(b)$ □

With just this in our toolbox, we are already equipped to handle many interesting results and hard problems.

Lemma 2.2 (Classic)
For some $P \in \mathbb{Z}[x]$, $\exists a, k \in \mathbb{N}$ such that $P^k(a) = a$, then prove that $P^2(a) = a$.

This means that if there is a cycle in an integer polynomial then it has cycle length 1 or 2.

Proof. For $k = 1$ or $k = 2$, result is direct so let's consider $k > 2$. Now FTSOC, consider smallest k which can be a cycle, we have

$$P(a)-a|P^2(a)-P(a) \mid P^3(a)-P^2(a) \mid \cdots |a-P^{k-1}(a) \mid P(a)-a$$

Thus, for all i, $\frac{P^{i+1}(a)-P^i(a)}{P^i(a)-P^{i-1}(a)} \in \{-1,1\}$ but if it is -1, then we get that $P^{i+1}(a) = P^{i-1}(a)$, and that is a contradiction as this is a 2 cycle.
Thus, $P^{i+1}(a)-P^i(a) = P(a)-a \implies P^k(a) = a + (k-1)(P(a)-a) \neq a$ which is a contradiction as well and thus we are done.

□

With this toolbox, we will now take an IMO 5!

Example 2.3 (IMO 2006/5)
Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial $Q(x) = P(P(\ldots P(P(x))\ldots))$, where P occurs k times. Prove that there are at most n integers t such that $Q(t) = t$.

Proof. By the previous result, we have that all periods are of length 1 or 2.
First, we assume that there is atleast one term b such that it is not a fixed point but $Q(b) = b$
Now if some other term a is not a fixed point but $Q(a) = a$ then let us consider $a, P(a)$ and $b, P(b)$ with WLOG $P(a) > a$ and $P(b) > b$ and $a > b$.
Now, if $P(a) > P(b)$, then $P(b) - a | P(a) - b \implies |P(b) - a| < |P(a) - b|$ but this is impossible. Now, if $P(a) < P(b)$, we get $P(b) - a | P(a) - b \implies P(a) + a = P(b) + b$.
Now, if a is a fixed point then $P(b) - a | b - a | P(b) - a$ but b is not a fixed point, thus $P(b) - a = a - b \implies a + P(a) = b + P(b)$.
So, all roots of $Q(x) = x$ are also roots of $P(x) + x = P(b) + b$ but this is an n degree polynomial. Thus, there atmost n solutions.
Now, if there are no 2 cyles then $P(x) = x$ has again atmost n solutions as it is an n degree polynomial!

□

Remark 2.4. It is worth noting that the condition $\deg P > 1$ is crucial as otherwise it's possible that if there are $> n$ solutions then we must have $P(x) + x$ as a constant polynomial or the simple identity polynomial $P(x) = x$. Thus, $P(x) = c - x$ is always an involution. But this is not true for our current problem as we are given that $\deg P > 1$.

This idea is clearly very powerful as it also now lets us talk about roots $\pmod n$ as if $n | P(x)$ then $n | P(x + kn)$ and we can simply talk about the congruency class. This is especially powerful for prime n.

§2.2 Size Considerations and picking large prime divisors

Size is clearly an idea that frequently occurs in polynomials, and it occurs in integer polynomials as one of the nicest properties of polynomials is that they get arbitrarily large and take on a lot of prime divisors. With that we prove our first result. Schur's theorem and present two different proofs both involving some sort of size idea.

For any polynomial $P \in \mathbb{Z}[x]$, define S_P as the set of primes p for which exists $a \in \mathbb{Z}$ such that $p | P(a)$.

Theorem 2.5 (Schur's theorem)
S_P is infinitely large.

Proof 1. FTSOC, S_P is finite. Let $S_P = \{p_1, p_2, \cdots p_k\}$. Now, observe that $P(0) \neq 0$ as $\forall$ q prime, we have $q | 0$.
Now, let $a_i = v_{p_i}(P(0))$.
We now consider $N = \prod_{i=1}^{k} p_i^{a_i+1}$. Now, for $P(mN)$, we have $v_{p_i}(P(mN)) = a_i$ and these are the only primes that divide $P(mN)$. Thus, $P(mN) = P(0)$ but m is arbitrary, thus $P(x) - P(0)$ has infinitely many roots, which is impossible.
We can get the same contradiction by claiming that this implies that $P(mN)$ is bounded but that is not possible for polynomials.□
Proof 2. This proof is of an analytical flavour. Observe that P takes $\Theta(N^{\frac{1}{\deg P}})$[4] values

[4]This is asymptotic notation, basically meaning that the functionn grows at roughly that pace wrt N. You can google "big-O notation " to get a clearer idea

less than N but if the set of prime factors is $\{p_1, p_2, \cdots p_k\}$ then the numbers less than N which have only these prime factors are less than $\Theta((\log N)^k)$ but any $\Theta((\log N)^k)$ function is eventually smaller than $\Theta(N^{\frac{1}{a}})$.□

Schur's now gives us a very powerful tool of finding arbitrary large prime divisors and its two proofs also introduce two very important ideas.

Let's now a problem that use Schur's theorem.

Example 2.6 (IberoAmerican 2019/6)

Let $a_1, a_2, \ldots, a_{2019}$ be positive integers and P a polynomial with integer coefficients such that, for every positive integer n,

$$P(n) \text{ divides } a_1^n + a_2^n + \cdots + a_{2019}^n.$$

Prove that P is a constant polynomial.

Looking at the problem, we have 2 very good reasons to look at prime divisors of P.

- It's an integer polynomial and we want degree 0.
- The given condition is a divisibility condition.

So, FTSOC, let's assume that P is non constant. Now, let's pick a very large prime divisor of P, let it be p. Now, let $p \mid P(n)$ but then $p \mid P(n+pk)$. Now, we look at the exponentials, right now we have no control yet over there values but because of Fermat's little theorem, if we get that if $p-1|m$ and $p|m-n$, we will need that $p|2019$ but because we can pick large p, we can simply pick a $p > 2019$ and $p > a_1, a_2, \cdots$ but as p and $p-1$ are co-prime, there is some m which satisfies

$$m \equiv 0 \pmod{p-1}, m \equiv n \pmod{p}$$

and we will be done.

There is a slight loophole here that we skipped! We might have that $p|a_i$ for all a_i but as we can make p arbitrarily large, we simply pick a prime greater than all a_i and 2019.

Thus, P is constant! □

§2.3 More work with primes

Building upon the previous trick, we try a few more problems.

Exercise 2.7 (STEMS 2021 Maths Category B)**.** Determine all non-constant monic polynomials $P(x)$ with integer coefficients such that no prime $p > 10^{100}$ divides any number of the form $P(2^n)$. Soln: 9

Example 2.8 (STEMS 2019)

Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be a polynomial such that $a_0, a_1, \ldots, a_n$ are all positive integers. Let $P_1(x) = P(x)$ and for each $k > 1$ define the polynomial $P_k(x) = P(P_{k-1}(x))$. Does there exist an $M > 0$ such that for all $m \geq M$ we have $m|P_{P(m)}(m)$?

The following proof is by Pranjal Srivastava.

Proof. Let $f(m)$ be the minimal natural such that $m|P_{f(m)}(0)$.
Observe that $f(m)|f(km)$ and $f(m)|P(m)$.
So $f(m)|P(mf(m))$ or $f(m)|P(0)$.

□

Exercise 2.9 (Iran)**.** $P(x)$ is a nonzero polynomial with integer coefficients. Prove that there exists infinitely many prime numbers q such that for some natural number n, $q|2^n + P(n)$.

§2.4 Euclidean Division

We can talk about Euclidean Division and use division algorithms with polynomials as well. We can also talk about the GCD of polynomials! in fact, we have the following results-

Theorem 2.10 (GCD)
If we have two polynomials $P, Q \in \mathbb{Q}[x]$, their GCD is also a rational polynomial.

Proof. WLOG, let $\deg P \geq \deg Q$. Now, we can apply Euclidean division algorithm to get $P = QS + R$ where S and R are also rational polynomials where $\deg R < \deg Q$. If R is the zero polynomial then we get that $\gcd(P, Q) = Q$. If not then observe that $\gcd(P, Q) = \gcd(Q, R)$ and the degrees are reduced. Thus, we can keep repeating the procedure and eventually get a rational polynomial as the gcd. □

Similarly, we can do the same for monic integer polynomials. Then, we in fact have that the gcd is also a monic integer polynomial. We leave this as an exercise.

Exercise 2.11. If P, Q are monic integer polynomials then $\gcd(P, Q)$ is also a monic integer polynomial.

Now, we remember the famous theorem relating to gcd in NT. Bezout's theorem!

Theorem 2.12 (Bezout's theorem)
If two rational polynomials P, Q have $\gcd D$, then there are rational polynomial R, S such that

$$PR - QS = D$$

You can try proving this on your own as you replicate the proof of normal Bezout's construction by going backward from the Euclidean Division.

Lets try a problem relating to Euclidean Division now.

Example 2.13 (EGMO 2013/4)
Find all positive integers a and b for which there are three consecutive integers at which the polynomial

$$P(n) = \frac{n^5 + a}{b}$$

takes integer values.

The following write-up is by Aditya Khurmi.

Proof. We claim that the solutions are $(a, b) = (k, 1), (l, 11)$, where k is any integer and l is any integer such that $11|l \pm 1$. These work, and now we will show that these are the only solutions.

Firstly assume $b > 1$, and say that $P(n-1), P(n), P(n+1) \in \mathbb{Z}$. Then

$$P(n+1)+P(n-1)-2P(n)\in\mathbb{Z} \implies b|20n^3+10n \tag{1}$$
$$P(n+1)-P(n-1)\in\mathbb{Z} \implies b|10n^4+20n^2+2 \tag{2}$$

Hence, $b|2(10n^4+20n^2+2)-n(20n^3+10n)=30n^2+4$ and $b|2n(30n^2+4)-3(20n^3+10n)=-22n$. Thus, $b|22n$, which we will refer to as (3).

Claim: If $p|b$, then $p=11$. Further, $v_{11}(b)\leq 1$ Proof: If $p=2$, then $2|n^5+a$ and $2|(n+1)^5+a$ which implies $2|(n+1)^5-n^5$, which is not possible.

Next assume $p>2$. Then we must have $p\nmid 2n$, otherwise (2) $\implies p|2$, absurd. So $p\nmid 2n, p|22n \implies p=11$ Now $11\nmid 2n \implies 11\nmid n$ and so $v_{11}(b)\leq v_{11}(22n)=1$, and the claim has been proven. □ Thus, $b=11$ as $b>1$ by our assumption. Now we have proven that $11\nmid n$ and so (1) $\implies 11|2n^2+1$. Thus $n^2\equiv 5 \Leftrightarrow n\in\{4,7\} \pmod{11}$. Now since $(4-1)^5\equiv 4^5\equiv(4+1)^5\equiv 1 \pmod{11}$ as well as $(7-1)^5\equiv 7^5\equiv(7+1)^5\equiv -1 \pmod{11}$, hence the solutions are indeed the claimed ones. ■ □

§2.5 Constructions

Now, we move onto constructions in integer polynomials! As we have already seen many ideas, let's dive right into problems!

Example 2.14 (USA EGMO TST 2020/6)
Find the largest integer $N \in \{1, 2, \ldots, 2019\}$ such that there exists a polynomial $P(x)$ with integer coefficients satisfying the following property: for each positive integer k, $P^k(0)$ is divisible by 2020 if and only if k is divisible by N. Here P^k means P applied k times, so $P^1(0) = P(0), P^2(0) = P(P(0))$, etc.

This problem is very neat as it basically calls upon us to construct polynomials with cycle lengths $\pmod p$.

Proof. First let's consider period of $0 \pmod 4$ as P_4, period of $0 \pmod 5$ as P_5 and $0 \pmod{101}$ as P_{101}. Here, period $\pmod n$ refers to smallest k such that $n|P^k(0)$ and similar notation will be used throughout. So, we have $P_4 \leq 4, P_5 \leq 5, P_{101} \leq 101$ and the desired $P_{2020} = lcm(P_4, P_5, P_{101})$. This is clearly maximized at $(4, 5, 99)$ so the desired maxima is 1980. Now, we need to show that we can in fact set up a polynomial with the claimed periods.
First, we set up a rational polynomial Q_1 which satisfies: $Q_1(0) = 1, Q_1(1) = 2, \cdots Q_1(97) = 98, Q_1(98) = 0$. This, can be done by Lagrange interpolation. Now, in case any coefficient is of the form $\frac{p}{q}$, we replace $\frac{1}{q}$ with the inverse mod 101 of q and get an integer polynomial, now multiply this polynomial with 20^{100}. Call this new polynomial R_1. R_1 has cycle length 99 mod 101 as our changes to it did not change anything mod 101 as $20^{100} \equiv 1 \pmod{101}$ and R_1 is always $0 \pmod{20}$.
Similarly, we set up $R_2(x) = 404^4(x + 1)$ and $R_3(x) = 505^2(x + 1)$.
Now, observe that $R_1 + R_2 + R_3$ satisfies the conditions we wanted.
Thus, we are done as $\boxed{N = 1980}$. □

Remark (On the construction)**.** In fact, the idea to construct such polynomials generalizes as expected.
In case, we wish to find a polynomial which has cycle lengths $c_1, c_2, \cdots c_n \pmod{p_1, p_2, \cdots p_n}$ respectively. We can set it up as
Let $M = p_1 p_2 \cdots p_n$
Q_i be a rational polynomial such that $Q_i(0) = 1, Q_i(1) = 2, \cdots Q(i) = c_i - 1, Q_i(c_i) = 0$ and now replace any rationals with their corresponding values mod p_i and call this P_i. Now, let $R_i = \left(\frac{M}{p_i}\right)^{p_i - 1} P_i$.
Now, the desired polynomial is $\sum R_i$.
Again you can do this for prime powers as well but there are some conditions on cycle lengths that are too tedious to write up for now.

Remark. This construction is directly motivated by the types of constructions we did before for Lagrange Interpolation as we set up polynomials for each part and then add them.

We now look at another polynomial problem with a different kind of construction idea.

Example 2.15 (APMO 2020/4)

Let $\mathbb{Z}$ denote the set of all integers. Find all polynomials $P(x)$ with integer coefficients that satisfy the following property:

For any infinite sequence $a_1, a_2, \ldots$ of integers in which each integer in $\mathbb{Z}$ appears exactly once, there exist indices $i < j$ and an integer k such that $a_i + a_{i+1} + \cdots + a_j = P(k)$.

As the part of our interest is constructions, we leave proving that all linear polynomials work to the reader and only try to show that polynomials with $\deg P \geq 2$ do not work. The idea now is $P(x+1) - P(x)$ gets arbitrary large as x gets large as it is also an $\deg P - 1$ polynomial.

Proof. We will construct a sequence now, that doesn't work. First, pick $a_1 = 1$. Now, in every step, we will define a sequence up till a_{2n-1}(for $n = 1$, we have defined the sequence), then pick a_{2n+1} to be the number with smallest modulus not yet picked and then we will pick a_{2n}. So, we start by picking $a_3 = 2$. Now, for a_{2n}, consider the sets of sums ending in a_{2n-1} with and without a_{2n+1}, as this is a finite set, let the smallest of these sums be s_1 and the largest be s_2. Now, consider a k such that $|P(k+1) - P(k)| > 2(|s_1| + |s_2|)$. Now, we can pick a_{2n} within this gap so adding any of the sums, our sum remains between $P(k)$ and $P(k+1)$.
We claim that this sequence works. FTSOC, assume it doesn't then consider the largest i for which a_{2i} is in the sequence. Now, by definiton of a_{2i}, this is a contradiction and we are done.

□

Equipped with these ideas, let's head into problems!

Remark. There is a fair bit of more theory to discuss in integer and rational polynomials but we discuss that in subsequent sections.

§2.6 Problems

Problem 2.16. Try the exercises.

Problem 2.17 (ELMO)**.** Big Bird has a polynomial P with integer coefficients such that n divides $P(2^n)$ for every positive integer n. Prove that Big Bird's polynomial must be the zero polynomial.

Problem 2.18 (Iran)**.** Find all polynomials $p \in \mathbb{Z}[x]$ such that $(m,n) = 1 \Rightarrow (p(m), p(n)) = 1$

Problem 2.19 (Poland)**.** Let $f(t) = t^3 + t$. Decide if there exist rational numbers x, y and positive integers m, n such that $xy = 3$ and:

$$\underbrace{f(f(\ldots f(f}_{m \text{ times}}(x))\ldots)) = \underbrace{f(f(\ldots f(f}_{n \text{ times}}(y))\ldots)).$$

Problem 2.20 (USATSTST 2018/1)**.** As usual, let $\mathbb{Z}[x]$ denote the set of single-variable polynomials in x with integer coefficients. Find all functions $\theta : \mathbb{Z}[x] \to \mathbb{Z}$ such that for any polynomials $p, q \in \mathbb{Z}[x]$, $\theta(p+1) = \theta(p) + 1$, and if $\theta(p) \neq 0$ then $\theta(p)$ divides $\theta(p \cdot q)$.

Problem 2.21. Let $f(x)$ be a monic polynomial of degree n with integer coefficients, and let $d_1, \cdots, d_n$ be pairwise distinct integers. Suppose that for infinitely many prime numbers p there exists an integer k_p for which $f(k_p + d_1) \equiv f(k_p + d_2) \equiv \cdots f(k_p + d_n) \equiv 0 \pmod{p}$. Prove that there exists an integer k_0 such that $f(k_0 + d_1) = f(k_0 + d_2) = \cdots = f(k_0 + d_n) = 0$

Problem 2.22. Suppose f is a polynomial in $\mathbb{Z}[X]$ and m is integer .Consider the sequence a_i like this $a_1 = m$ and $a_{i+1} = f(a_i)$ find all polynomials f and alll integers m that for each i:

$$a_i | a_{i+1}$$

Problem 2.23. There are $n > 2$ lamps arranged (evenly spaced) in a circle. Initially, one of them is turned on, and the rest are off. It is permitted to choose any regular polygon whose vertices are lamps and toggle all of their states simultaneously. For which positive integers n is it possible to turn all the lamps of after a finite number of such operations?

Problem 2.24 (USAMTS 4/3/29)**.** A positive integer is called uphill if the digits in its decimal representation form an increasing sequence from left to right. That is, a number $\overline{a_1 a_2 \cdots a_n}$ is uphill if $a_i \leq a_{i+1}$ for all i. For example, 123 and 114 are both uphill. Suppose a polynomial $P(x)$ with rational coefficients takes on an integer value for each uphill positive integer x. Is it necessarily true that $P(x)$ takes on an integer value for each integer x? Similarly define downhill integers, is it necessary now?

Problem 2.25 (USATST 2009/3)**.** For each positive integer n, let $c(n)$ be the largest real number such that

$$c(n) \leq \left| \frac{f(a) - f(b)}{a - b} \right|$$

for all triples (f, a, b) such that

–f is a polynomial of degree n taking integers to integers, and –a, b are integers with $f(a) \neq f(b)$.

Find $c(n)$.

Problem 2.26 (USATSTST 2016/3)**.** Decide whether or not there exists a nonconstant polynomial $Q(x)$ with integer coefficients with the following property: for every positive integer $n > 2$, the numbers

$$Q(0),\ Q(1), Q(2),\ \ldots,\ Q(n-1)$$

produce at most $0.499n$ distinct residues when taken modulo n. Soln: 9

§3 Some Theory and Definitions

As the next couple sections are more technical and more advanced, we will need some more definitions than we are currently equipped with. But, here we will only be using handwavy definitions and you can google or check in Napkin for more formal definitions.

- A **ring** is a set where you can add, subtract and multiply terms and has multiplicative identity "1" and additive identity "0". Multiplication and addition are commutative. For example, $\mathbb{Z}, \mathbb{R}[x], \mathbb{Z}[x], \mathbb{Z}/n\mathbb{Z}$ etc.
- A **field** is a set equipped with division as well except dividing with "0". Examples include, $\mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \mathbb{C}$ etc.
- A **unit** is any term with a multiplicative inverse, for example, anything in $\mathbb{R}$ with respect to $\mathbb{R}[x]$ is a unit.
- An **irreducible element** in a ring is anything that cannot be written as a product of two non-units for example, any linear polynomial in $\mathbb{Q}[x]$.
- A **Unique Factorization Domain (UFD)** is any ring in which every element has a unique factorization into irreducible elements upto multiplication by units and no two non zero elements multiply to 0. For example,
  - $\mathbb{Z}$ is a UFD, as the primes behave as irreducibles and ± 1 as units and no two non-zero things multiply to 0. Similarly, $\mathbb{R}[x]$ is a UFD and so are $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$.
  - $\mathbb{Z}/n\mathbb{Z}$ is not a ring for composite n but is in fact a field for n prime as for example, if $n = 6$, $2, 3$ multiply to 0, thus there are two non-zero elements multiplying to 0.
- A number α is an **Algebraic Integer** if $\exists\ P \in \mathbb{Z}[x]$ such that P is monic and $P(\alpha) = 0$.
- A number α is called an **Algebraic Number** if $\exists P \in \mathbb{Q}[x]$ such that $P(\alpha) = 0$.

It is worth noting that $\mathbb{R}[x_1, x_2, \cdots x_n]$ is also a UFD. in fact, if $\mathbb{R}$ is any UFD, then $\mathbb{R}[x_1, x_2, \cdots x_n]$ is also a UFD.

Now equipped with these definitions, we are ready to dive into the next sections.

§4 Irreducibility

> **Remark.** Here, often while talking about polynomials in $\mathbb{Z}[x]$, we will pretend that irreducibility means the product of two non constant factors even though constants like $2, 3$ etc are not units and thus things like $2x^2 - 4$ are not irreducible as they can be written as a product of 2 and $x^2 - 2$ both of which are non-units, but for the sake of comfort we will do this, even though it is not entirely correct to do so.

Now, we move onto the main content!

The following theorem by Gauss is very important as it introduces very important ideas for irreducibility over $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ and their interchangeability.

Theorem 4.1 (Gauss)
If $P \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}[x]$ then it is irreducible over $\mathbb{Q}[x]$.

Proof. FTSOC, let $P = g \cdot h$ where $g, h \in \mathbb{Q}[x]$. Now, we can write $gh = \frac{p_1 p_2}{n}$ where p_1 and p_2 are in $\mathbb{Z}[x]$ and n is some integer. Now, let p be a prime dividing n but not all the coefficients of either polynomial(else we could have already divided). Now, we reduce all coefficients mod p of both polynomials. Let the reduced polynomials be q_1 and q_2. Now, none of the coefficients of q_1 and q_2 are divisible by p. Let the leading coefficient of q_1 be a_1 and for q_2 be a_2. Now, $p | a_1 a_2$. Thus, it must divide atleast one of them. Contradiction!
Thus, n does not have any prime divisors and thus must be 1 so P can be written as a product of two integer polynomials. Contradiction! □

This is a very powerful tool for us!

§4.1 Irreducibility by working in $\mathbb{F}_p$

Let us begin with the most famous of all olympiad irreducibility criteria involving primes.

Theorem 4.2 (Eisenstein's Irreducibility Criterion)
Let $P = a_n x^n + a_{n-1} x^{n-1} + \cdots a_0 \in \mathbb{Z}[x]$ such that $p \nmid a_n$ and $p | a_0, a_1, a_2, \cdots a_{n-1}$ but $p^2 \nmid a_0$ then P is irreducible over $\mathbb{Z}[x]$ and thus $\mathbb{Q}[x]$.

Proof. We again repeat the idea as before. We can now consider $P = f \cdot g$ and consider both f and $g \pmod p$. Now, $x^n = fg \pmod P$ so we can say $f = x^i + pQ(x)$ and $g = x^{n-i} + p(R(x))$ for some polynomials Q, R. But, now constant term is given by $pQ(x) \cdot pR(x) = p^2 QR$ but the constant term is not divisible by 0. Contradiction! □

This is not just a very important theorem but also introduces the very nice idea of going $\pmod p$ and talking about what happens to the factors. A very famous example involving the criteria is the following IMO 1993 problem which is left as an exercise.

Exercise 4.3 (IMO 1993)**.** Show that $x^n + 5x^{n-1} + 3$ is irreducible over $\mathbb{Z}[x]$.

§4.2 Talking about Size

Lemma 4.4

Suppose P is an integer monic polynomial such that at most one of its roots has absolute value atleast one, then it is irreducible over $\mathbb{Q}[x]$ if $P(0) \neq 0$.

Proof. FTSOC, let us let $P = QR$. Now, seeing how the roots split, we can observe that for one of Q and R, all the roots must have modulus less than 1. But then its product of roots will be less than 1 and not an integer. This is not possible as by Gauss, we can assume that Q, R are integer monic polynomials. □

Let us consider one more example to drive the idea of size home.

Lemma 4.5

If $P(x) \in \mathbb{Z}$ is a polynomial then $\exists n \in \mathbb{Z}$ such that $P(x) - n$ is irreducible.

Proof. This lemma is very powerful and nice but introduces us to ideas involving size of things.
Let $P = a_k x^k + \cdots a_0$ and let n be such that the constant term of $P(x) - n$ is a very large prime. Now, let $P(x) - n = Q(x)R(x)$. But, now the constant terms of Q and R multiply to a prime so one of them must be ± 1. WLOG that is Q.
Now, the modulus of the product of roots of Q is 1 so there is atleast one root with modulus less than or equal to 1. Let it be α.
Now, $P(\alpha) - n = 0$ but $|P(\alpha)| = |n| \implies |n| \leq |a_1| + |a_2| + \cdots$ but we can make modulus of n arbitrary large by picking a large enough prime.

This idea of making size of something very large keeps on popping up everywhere in polynomials as they are many things we can think about with them and thus many things we can control.

Exercise 4.6 (Selmer)**.** For any $n \geq 2$, prove that $f(x) = x^n - x - 1$ is irreducible.

□

§4.3 More Criteria

Now, we will write a few more criteria but not prove them for now and the proofs are left as exercises(these are very doable so do try them).

Theorem 4.7 (Cohn's Criterion)

Assume that $b \geq 2$ is a natural number and $P(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is a polynomial such that $0 \leq a_i \leq b - 1$. If $P(b)$ is a prime number then $P(x)$ is irreducible in $\mathbb{Z}[x]$.

Theorem 4.8 (Perron's Criterion)
Suppose $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and $|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|$ and $a_0 \neq 0$ then P is irreducible.

Remark 4.9. Perron's criterion has a very neat size proof without appealing to Rouche's theorem and it can be found in Yufei Zhao's polynomials handout in case you are unable to prove it on your own

§4.4 Problems on Irreducibility

Problem 4.10. Try the exercises and theorems/lemmas given without proof.

Problem 4.11. Show that the cyclotomic polynomial[5] $\Phi_n(x)$ is irreducible $\forall n \in \mathbb{N}$.

Problem 4.12. For distinct integers $a_1, a_2, \cdots a_n$

$$(x - a_1)(x - a_2) \cdots (x - a_n) - 1$$

is irreducible over $\mathbb{Z}[x]$. Soln: 9

Problem 4.13 (ELMO 2012/3)**.** For co-prime m, n, $x^m - y^n$ is irreducible over the complex numbers. Soln: 9

Problem 4.14 (Romania 2003)**.** Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial over the ring of integer polynomials, such that $|f(0)|$ is not a perfect square. Prove that if the leading coefficient of f is 1 (the coefficient of the term having the highest degree in f) then $f(X^2)$ is also irreducible in the ring of integer polynomials.

Problem 4.15. For any odd prime p and k such that $(k, p) = 1$, $x^p - x - k$ is irreducible over the rationals.

Problem 4.16 (Japan 1999)**.** Prove that for all $n \in \mathbb{N}$,

$$(x^2 + 1)(x^2 + 2^2) \cdots (x^2 + n^2) + 1$$

is irreducible.

Problem 4.17 (China TST 2008/ Quiz 3)**.** Let $n > m > 1$ be odd integers, let $f(x) = x^n + x^m + x + 1$. Prove that $f(x)$ can't be expressed as the product of two polynomials having integer coefficients and positive degrees.

Remark. The China TST problem is extremely hard.

[5] You can skip this for now in case you don't know what cyclotomic polynomials are but they are defined later on in the miscelleanous section

§5 Fancier Integer Polynomials

Note. In this section, if I use the word polynomial, they refer to rational polynomials unless explicityly stated otherwise.

§5.1 Minimal Polynomials and Galois Conjugates

Definition 5.1. For any algebraic number α, define its minimal polynomial(upto scaling) as the rational polynomial of minimum degree such that $P(\alpha) = 0$.

Lemma 5.2
Minimal polynomials are irreducible.

Proof. Assume not, then FTSOC, $P = QR$, thus atleast one of Q and R has root α, and we would have found a smaller degree polynomial. Contradiction! □

Theorem 5.3
If $Q(x)$ is the minimal polynomial of an algebraic number α and $P(x) \in \mathbb{Q}[x]$ is such that $P(\alpha) = 0$, then $Q|P$.

Proof. Assume not, now perform Euclidean division. Thus, $P(x) = S(x)Q(x) + R(x) \implies R(\alpha) = 0$. But, $\deg R < \deg Q$ contradicting the minimality of degree of Q. Thus, $R = 0$. Thus, $Q|P$. □

Theorem 5.4
The set of algebraic numbers given by $\overline{Q}$ is a field.

Try proving this on your own! Hint: Remember the ideas discussed in Symmetric Polynomials!

Now, as we talked about Minimal Polynomials of Algebraic Numbers, we can do the same for Algebraic Integers.

Definition 5.5. Define the minimal polynomial P of an algebraic integer α to be the monic integer polynomial with $P(\alpha) = 0$

Theorem 5.6
The set of algebraic integers given by $\overline{Z}$ is a ring.

Remark. Observe that this is basically the same as 1.13.

Lemma 5.7 (Galois Conjugates)
If $P \in \mathbb{Q}[x]$ is an irreducible polynomial with roots α, β and there is some $Q \in \mathbb{Q}[x]$ such that $Q(\alpha) = 0$ then $Q(\beta) = 0$.

Proof. Observe that the minimal polynomial of α divides P but P is irreducible so P is the minimal polynomial of α. Thus, $P|Q$ but that implies Q has root β. □

The roots of an irreducible polynomial are thus called "Galois Conjugates" as now they always appear together like conjugates.

Lemma 5.8
Irreducible polynomials do not have double roots in $\mathbb{Q}[x]$.

Proof. Assume they do, then if α is a root of the polynomial P, and P is irreducible then P is the minimal polynomial of P. But now if α is a double root, then its also a root of $P'(x)$ which is a contradiction to P being a minimal polynomial. □

We look at a few more results, before moving onto problems.

§5.2 Rational Root Theorem and Rationals as Algebraic Integers

This is perhaps something I should have put in the previous section but well it's here now :)

Theorem 5.9
If a rational $\frac{p}{q}$ is a root of an integer polynomial $P = a_n x^n + \cdots a_0$, then $q|a_n$ and $p|a_0$.

Proof. Consider $v_q(P(\frac{p}{q}))$. In case $q \nmid a_n$ then it is $-n$ but then $P(\frac{p}{q}) \neq 0$, hence $q|a_n$. Similar idea gives $p|a_0$ □

Now, this a very nice result as it also implies that if a rational is an algebraic integer, then it must an integer.

Let's now prove an important theorem with just the ideas we have developed till now.

Example 5.10 (Niven's Theorem)
If $\cos(\frac{2p\pi}{q}) \in \mathbb{Q}$ for some rational $\frac{p}{q}$, then $\cos(\frac{2p\pi}{q}) \in \{\frac{1}{2}, \frac{-1}{2}, 1, -1, 0\}$

Proof. Observe that $e^{(\frac{2p\pi}{q})}$ is a root of $x^q - 1$ and $e^{-(\frac{2p\pi}{q})}$ a root of $x^q - 1$ as well. Thus, they are algebraic integers. Thus, $e^{(\frac{2p\pi}{q})} + e^{-(\frac{2p\pi}{q})} = 2\cos(\frac{2p\pi}{q})$ is an algebraic integer as well.
But, then as $\cos(\frac{2p\pi}{q})$ is rational, $2\cos(\frac{2p\pi}{q})$ is a rational which is an algebraic integer. Thus, it must be an integer and our result follows. □

Exercise 5.11 (INMO 2020/5)**.** Infinitely many equidistant parallel lines are drawn in the plane. A positive integer $n \geqslant 3$ is called frameable if it is possible to draw a regular polygon with n sides all whose vertices lie on these lines, and no line contains more than one vertex of the polygon.
(a) Show that $3, 4, 6$ are frameable.
(b) Show that any integer $n \geqslant 7$ is not frameable.
(c) Determine whether 5 is frameable.

§5.3 Some Solved Examples to make the idea clearer

Example 5.12 (Miklos Scweitzer 2015/5)
Let $n \geq 4 \in \mathbb{N}$ and $P, Q \in \mathbb{C}[x]$ be such that

$$P(Q(x)) = x^n + x^{n-1} + \cdots x + 2016$$

Prove that atleast one of P and Q is linear.

Proof. Let's assume that P, Q are not integers. Now, for any root α_i, of $P(x)$, roots of $Q(x) - \alpha_i$ are roots of $P(Q(x))$. Thus, the sum of roots $Q(x) - \alpha_i$ is also the sum of roots of $Q(x)$ if $\deg Q > 1$, but this sum is counted $\deg P$ times, to get the sum of roots as -1. Thus, the sum of roots of $Q(x) - \alpha_i$ have sum $\frac{-1}{\deg P}$. But, they all are roots of $P(Q(x))$ and thus algebraic integers and $\overline{Z}$ is a ring. So, if their sum is a rational, it must be an integer. Thus, $\deg P = 1$ and we are done. □

This was a fairly hard problem as can be expected from any Miklos problem but the ideas that we used are not all that difficult to find.

The following example has a similar taste as well.

Example 5.13 (Simpler version of Japan TST)
Let P be a real monic polynomial such that P^2, P^3 are integer polynomials. P.T. P is an integer polynomial.

Proof. First, we show that P is a rational polynomial. Observe that $P^3 = P(P^2)$, so as P^2 takes integers to integers and so does P^3, P takes integers to integers for infinitely many integers. Thus, P is rational by applying Lagrange interpolation.

Now, let α be a root of P. Thus, $P(P^2(\alpha)) = P(P(0))$ is an integer. Thus, α is a root of $P^3(x) - P(P(0))$ which is a monic integer polynomial. Thus, α is an algebraic integer. Thus, all roots of P are algebraic integers and as it is monic, it must thus be an integer polynomial. □

Hopefully, some ways that we can use the above ideas are clear and you're ready to attempt some problems. So let's dive in.

§5.4 Problems

Problem 5.14. Try any exercises above or unproved examples/theorems/lemmas given.

Problem 5.15. What is the period of the Fibonacci sequence $\pmod{127}$

Problem 5.16 (ISL 2003)**.** The sequence a_0, a_1, a_2, ... is defined as follows:

$$a_0 = 2, \qquad a_{k+1} = 2a_k^2 - 1 \quad \text{for } k \geq 0.$$

Prove that if an odd prime p divides a_n, then 2^{n+3} divides $p^2 - 1$.

Problem 5.17 (Fermat's Last Theorem for Polynomials)**.** Let f, g, h be relatively prime non constant polynomials with complex coefficients. Let $n \geq 3$ be a natural. Show that

$$f^n + g^n \neq h^n$$

Soln: 9

Problem 5.18 (Infinity Dots 2018/5)**.** Let $c_1, c_2, \ldots, c_k$ be integers. Consider sequences $\{a_n\}$ of integers satisfying

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

for all $n \geqslant k+1$. Prove that there is a choice of initial terms $a_1, a_2, \ldots, a_k$ not all zero satisfying: there is an integer b such that p divides $a_p - b$ for all primes p.

Problem 5.19 (USATST 2017/3)**.** Let $P, Q \in \mathbb{R}[x]$ be relatively prime nonconstant polynomials. Show that there can be at most three real numbers λ such that $P + \lambda Q$ is the square of a polynomial.

Problem 5.20 (APMO 2018/5)**.** Find all polynomials $P(x)$ with integer coefficients such that for all real numbers s and t, if $P(s)$ and $P(t)$ are both integers, then $P(st)$ is also an integer. Soln: 9

Problem 5.21 (Iran 2019 Round 3 A2)**.** $P(x)$ is a monic polynomial with integer coefficients so that there exists monic integer coefficients polynomials $p_1(x), p_2(x), \ldots, p_n(x)$ so that for any natural number x there exist an index j and a natural number y so that $p_j(y) = P(x)$ and also $deg(p_j) \geq deg(P)$ for all j.Show that there exist an index i and an integer k so that $P(x) = p_i(x + k)$.

Problem 5.22 (USATST 2017/6)**.** Prove that there are infinitely many triples (a, b, p) of positive integers with p prime, $a < p$, and $b < p$, such that $(a + b)^p - a^p - b^p$ is a multiple of p^3.

Problem 5.23 (LMAO Senior 2020/6)**.** Determine all monic polynomials P with integral co-efficients such that $P(0) \neq 1$ and $\forall$ sufficiently large integers n, we have

$$P(n^{2020}) | n^{P(n)} + P(P(n))$$

Soln: 9

Problem 5.24 (Iran 2020 Round 3/ A4)**.** We call a polynomial $P(x)$ intresting if there are 1398 distinct positive integers $n_1, ..., n_{1398}$ such that

$$P(x) = \sum x^{n_i} + 1$$

Does there exist infinitly many polynomials $P_1(x), P_2(x), ...$ such that for each distinct i, j the polynomial $P_i(x)P_j(x)$ is interesting.

§6 Miscelleanous

This section serves to briefly discuss various ideas that can come up but are not very common but are good to know.

§6.1 Newton Forward Differences

Let's consider $P_1(x) = P(x+1) - P(x)$. Now, if P is a polynomial, then $P_1(x)$ is also a polynomial with degree 1 less than P.
Similarly we can define the recurrence $P_{i+1}(x) = P_i(x+1) - P_i(x)$. Thus, $P_n(x)$ is a polynomial with degree, $\deg P - n$.

Now, let us see what these polynomials actually look like.

$$\begin{aligned}
P_1(x) &= P(x+1) - P(x) \\
P_2(x) &= P(x+2) - 2P(x+1) + P(x) \\
P_3(x) &= P(x+3) - 3P(x+2) + 3P(x+1) - P(x) \\
&\vdots \\
P_n(x) &= P(x+n) - nP(x+n-1) + \binom{n}{2} P(x+n-2) + \cdots + (-1)^n P(x)
\end{aligned}$$

So, we in fact have that $P_n(x) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} P(x+i)$
Particularly interesting are $P_n(0)$ as they give us the following nice result. For ease, we will say that $P(x) = P_0$

Theorem 6.1 (Newton's Forward Differences Theorem)
$P(x) = \sum_{i \geq 0} P_i(0) \binom{x}{i}$

This is a very interesting theorem even though its not commonly used in problems. Let's look at one that actually uses it.

Exercise 6.2. If P is an n degree polynomial with leading coefficient a_n, then $P_n(x) = n! a_n$

Example 6.3 (OMO 2020)
Evaluate

$$\sum_{k=0}^{2n} (-1)^k \binom{2n}{k} \cos\left(2n \cos^{-1}\left(\frac{k}{2n}\right)\right)$$

We will actually do this in the next section! but you are free to try on your own.

§6.2 Chebyshev Polynomials

Chebyshev Polynomials are special polynomials that let us talk about $\cos(n\theta)$ and $\frac{\sin n\theta}{\sin \theta}$ as polynomials in $\cos\theta$.
So, we can define two types of Chebyshev Polynomials

- Chebyshev Polynomials of the first kind- $T_n(\cos\theta) = \cos(n\theta)$
- Chebyshev Polynomials of the second kind $U_n(\cos\theta) = \frac{\sin((n+1\theta))}{\sin\theta}$

Theorem 6.4 (Chebyshev Polynomials)
There exist integer polynomials T_n and U_n with the following properties-

- $T_n(\cos\theta) = \cos(n\theta)$
- $U_n(\cos\theta) = \frac{\sin((n+1\theta))}{\sin\theta}$

Now, clearly T_0, U_0 are both identically 1 and $T_1 = x$ and $U_1 = 2x$, now let us develop some recursion to find the next Chebyshev Polynomial!

$$T_{n+1}(\cos\theta) = \cos((n+1)\theta) = \cos(n\theta)\cos\theta + \sin(n\theta)\sin\theta$$
$$= T_n(\cos\theta)\cos\theta + \sin^2\theta U_{n-1}(\cos\theta) = T_n(\cos\theta)\cos\theta + (1-\cos^2\theta)U_{n-1}(\cos\theta)$$
$$\iff T_{n+1} = xT_n + (x^2-1)U_{n-1}$$

$$U_{n+1}(\cos\theta) = \frac{\sin((n+2)\theta)}{\sin\theta} = \cos((n+1)\theta) + \frac{\sin((n+1)\theta)}{\sin\theta}\cos\theta$$
$$= T_{n+1}(\cos\theta) + U_n(\cos\theta)\cos\theta \iff U_{n+1} = T_{n+1} + xU_n$$

As $\mathbb{Z}[x]$ is a ring, our recurrences only generate integer polynomials and we are done!

Exercise 6.5. Show that the leading coefficient of T_n is 2^{n-1} and it has degree n.

Now, let us try the previous example.

Example (OMO 2020)
Evaluate
$$\sum_{k=0}^{2n}(-1)^k\binom{2n}{k}\cos\left(2n\cos^{-1}\left(\frac{k}{2n}\right)\right)$$

We can now write the whole expression $\cos\left(2n\cos^{-1}\left(\frac{k}{2n}\right)\right)$ as $T_{2n}(\frac{k}{2n})$. Now, let us replace transform $T_{2n}(\frac{k}{2n})$ instead to be $Q(k)$ by replacing any term x with $\frac{x}{2n}$.
Now, we have the expression, as Q is a polynomial of degree $2n$, the expression, $\sum_{k=0}^{2n}(-1)^k\binom{2n}{k}Q(k)$ represents $Q_{2n}(0)$ by the idea developed in the previous section.
But in fact, this expression becomes $2n!a_{2n}$ where a_{2n} is the leading coefficient of Q. But the leading coefficient of Q is given by the term $2^{2n-1}(\frac{x}{2n})^{2n}$. So, our answer is finally

$$\boxed{\frac{(2n-1)!}{(n^{2n-1})}}$$

§6.3 Cyclotomic Polynomials

We have previously referred to cyclotomic polynomials without any introduction but we will now discuss them slightly.

Definition 6.6. n^{th} **Primitive roots of unity** are roots of the unity of the form $e^{\frac{2\pi ik}{n}}$ such that $(k, n) = 1$.

Definition 6.7. $\Phi_n(x)$ is defined as the monic polynomial with roots exactly as the primitive nth roots of unity.

We now have that $\deg \Phi_n(x) = \phi(n)$ as there are $\phi(n)$ primitve roots of unity and also

Lemma 6.8
$x^n - 1 = \prod_{d|n} \Phi_d(x)$

Theorem 6.9
$\Phi_n(x) \in \mathbb{Z}[x]$.

We prove by induction. The result is direct for $n = 1$, as $\Phi_1(x) = x - 1$ but now, by the previous lemma, we have $\Phi_n(x) = \frac{x^n-1}{\prod_{d|n, d\neq n} \Phi_d(x)}$ We now have that $\Phi_n(x)$ is a polynomial and can also be written as the ratio of two integer polynomials. Thus, it must also be an integer polynomial by Gauss Lemma!

$\phi_n(x)$ and cyclotomic polynomials are rarely useful for polynomial problems but they are quite useful in number theory. in fact, we can prove the existence of primitive roots $\pmod p$ using cyclotomic polynomials.

We also have the following lemma

Lemma 6.10
$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$

This is a direct result of mobius inversion and is thus left as an exercise.
Now, we prove the existence of primitive roots.

Example 6.11 (Primitive roots exist $\pmod p$)
For every prime p, there exist some primitive roots.

Proof. We can write $x^{p-1} - 1 = \prod_{d|p-1} \Phi_d(x)$. But since, any polynomial of degree d has atmost d roots in $\mathbb{F}_p[x]$, and $x^{p-1} - 1$ has exactly $p - 1$ roots, every factor of $x^{p-1} - 1$ has as many roots as its degree and roots do not repeat in co-prime factors. Now, if any root of $\Phi_{p-1}(x)$ has order $a \neq p - 1$ then $p | x^a - 1 = \prod_{d|a} \Phi_d(x)$, thus it is a root of a different factor as well. Contradiction! Thus, all roots of $\Phi_{p-1}(x)$ are primitive roots and there are exactly $\phi(p - 1)$ of these. □

This shows the power of cyclotomic polynomials. For more reading on cyclotomic polynomials in olympiads, I suggest Cyclotomic Polynomials in Olympiad Number Theory.

§6.4 Multivariate Polynomials

Now, we will talk about some multivariate polynomials.

As before, we have our most important result-

Theorem 6.12 (UFDs)
$\mathbb{C}[x_1, x_2, \cdots x_n], \mathbb{R}[x_1, x_2, \cdots x_n], \mathbb{Q}[x_1, x_2, \cdots x_n], \mathbb{Z}[x_1, x_2, \cdots x_n]$ are all UFDs.

This is left as an exercise.

It's now important to note that we can still about ideas like Euclidean Division, co-primality, GCD of these polynomials etc.

As for the entire document, we have not actually solved any problems involving multivariate polynomials(even though there have been exercises and theorems involving them), let's do that now.

Example 6.13 (USA TSTST 2016/1)
Let $A = A(x, y)$ and $B = B(x, y)$ be two-variable polynomials with real coefficients. Suppose that $A(x, y)/B(x, y)$ is a polynomial in x for infinitely many values of y, and a polynomial in y for infinitely many values of x. Prove that B divides A, meaning there exists a third polynomial C with real coefficients such that $A = B \cdot C$.

Proof. When trying to prove results where one thing divides another, for example here, we want to show that $B|A$, then Euclidean Division is a natural choice but it's hard to directly apply Euclidean division in a way that is helpful.
So, for this we consider the space of rational functions in y $\mathbb{R}(y)$ i.e. functions of the form $\frac{P(y)}{Q(y)}$ where P and Q are polynomials. Now, in $R(y)[x]$[6], we can perform Euclidean Division.

So, we can now write $A = QB + R$ where $B, R \in \mathbb{R}(y)[x]$.

Now, let us write Q, R as $Q = \frac{Q_1(x,y)}{A_1(y)}$ and $R = \frac{R_1(x,y)}{B_1(y)}$. Thus, as $\deg R < \deg B$(note that we are talking about the degree of x), we have for infinitely many values of y that $R_1(x, y) = 0$. Thus, $R_1(x, y)$ is identically 0. Thus, we get that $A = BQ$. But, $Q \in \mathbb{R}(y)[x]$.

But, the same argument can be done with x and y replaced. So, we get that $Q \in \mathbb{R}(x)[y]$.

[6]This basically is as before, these are polynomials where coefficients of x are rational functions of y like before, $\mathbb{R}[x]$, is the set of polynomials with coefficients in $\mathbb{R}$

Thus, $\frac{A}{B}$ can be written as $\frac{Q_1(x,y)}{A_1(y)} = \frac{Q_2(x,y)}{A_2(x)}$. WLOG, $\gcd(Q_1, A_1) = 1 = \gcd(Q_2, A_2)$ Now, $A_1(y)|A_2(x) \cdot Q_1(x,y) \implies A_1(y)|Q_1(x,y)$ as A_1, A_2 are functions in seperate variables and thus co-prime. Thus, A_1 is a constant and so is A_2. Thus, we are done! □

This idea of applying Euclidean division in a slightly modified form is extremely nice. With it in mind, try the following problem.

§6.5 Advanced Results

The following results are more advanced results from different areas which can sometimes be helpful for olympiad problems but rarely come up.

§6.5.1 Alon's Combinatorial Nullstellensatz

The following is a very nice result but is more useful for combinatorial problems and probably its own application on the IMO was in 2007. But, if you leave usefulness aside, its a very nice result to know! For a more detailed introduction, you can refer to My handout on the topic or of course, Noga Alon's original paper

Theorem 6.14 (Combinatorial Nullstellensatz)
Let $\mathbb{F}$ be a field, and let $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$ be a polynomial on n variables $x_1, x_2, \cdots, x_n$ of degree $t_1 + t_2 + \cdots + t_n$, where each t_i is a non-negative integer. If $S_1, S_2, \cdots, S_n$ are non-empty subsets of $\mathbb{F}$ such that $|S_i| = t_i + 1$, then there exists an $(s_1, s_2, \cdots, s_n) \in S_1 \times S_2 \times \cdots \times S_n$ such that

$$f(s_1, s_2, \cdots, s_n) \neq 0$$

if the coefficient of ${x_1}^{t_1}{x_2}^{t_2}\cdots{x_n}^{t_n}$ in f is non-zero.

Proof. The following write-up is by Shourya Pandey.
Consider the case where the degree of each x_i is at most t_i. Since the degree of f is $t = t_1 + t_2 + \cdots + t_n$, this means the only monomial with degree t is $x_1^{t_1}x_2^{t_2}\cdots x_n^{t_n}$. Let us interpret the polynomial f has a polynomial only in x_n, with coefficients from $x_1, x_2, x_3, \cdots, x_{n-1}$. Then, this polynomial has degree t_n in x_n. Consider the coefficient of $x_n^{t_n}$. This is a polynomial $f' \in \mathbb{F}[x_1, x_2, \cdots, x_{n-1}]$, with degree $t_1 + t_2 + \cdots + t_{n-1}$, and such that x_i has degree at most t_i in f'. By induction, there is a setting of $x_1, x_2, \cdots, x_{n-1}$ from $S_1, S_2, \cdots, S_{n-1}$ respectively, such that f' evaluates to not zero. Take this substitution in f. This gives us a polynomial $g \in \mathbb{F}[x_n]$ of degree t_n. Since x_n can take $t_n + 1$ values, one of these values keeps g non-zero, and the proof is finished.

Now, we want to get rid of the assumption that the degree of x_i is not at most t_i.
Note that we are only concerned with the value of x_i in S_i, for all i. Consider S_1 for now. Suppose $S_1 = \{a_1, a_2, \cdots, a_{t_1+1}\}$. Then note that for any $x_1 \in S_1$,

$$(x_1 - a_1)(x_1 - a_2)\cdots(x_1 - a_{t_1+1}) = 0$$

which means that we can do the following.

This means we can replace all occurrences of x_1^d, for $d \geq t_1 + 1$, with a polynomial of degree at most t_1 (how?), while keeping the evaluation of the polynomial the same in S_1. Also note that this substition will **not** alter the coefficient of $x_1^{t_1}x_2^{t_2}\cdots x_n^{t_n}$ (why?)

We do this process of "degree reduction" for all variables, and arrive at a polynomial p such that $f(s_1, s_2, \cdots, s_n) = p(s_1, s_2, \cdots, s_n)$, and such that p falls in the category of the first paragraph. This finishes the proof. □

Exercise 6.15 (IMO 2007/6)**.** Let $n > 1$ be an integer. In the space, consider the set

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \cdots, n\}, x + y + z > 0\}$$

Find the smallest number of planes that jointly contain all $(n+1)^3 - 1$ points of S, but none of the planes contain the point $(0, 0, 0)$. Soln: 9

§6.5.2 Rouche's theorem

The following is a powerful tool and can be useful for proving irreducibility criterion as well like Perron's but its rarely needed for olympiad problems.

Theorem 6.16 (Rouche's theorem)

If f and g are two holomorphic[a] functions on and inside a circle γ such that $|g| > |f - g|$ on γ then f and g have an equal number of roots(with multiplicity) inside γ.

[a] You don't need to worry about this right now as we only care about polynomials, but if you are curious then you can google it

As this result is from Complex Analysis, and its proof is out of the scope of this handout, we will omit it but still see some usage.

Example 6.17 (Perron's criterion)

Suppose $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and $|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|$ and $a_0 \neq 0$ then P is irreducible.

Proof. By taking $P = f$ and $g = a_{n-1}x^{n-1}$ and γ as the unit circle, we get that P has $n - 1$ roots inside the unit circle. Thus, if P is reducible as QR, then one of its factors will have all roots inside the unit circle but then the product cannot be an integer. Note, that 0 is not a root of P. □

Exercise 6.18 (IMO 1993)**.** $x^n + 5x^{n-1} + 3$ is irreducible.

§6.5.3 Mason Stothers

The following is a very powerful theorem but is again rarely needed for olympiad problems.

Theorem 6.19 (Mason Stothers)

Let $a, b, c \in \mathbb{C}[x]$ such that not all three are constant and $a + b = c$ such that $\gcd(a, b, c) = 1$ then $\max(\deg a, \deg b, \deg c) \leq \deg(rad(abc)) - 1$

The following writeup of the proof is by Kazi Aryan Amin.

Proof. Notation : Since $\mathbb{Z}[X]$ is a UFD, it is possible to write every $f \in Z[X]$ as a product of irreducible factors, say $f = cp_1^{a_1} \cdot p_2^{a_2} \ldots$, where p_i are irreducible polynomials in $\mathbb{Z}[X]$ and $c \in \mathbb{Z}$. Define $\operatorname{rad} f$ to be the polynomial which is the product of the distinct irreducible factors of f, ie $\operatorname{rad} f = \prod_i p_i$.

The main lemma we use is the fact that $\frac{f}{\operatorname{rad} f}$ divides f, f'.

Note that we have :

$$cc' = c(a' + b') = c'(a + b) \implies bc' - b'c = ac' - ca'$$

First we prove that $ac' - ca' \neq 0$. If it was zero, then we get that $a \mid ca' \implies a \mid a'$, which is false. (We have used the fact that $(a, c) = 1$.)

Now assume for the sake of contradiction that the theorem doesnt hold. WLOG $\deg a \geq \deg \operatorname{rad} abc$. We prove that $bc' - cb' = 0$, which will result in a contradiction.

Note that since $\frac{f}{\operatorname{rad} f}$ divides f, f', hence it also divides any linear combination of them. Hence we have the following divisibility relations :

$$\frac{c}{\operatorname{rad} c} \mid bc' - cb'$$
$$\frac{b}{\operatorname{rad} b} \mid bc' - cb'$$
$$\frac{a}{\operatorname{rad} a} \mid ac' = ca' = bc' - cb'$$

Now since a, b, c are pairwise coprime, we have $\operatorname{rad} abc = \operatorname{rad} a \cdot \operatorname{rad} b \cdot \operatorname{rad} c$. We combine the divisiblities to get :

$$\frac{abc}{\operatorname{rad} abc} \mid bc' - cb'$$

Now note that we have :

$$\deg \frac{abc}{\operatorname{rad} abc} = \deg abc - \deg \operatorname{rad} abc \geq \deg abc - \deg a > \deg cb' - bc'$$

However the divisibility relation implies that $cb' - bc' = 0$, which is a contradiction. □

This is a very powerful theorem, so let us see one example of it being used.

Example 6.20 (RMMSL 2018 A1)

Let m and n be integers greater than 2, and let A and B be non-constant polynomials with complex coefficients, at least one of which has a degree greater than 1. Prove that if the degree of the polynomial $A^m - B^n$ is less than $\min(m, n)$, then $A^m = B^n$.

Proof. FTSOC, $A^m - B^n \neq 0$ and WLOG, $\deg A > 1$. If A, B have any common root α then $(x - \alpha)^{\min(m,n)} | A^m - B^n$ so $A^m - B^n = 0$ as we have $\deg A^m - B^n < \min(m.n)$. Thus, A, B are co-prime.
Now, by Mason Stothers we have that $\max(m \deg A, n \deg B) \leq \deg A + \deg B + \min(m, n) - 2$. Thus, $m \deg A + n \deg B \leq 2 \deg A + 2 \deg B \leq 2 \deg A + 2 \deg B + m + n - 4 \implies$

$(m-2)\deg A + (n-2)\deg B \leq m+n-4$ but since $m, n > 2$, we get that $(m-2)(\deg A - 1) + (n-2)(\deg B - 1) \leq 0$ which is false by the given conditions so we are done.

□

Exercise 6.21 (Fermat's last theorem for poly)**.** Let f, g, h be relatively prime non constant polynomials with complex coefficients. Let $n \geq 3$ be a natural. Show that

$$f^n + g^n \neq h^n$$

With this, we conclude this section and move on to the problem sets!

§6.6 Miscelleanous Problem Set

Problem 6.22. Try the given exercises above.

Problem 6.23 (ISL 1997)**.** Let p be a prime number and f an integer polynomial of degree d such that $f(0) = 0, f(1) = 1$ and $f(n)$ is congruent to 0 or 1 modulo p for every integer n. Prove that $d \geq p - 1$.

Problem 6.24 (Romania)**.** Let $f \in \mathbb{C}[x]$ be a monic polynomial. Prove that we can find a $z \in C$ such that $|z| = 1$ and $|f(z)| \geq 1$.

Problem 6.25 (Putnam 2000/A6)**.** Let $f(x)$ be a polynomial with integer coefficients. Define a sequence $a_0, a_1, \cdots$ of integers such that $a_0 = 0$ and $a_{n+1} = f(a_n)$ for all $n \geq 0$. Prove that if there exists a positive integer m for which $a_m = 0$ then either $a_1 = 0$ or $a_2 = 0$.

Problem 6.26 (Japan 2017/5)**.** Let $x_1, x_2, \cdots, x_{1000}$ be integers, and $\sum_{i=1}^{1000} x_i^k$ are all multiples of 2017 for any positive integers $k \leq 672$. Prove that $x_1, x_2, \cdots, x_{1000}$ are all multiples of 2017.

Problem 6.27 (Iran 2017/ Round 3/ A4)**.** Let $P(x)$ be a non-zero polynomial with real coefficient so thay $P(0) = 0$.Prove that for any positive real number M there exist a positive integer d so that for any monoic polynomial $Q(x)$ with degree at least d the number of integers k so that $|P(Q(k))| \leq M$ is at most equal to the degree of Q.

Problem 6.28 (USA TSTST 2011/9)**.** Let n be a positive integer. Suppose we are given $2^n + 1$ distinct sets, each containing finitely many objects. Place each set into one of two categories, the red sets and the blue sets, so that there is at least one set in each category. We define the symmetric difference of two sets as the set of objects belonging to exactly one of the two sets. Prove that there are at least 2^n different sets which can be obtained as the symmetric difference of a red set and a blue set.

Problem 6.29 (ISL 2019 A6)**.** A polynomial $P(x, y, z)$ in three variables with real coefficients satisfies the identities

$$P(x, y, z) = P(x, y, xy - z) = P(x, zx - y, z) = P(yz - x, y, z).$$

Prove that there exists a polynomial $F(t)$ in one variable such that

$$P(x, y, z) = F(x^2 + y^2 + z^2 - xyz).$$

Problem 6.30 (Chevalley-Warning)**.** Let p be an odd prime number. Let $f_1, f_2, \cdots, f_k$ be polynomials in $\mathbb{Z}_p[x_1, x_2, \cdots, x_n]$ such that $n > \sum_{i=1}^{k} \deg(f_i)$. Show that if the polynomials $f_1, f_2, \cdots, f_k$ have a common zero $(c_1, c_2, \cdots, c_n)$. then they have another common zero.

§7 Final Combined Problem Set

We now have a final problem set using ideas from all topics used till now or nice problems I just didn't know where to place :). Some of the problems here are also incredibly hard but nice results to know and try to prove.

Problem 7.1 (ISL 2005/A1)**.** Find all pairs of integers a, b for which there exists a polynomial $P(x) \in \mathbb{Z}[X]$ such that product $(x^2 + ax + b) \cdot P(x)$ is a polynomial of a form

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

where each of $c_0, c_1, \ldots, c_{n-1}$ is equal to 1 or -1.

Problem 7.2 (INMO 2020/2)**.** Suppose $P(x)$ is a polynomial with real coefficients, satisfying the condition $P(\cos\theta + \sin\theta) = P(\cos\theta - \sin\theta)$, for every real θ. Prove that $P(x)$ can be expressed in the form

$$P(x) = a_0 + a_1(1-x^2)^2 + a_2(1-x^2)^4 + \cdots + a_n(1-x^2)^{2n}$$

for some real numbers $a_0, a_1, \ldots, a_n$ and non-negative integer n.

Problem 7.3 (IMO 2016/5)**.** The equation

$$(x-1)(x-2)\cdots(x-2016) = (x-1)(x-2)\cdots(x-2016)$$

is written on the board, with 2016 linear factors on each side. What is the least possible value of k for which it is possible to erase exactly k of these 4032 linear factors so that at least one factor remains on each side and the resulting equation has no real solutions?

Problem 7.4 (USA TST 2012)**.** Consider (3-variable) polynomials

$$P_n(x,y,z) = (x-y)^{2n}(y-z)^{2n} + (y-z)^{2n}(z-x)^{2n} + (z-x)^{2n}(x-y)^{2n}$$

and

$$Q_n(x,y,z) = [(x-y)^{2n} + (y-z)^{2n} + (z-x)^{2n}]^{2n}.$$

Determine all positive integers n such that the quotient $Q_n(x,y,z)/P_n(x,y,z)$ is a (3-variable) polynomial with rational coefficients.

Problem 7.5 (KWPT 2021/15)**.** Find all pair of constants (a, b) such that there exists real-coefficient polynomial $p(x)$ and $q(x)$ that satisfies the condition below.
Condition: $\forall x \in \mathbb{R},\ \ p(x^2)q(x+1) - p(x+1)q(x^2) = x^2 + ax + b$

Problem 7.6 (Russia 2004/11.3)**.** The polynomials $P(x)$ and $Q(x)$ are given. It is known that for a certain polynomial $R(x, y)$ the identity $P(x) - P(y) = R(x, y)(Q(x) - Q(y))$ applies. Prove that there is a polynomial $S(x)$ so that $P(x) = S(Q(x)) \quad \forall x$.

Problem 7.7 (Kurschak 2017/2)**.** Do there exist polynomials $p(x)$ and $q(x)$ with real coefficients such that $p^3(x) - q^2(x)$ is linear but not constant?

Problem 7.8 (USOJMO 2020/6)**.** Let $n \geq 2$ be an integer. Let $P(x_1, x_2, \ldots, x_n)$ be a nonconstant n-variable polynomial with real coefficients. Assume that whenever $r_1, r_2, \ldots, r_n$ are real numbers, at least two of which are equal, we have $P(r_1, r_2, \ldots, r_n) = 0$. Prove that $P(x_1, x_2, \ldots, x_n)$ cannot be written as the sum of fewer than $n!$ monomials. (A monomial is a polynomial of the form $cx_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$, where c is a nonzero real number and d_1, d_2, …, d_n are nonnegative integers.)

Problem 7.9 (USATST 2021/7)**.** Find all nonconstant polynomials $P(z)$ with complex coefficients for which all complex roots of the polynomials $P(z)$ and $P(z)-1$ have absolute value 1. Soln: 9

Problem 7.10 (USA TST 2020/5)**.** Find all integers $n \geq 2$ for which there exists an integer m and a polynomial $P(x)$ with integer coefficients satisfying the following three conditions:
$m > 1$ and $\gcd(m, n) = 1$; the numbers $P(0)$, $P^2(0)$, ..., $P^{m-1}(0)$ are not divisible by n; and
$P^m(0)$ is divisible by n.
Here P^k means P applied k times, so $P^1(0) = P(0)$, $P^2(0) = P(P(0))$, etc.

Problem 7.11 (ISL 2002 N6)**.** Find all pairs of positive integers $m, n \geq 3$ for which there exist infinitely many positive integers a such that

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

is itself an integer.

Problem 7.12 (ISL 2005 N3)**.** Let a, b, c, d, e, f be positive integers and let $S = a+b+c+d+e+f$.
Suppose that the number S divides $abc+def$ and $ab+bc+ca-de-ef-df$. Prove that S is composite.

Problem 7.13 (USAMO 2006/3)**.** For integral m, let $p(m)$ be the greatest prime divisor of m. By convention, we set $p(\pm 1) = 1$ and $p(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence

$$\{p\left(f\left(n^2\right)\right) - 2n\}_{n \geq 0}$$

is bounded above. (In particular, this requires $f\left(n^2\right) \neq 0$ for $n \geq 0$.)

Problem 7.14 (Kronecker's theorem)**.** Let α be an algebraic integer on the unit circle. Assume that all of its galois conjugates are also on the unit circle. Prove that α is a root of unity. Soln: 9

Problem 7.15 (Infinity Dots 2018/4)**.** Let $P \in \mathbb{Z}[x]$ be a nonconstant polynomial without integral roots. Prove that there is a positive integer $m \leqslant 3 \cdot \deg P$ such that $P(m)$ does not divide $P(m+1)$.

Problem 7.16 (IMO 2017/6)**.** An ordered pair (x, y) of integers is a primitive point if the greatest common divisor of x and y is 1. Given a finite set S of primitive points, prove that there exist a positive integer n and integers $a_0, a_1, \ldots, a_n$ such that, for each (x, y) in S, we have:

$$a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \cdots + a_{n-1} x y^{n-1} + a_n y^n = 1.$$

Problem 7.17 (ISL 2015 A6)**.** Let n be a fixed integer with $n \geq 2$. We say that two polynomials P and Q with real coefficients are block-similar if for each $i \in \{1, 2, \ldots, n\}$ the sequences

$$P(2015i), P(2015i-1), \ldots, P(2015i-2014) \quad \text{and}$$
$$Q(2015i), Q(2015i-1), \ldots, Q(2015i-2014)$$

are permutations of each other.
(a) Prove that there exist distinct block-similar polynomials of degree $n+1$.
(b) Prove that there do not exist distinct block-similar polynomials of degree n.

Problem 7.18 (KWPT 2021/8)**.** P is an monic integer coefficient polynomial which has no integer roots. $\deg P = n$ and define
$A := v_2(P(m))|m \in Z, v_2(P(m)) \geq 1$. If $|A| = n$, show that all of the elements of A are smaller than $\frac{3}{2}n^2$.

> **Remark.** I don't actually know the solution(only such in the handout) to this problem so it would be great if someone could tell me :)

Problem 7.19 (USEMO 2019/2)**.** Let $\mathbb{Z}[x]$ denote the set of single-variable polynomials in x with integer coefficients. Find all functions $\theta : \mathbb{Z}[x] \to \mathbb{Z}[x]$ (i.e. functions taking polynomials to polynomials) such that for any polynomials $p, q \in \mathbb{Z}[x]$, $\theta(p+q) = \theta(p) + \theta(q)$; for any polynomial $p \in \mathbb{Z}[x]$, p has an integer root if and only if $\theta(p)$ does.

Problem 7.20 (KöMaL)**.** Let $p(x) = a_{21}x^{21} + a_{20}x^{20} + \cdots a_1 x + 1$ be a polynomial with integer coefficients and real roots such that the absolute value of all of its roots are less than $1/3$, and all the coefficients of $p(x)$ are lying in the interval $[-2019a, 2019a]$ for some positive integer a. Prove that if this polynomial is reducible in $\mathbb{Z}[x]$, then the coefficients of one its factors are less than a.

Problem 7.21. Let $P(x_1, x_2), Q(x_1, x_2)$ be polynomials with complex coefficients in two variables x, y such that there exist infinitely many pairs $(a, b) \in \mathbb{R}^2$ for which $P(a, b) = Q(a, b) = 0$. Prove that P and Q have a non constant common factor. Soln: 9

Problem 7.22 (Alon)**.** Let p be a prime and let $h = h(x_0, x_1, \cdots, x_k)$ be a polynomial over $\mathbb{Z}_p$. Let $A_0, A_1, \cdots A_k$ be nonempty subsets of $\mathbb{Z}_p$, where $|A_i| = c_i + 1$ and define $m = \sum_{i=0}^{k} c_i - \deg h$. If the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in

$$(x_0 + x_1 + \cdots x_k)^m \cdot h(x_1, x_2, \cdots x_m)$$

is nonzero (in $\mathbb{Z}_p$) then

$$|\{a_0 + a_1 + \cdots a_k | a_i \in A_i, h(a_0, a_1, \cdots a_k) \neq 0\}| \geq m + 1$$

and hence $m < p$.

§8 References and Acknowledgements

The following resources were referred in making the handout-

- Modern Olympiad Number Theory by Aditya Khurmi
- Yufei Zhao's Polynomials
- Cyclotomic Polynomials in Olympiad Number Theory
- Wikipedia was used extensively and I have run out of a list of pages checked.
- Same holds true for AoPS, especially contest collections :)

I would like to especially thank Pranjal Srivastava for helping me develop a deeper appreciation for polynomials and also making it one of my stronger subjects. A lot of the problems in this handout are ones he has suggested and have helped me develop an intuition for the subject.

I would also like to thank Kazi Aryan Amin, Shourya Pandey and Aditya Khurmi for allowing me to use their proof write-ups for a few problems and for problem recommendations for the handout.

I would also like to thank Aatman Supkar, and Aditya Khurmi who proofread the handout and helped find numerous errors and typos. Inadvertently, there will be some typos but I will try to keep updating them for future versions! It would be helpful if you pointed these out to me.

§9 Selected Solutions

I may write hints for some problems and more solutions some time in the future, but for now, we have a few selected solutions.

1.7 INMO 2018

We claim $\boxed{P = cx^n}$ is the only solution.
Now let α be a root of P with largest modulus. FTSOC $\alpha \neq 0$ Now, let $x^2 + x + 1 = \alpha$. This, equation has solutions β_1, β_2. Now, plugging back in we get that $(\beta_1 - 1)\alpha$ and $(\beta_2 - 1)\alpha$ are also roots of P.
But, $|(\beta_1 - 1)(\alpha)| + |(\beta_2 - 1)\alpha| \geq |(\beta_1 + \beta_2 - 2)\alpha| = 3|\alpha| > 2|\alpha|$ but then we would have found a root with a larger modulus than α. Contradiction!

1.10 LMAO 2020 Senior/2

The following solution and remarks are by Pranjal Srivastava(One of the co-authors of the problem).

We define $P^k(x) = \underbrace{P(P(\cdots P(x)\cdots))}_{k \text{ times}}$

Call a number t **cute** if $P(x) = t$ has less then m distinct roots. The **cuteness** of t, denoted $c(t)$, is defined as $m-$ number of distinct roots of $P(x) = t$.

Lemma: For any subset S of the complex numbers $\sum_{s\in S} c(s) < m$
Proof: It is well known that a complex number t is cute if and only if $t = P(t_0)$ for some root t_0 of P'. Also observe by differentiating $(x - t_0)^{c(t)}Q(x)$ using product rule, that the cuteness of t is just the sum of multiplicities of all possible such t_0 as roots of P'

Let R_k denote the set of roots of $P^k(x) = 0$, and let $r_k = |R_k|$ Observe that $r_{k+1} = mr_k - \sum_{t\in R_k} c(t)$ [since an element of R_{k+1} is just a root of $P(x) = t$ for some $t \in R_k$. This implies that $(r_k - 1)m < r_{k+1} < r_k m$

We now create c in base m. Let the k'th digit of c be $r_{k+1} - mr_k$. For the sake of convenience, we refer to the k'th digit as d_k
From definition, we see that $\lfloor cm^k \rfloor = r_k - 1$
Thus, the only case where this choice of c could potentially fail is when $cm^k = r_k - 1$ i.e. the sequence d_i is eventually constant at 0. However, note that since $P(0) \neq 0$, no cute number can belong to both R_k and R_{k+1}. Further, $d_k + d_{k+1} \geq m$

We will now show that the digits of c are periodic

Note that, if for no $t > 0$, is $P^t(0) = 0$, all the R_i are pairwise disjoint. This will imply that for all large enough R_i, no element of R_i is cute, and for all large enough k, $d_k = m - 1$ [This is more convenient than saying that the base$-m$ expansion terminates]

We now try to see what happens there is some t, such that $P^t(0) = 0$
Observe that $R_i \subseteq R_{i+t}$. Also observe that $\sum_{s\in R_i} c(s) \leq \sum_{s\in R_{i+t}} c(s)$.
Since this summation over cuteness over R_k, R_{k+t} is a bounded increasing sequence, it is eventually constant. Further, we have that for all large k, $\sum_{s\in R_i} c(s) = \sum_{s\in R_{i+t}} c(s)$

As we have discussed, this implies that the expansion of c in base-m is periodic, and that c is rational.

> **Remark.** The condition $P(0) = 0$ can be significantly weakened. The problem fails precisely when $P(0) = 0$ and for all cute t, $P^k(t) = 0$ for all sufficiently large k. A related result still holds, $r_k = \lfloor cm^k \rfloor + 1$ in this case.
>
> We also have that $\sum_{i=1}^{t} d_{k+i} > (t-1)m$. Thus, the digits of c are 'larger' than one would expect.

1.18 Rationals go to rationals

Proof. Let the rationals be $q_1, q_2, \cdots q_{n+1}$ and let $q_i = r_i$. Now, by the Lagrange interpolation formula, we can generate a polynomial but the terms we set up in that are all rationals, hence we are done. □

1.23 RMM 2018/2

We begin by differentiating both sides.

$$P'(x)P(x)^8(10P+9) = Q'(x)Q(x)^{19}(21Q+20)$$
$$\implies 10P+9 | Q'(x)Q(x)^{19}(21Q+20)$$

Now, $\deg P = \deg(10P+9) > \deg Q' + \deg(21Q+20)$, thus if we could show $\gcd(10P+9, Q) = 1$, we would be done and get that the answer is no but

$$\gcd(10P+9, P^9(P+1)) = 1 \implies \gcd(10P+9, Q^{20}(Q+1)) = 1 \implies \gcd(10P+9, Q) = 1$$

and we are done.

2.7 STEMS 2021

We claim that the answer is $\boxed{x^a}$. Now, assume not.
FTSOC let P be a polynomial not of this form that works. Now, $P = x^a Q(x)$ for some $a \in \mathbb{N}_0$ where $x \nmid Q$ and Q is non constant. Now, if P that satisfies problem conditions, then so does Q. Now, we only talk about Q.
Let b be a number such that $Q(2^b) \neq 0$. It exists as otherwise Q would have infinitely many roots. Now, let $\{p_1, p_2, \cdots p_k\}$ be the finite set of odd primes less than 10^{100}. Now, let $k_i = v_{p_i}(P(2^b))$ and $s_i = p_i^{k_i}(p-1)$.
Now, let $P = \prod_{i=1}^{k} s_i$. Now, consider $n = Pm + b$ where m is a variable large natural.
Now, observe that $2^{n-b} \equiv 1 \pmod{p_i^{k_i+1}}$. Thus, $P(n) \equiv P(2^b) \pmod{p_i^{k_i+1}}$. Thus, $v_{p_i}(P(n)) = k_i$.
Also, let us consider $v_2(P(n))$. Observe that for m large enough, we have that $v_2(0) < n$. Thus, we have $v_2(P(2^n)) = v_2(P(0))$ for large enough m.
Thus, for all primes less than 10^{100}, $v_p(P(2^n))$ is bounded and $P(2^n)$ has no larger prime factors. Thus, $P(2^n)$ is bounded. But as m gets arbitrarily large, 2^n gets arbitrarily large and thus $P(2^n)$ gets arbitrarily large. Contradiction!!

2.26 USATSTST 2016/3

This is kind of underwhelming, you can check that $Q(x) = 84(x^4-1)^2$ works.

4.12

Assume not, now FTSOC let $P(x) = \prod_{i=1}^{n}(x-a_i) - 1 = fg$ where f, g are monic integer polynomials. Now, $f(a_i)g(a_i) = -1 \implies \{f(a_i), g(a_i)\} = \{1, -1\} \implies f+g$ has roots $a_1, a_2, \cdots a_n$. But, $f+g$ has degree less than n and is not 0 as both f and g have leading coefficients 1. Contradiction!

4.13 ELMO 2012/3

This one is very nice! We can factorize the $(x^m - y^n)$ as polynomials over $x^{\frac{1}{n}}$ and $y^{\frac{1}{m}}$. Thus, $P(x,y) = x^m - y^n = \prod_{\omega_{mn}=1}(x^{\frac{1}{n}} - \omega y^{\frac{1}{m}})$. Now, if it is reducible then, there must be a multiple of mn factors involved. Thus, $x^m - y^n$ is irreducible!

5.17 Fermat's Last for polynomials

With factorization. FTSOC, assume such polynomials exist. Now, we pick the polynomials f, g with minimal $\deg f + \deg g$. Now, we also assume n is prime. Now, we can factorize $f^p + g^p = \prod_{\omega^p=1}(f+\omega g) = h^p$. Now, all these factors are co-prime, thus each must also be a pth power. Now, $(f+g)(-\omega) + (f+\omega g)(1+\omega) = f + \omega^2 g$. But, from the factorization, these 3 are perfect pth powers. Thus, we have a found a lower solution and we are done. □

Mason Stother's. $\max(\deg f^n, \deg g^n, \deg h^n) \leq \deg(rad(fgn)^n) - 1 \implies \frac{n(\deg f + \deg + \deg h)}{3} \leq \deg f + \deg g + \deg h - 1$ but $n \geq 3$ and thus, we are done. □

5.20 APMO 2018/5

First, we appeal to 4.5 so we have some n such that $P(x) - n$ is irreducible. Now, let α be a number such that $P(\alpha) = n$. Now, $P(x) - n$ has root α. Thus, α has minimal polynomial $P(x) - P(\alpha)$, thus it divides any integer polynomial with root α. Now, we know by the problem condition that $P(2\alpha)$ is also an integer. Thus, $P(x) - P(2\alpha)$ is also an integer polynomial. Thus, $P(x) - P(\alpha) | P(2x) - P(2\alpha)$. But, the leading coefficient of $P(2x)$ is $2^{\deg P}$ times the leading coefficient of P. Thus, $2^{\deg P}(P(x) - P(\alpha)) = P(2x) - P(2\alpha)$. Now, comparing coefficients, we have that all coefficients except first and last are 0. Now, we can do routine calculation to show that $P(x) = \pm x^n + c$.

5.23 LMAO Senior 2020 P6

I am including the official solution with permission here-
We claim that all polynomials P satisfying the given condition are $P(x) = x^m$ for $m \geq 2020$. It is easy to see that these polynomials do indeed satisfy the given conditions. Now we shall show that these are the only solutions

Lemma: Let A and B be 2 polynomials with integral co-efficients such that $\forall$ sufficiently large n, all prime factors of $A(n)$ divide $B(n)$ too. Then all irreducibles over $\mathbb{Q}[x]$ dividing A divide B too.
Proof: Let FSOC $\exists$ irreducible R over $\mathbb{Q}[x]$ such that R divides A but it doesn't divide B. We may assume WLOG that R is monic. Now since R is an irreducible and it doesn't divide B, $\gcd(R, B) = g$ for some $g \in \mathbb{Z}$. So $\forall n \in \mathbb{N}$ we have $a | B(n)$ and $a | R(n)$ implies $a | g$. By Schur's theorem, $\exists$ prime factor p of $R(n)$ for some sufficiently large $n \in \mathbb{N}$ such

that $p > |g|$. But now $p|R(n) \implies p|A(n) \implies p|B(n)$. So $p|g \implies |g| \geq p$ which is a contradiction. So our assumption that $\exists$ irreducible R over $\mathbb{Q}[x]$ such that. R divides A but it doesn't divide B was wrong. So all irreducibles over $\mathbb{Q}[x]$ dividing A divide B too. This proves the lemma.

Let's assume from now on that $P(n^{2020})|n^{P(n)} + P(P(n))\ \forall n > N$ for some N. Also let us define $|P(1) - P(0)|$ to be c.

Claim 1: Let $p|P(n^{2020})$ for some $n > N$. Then $p|n^{c+1} - n$.
Proof: Let $p|P(n^{2020})$ for some $n > N$. If $p|n$ then it is obvious. So let us assume $p \nmid n$. Let $k \in \mathbb{N}$. Then $n + pk \equiv n\ (mod\ p) \implies (n + pk)^{2020} \equiv n^{2020}\ (mod\ p) \implies P((n + pk)^{2020}) \equiv P(n^{2020})\ (mod\ p)$
So $p|P((n + pk)^{2020}) \implies p|P(P(n + pk)) + (n + pk)^{P(n+pk)}$.
But $p|P(n^{2020}) \implies p|P(P(n)) + n^{P(n)}$.
Now $n + pk \equiv n\ (mod\ p) \implies P(P(n + pk)) \equiv P(P(n))\ (mod\ p)$.
$(n + pk)^{P(n+pk)} \equiv n^{P(n+pk)}\ (mod\ p)$
$n + pk \equiv n + k\ (mod\ p - 1)$. So $P(n + pk) \equiv P(n + k)\ (mod\ p - 1)$. Hence by Fermat's little theorem, $n^{P(n+pk)} \equiv n^{P(n+k)}\ (mod\ p)$. So we have $(n + pk)^{P(n+pk)} \equiv n^{P(n+k)}\ (mod\ p)$.
Summing everything up we obtain that
$n^{P(n+k)} \equiv (n + pk)^{P(n+pk)} \equiv -P(P(n + pk)) \equiv -P(P(n)) \equiv n^{P(n)}\ (mod\ p)$.
This clearly implies that $\forall a, b > N$ we have $n^{P(a)} \equiv n^{P(b)}\ (mod\ p)$. Let t be the order of n modulo p. Then we have that $\forall a, b > N$, $t|P(a) - P(b)$. Choose $a, b > N$ s.t. $a \equiv 1\ (mod\ t)$ and $b \equiv 0\ (mod\ t)$. So $P(a) - P(b) \equiv P(1) - P(0)\ (mod\ t) \implies t|P(1) - P(0)$. So $n^c \equiv 1\ (mod\ p) \implies p|n^{c+1} - n$. This completes the proof of our claim.

Now if P is constant it is easy to see that $P \equiv 1$. But $P(0) \neq 1$. So P is non constant. Let $Q(x) = P(x^{2020})$ and let $T(x) = x^{c+1} - x$. Then applying the lemma on Q and T we obtain that every irreducible over $\mathbb{Q}$ dividing Q divides T too which implies that all roots of Q are roots of T too. But the roots of T are either roots of unity or 0. So all the roots of Q are either roots of unity or 0. So all roots of P too are either 0 or some roots of unity.

Claim 2: If $P(1) \neq 0$ then $P(1)|P(0) + 1$ and $P(1) = 0$ implies $P(0) = -1$.
Proof: Let $a|P(1)$ s.t. $a > 0$. Then choose $k > 0$ s.t. $1 + ak > N$. Then $a|P(1) \implies a|P(1 + ak) \implies a|P(P(1 + ak)) + (1 + ak)^{P(1+ak)}$. But $1 + ak \equiv 1\ (mod\ a)$. So we have $P(P(1 + ak)) \equiv P(P(1))\ (mod\ a)$. Also $P(1) \equiv 0\ (mod\ a)$. Hence $P(P(1)) \equiv P(0)\ (mod\ a)$. Also clearly $(1 + ak)^{P(1+ak)} \equiv 1\ (mod\ a)$. So we obtain $P(0) \equiv P(P(1)) \equiv P(P(1 + ak)) \equiv -(1 + ak)^{P(1+ak)} \equiv -1\ (mod\ a)$ or $a|1 + P(0)$. So all divisors of $P(1)$ divide $P(0) + 1$ too. Thus either $P(1) = 0$ and $P(0) + 1 = 0$ or $P(1)|P(0) + 1$ which is essentially the claim.

Case 1: $P(0) = 0$
Clearly $P(1)|P(0) + 1$ by claim 2. So $P(1)|1 \implies P(1) = 1$ or $P(1) = -1$. In any case $c = 1$. So $T(x) = x^2 - x$. This implies that roots of Q can be out of 1 or 0. But $Q(1) = P(1) \neq 0$. So only 0 can be a root of Q. We immediately obtain that 0 is only possible root of P too as $Q(x) = P(x^{2020})$. Also P is monic. From this we get $P(x) = x^k$ for some k. Plugging this into given divisibility condition we obtain the solutions $P(x) = x^m$ for $m \geq 2020$.

Case 2: $P(0) \neq 0$

So all roots of P are roots of unity. From this we obtain that modulus of constant co-efficient shall be 1. But P has integer co-efficients. So constant co-efficient must be 1 or -1 or in other words $P(0)$ is 1 or -1. But it is given that $P(0) \neq 1$. So $P(0) = -1$. Let's assume that $P(1) \neq 0$. Then if P is written as product of irreducibles we obtain that constant co-efficient of each irreducible is 1.(because if ω is a root of that irreducible then $\overline{\omega}$ is also a root,also $|\omega|$ =1 hence if ω is not real we have product of ω and $\overline{\omega}$ is 1. and if it is real it has to be 1 as $P(1) \neq 0$) So $P(0) = 1$ which is a contradiction. So $P(1) = 0$. So again $c = 1$. Hence $T(x) = x^2 - x$. From this we obtain roots of Q must be out of 0 and 1 only. But clearly $Q(-1) = P(1) = 0$ which means that -1 is a root of Q which is a contradiction. So we do not get any solutions from this case.

This completes the proof. Q.E.D.

6.15 IMO 2007/6

Proof. (writeup by Shourya Pandey)
Let us first try obvious upper bounds. The existence of $3n$ planes that satisfy the conditions of the problem is easy to find; simply take the planes $x = i, y = i$, and $z = i$ for all $1 \leq i \leq n$. See if you can find other constructions (I can think of one more construction).
Let us now try proving that this is indeed the answer. We know that the equation of a plane is of the form $ax + by + cz + d = 0$, for some $a, b, c, d \in \mathbb{R}$, where not all of a, b, c are 0. Somehow, the problem can be associated to CN, because we have $n + 1$ choices for each of x, y, z, similar to what we had in the theorem statement. This would seem to suggest that we should try to make some polynomial of degree $n + n + n = 3n$, such that it has a non-zero $x^n y^n z^n$ term. The $3n$ bound we got before may not be a coincidence. Of course, this all is just "wishful thinking".

Suppose the answer to the question was $k < 3n$. Now, we wish to apply CN and get a contradiction. The obvious way of getting a contradiction (via CN) is to construct a polynomial f as in the theorem statement, such that $f(s_1, s_2, \cdots, s_n) = 0$ for all $s_1 \in S_1, s_2 \in S_2, \cdots, s_n \in S_n$. So our aim is to find a polynomial $f \in \mathbb{F}(x, y, z)$ such that

- f has degree $n + n + n = 3n$.
- $x^n y^n z^n$ has a non-zero coefficient in f.
- $f(a, b, c) = 0$ for all $a, b, c \in \{0, 1, 2, \cdots, n\}$

If we are able to do this, then we are done, as we have contradicted the statement of CN.

Let us return to our assumption that $k < 3n$ planes work. Suppose the k planes that satisfy the conditions of the problem were $a_i x + b_i y + c_i z + d_i = 0$, where $1 \leq i \leq k$. Consider the polynomial $P \in \mathbb{R}[x, y, z]$ defined as

$$P(x, y, z) = \prod_{i=1}^{k} (a_i x + b_i y + c_i z + d_i)$$

This function satisfies $P(a, b, c)$ for all $(a, b, c) \in \{0, 1, \cdots, n\}^3$ except at $(0, 0, 0)$. Great. Let us try to think of another obvious polynomial that is 0 for all $(a, b, c) \in \{0, 1, \cdots, n\}^3$ except at $(0, 0, 0)$, **and such that it has degree** $3n$ **and a non-zero coefficient of** $x^n y^n z^n$. The reason for this will be clear in some time. There are several candidates

here. One of them, inspired by the observation that $1 \leq x+y+z \leq 3n$ for all points in $\{0,1,\cdots,n\}^3$ other than $(0,0,0)$, is

$$Q(x,y,z) = \prod_{i=1}^{3n}(x+y+z-i)$$

Another possibility is to choose the polynomial

$$R(x,y,z) = \prod_{i=1}^{n}(x-i)(y-i)(z-i)$$

which comes from our construction before. Note that both of them satisfy what we wanted (why?)

But what do we do with this? Consider the polynomial

$$f(x,y,z) = Q(x,y,z) + \alpha P(x,y,z)$$

where $\alpha = -\frac{Q(0,0,0)}{P(0,0,0)}$. We are done! This polynomial checks all items in the list we made before.

□

7.9 USATST 2021/7

Let $P = a_n x^n + a_{n-1}x^{n-1} + \cdots a_0$ with roots $\alpha_1, \alpha_2, \cdots$ and $P-1$ with roots $\beta_1, \beta_2, \cdots$. Now, as all roots are root of unity, we have that $|a_0| = |a_0 - 1|$. Thus, the real part must be the negative and $Re(a_0) = -Re(a_0 - 1) \implies Re(a_0) = 0.5$. Thus, $a_0 = \overline{1-a_0}$. Claim: $\forall i \in \{1,2,\cdots n-1\}, a_i = 0$. Proof: Let $a_i \neq 0$. Now, we have

$$\sum_{1 \leq x_1 < x_2 \cdots < x_{n-i} \leq n} \alpha_{x_1}\alpha_{x_2}\cdots\alpha_{x_{n-i}} = \sum_{1 \leq x_1 < x_2 \cdots < x_{n-i} \leq n} \beta_{x_1}\beta_{x_2}\cdots\beta_{x_{n-i}}$$

. But, we also have $\alpha_1\alpha_2\cdots\alpha_n \neq \beta_1\beta_2\cdots\beta_n$. Thus,

$$\sum_{1 \leq x_1 < x_2 \cdots < x_i \leq n} \frac{1}{\alpha_{x_1}\alpha_{x_2}\cdots\alpha_{x_i}} \neq \sum_{1 \leq x_1 < x_2 \cdots < x_i \leq n} \frac{1}{\beta_{x_1}\beta_{x_2}\cdots\beta_{x_i}}$$

Now, taking conjugates ($\overline{\alpha_j} = \frac{1}{\alpha_j}$ and same for β_j).

$$\sum_{1 \leq x_1 < x_2 \cdots < x_i \leq n} \alpha_{x_1}\alpha_{x_2}\cdots\alpha_{x_i} \neq \sum_{1 \leq x_1 < x_2 \cdots < x_i \leq n} \beta_{x_1}\beta_{x_2}\cdots\beta_{x_i}$$

But, we know this cannot be as a_{n-i} and a_n are common. Hence, $a_i = 0$ and the claim follows.

Now, we just have that $P = ax^n + c$ such that $|c| = |a|$ and $Re(c) = \frac{1}{2}$ and all such polynomials work.

7.14 Kronecker's Theorem

This proof is a gem and is thus included!
Let $\alpha_1, \alpha_2, \cdots \alpha_k$ be it's galois conjugates and itslef as α_0. Now, by 1.12(the fundamental theorem of symmetric polynomials), $P_j(x) = \prod_{0 \leq i \leq k}(x - \alpha_i^j)$ for any natural j is an integer polynomial.
But there are only finitely many integer polynomials which have all roots as roots of unity of degree $\leq k+1$ as we can bound each coefficient using the triangle inequality!
Thus, for infinitely many j, we have that $P_j(x)$ are same. Thus, we can write α_i for all i in two ways as α_0^k and α_0^l by infinite PHP. Thus, $\alpha_0^{k-l} = 1$. Thus, α_0 is a root of unity!

7.21 Very cute

We will prove via induction! Pick the pair polynomial which fails and has sum of degree of x_1 minimum.
Now, if this degree is 0, then we know that our result is true as it is true for functions in just x_2 so we assume that degree of x_1 is greater than 0. Now, when we say $\deg P$ or $\deg Q$, we refer only to degree of x_1. Now, WLOG $\deg P \geq \deg Q$
Now, let $A = \mathbb{C}(x_2)$ be the space of rational functions in x_2. Now, we can apply Euclidean Division in $\mathbb{C}(x_2)[x_1]$ and say $P = QS + R$ where S and R are in $A[x_1]$ and $\deg R < \deg Q$.
Thus, $S = \frac{S_1}{A_1}$ and $R = \frac{R_1}{B_1}$ where $S_1, R_1 \in \mathbb{C}[x_1, x_2]$ and $A_1, B_1 \in \mathbb{C}[x_2]$.
Thus, $PA_1B_1 = QS_1B_1 + R_1A_1$. Now, as P and Q share infinitely many roots, one of A_1 and R_1 shares infinitely many of these roots with P, Q. We have $\deg P \geq \deg Q > \deg R_1$ and $\deg P > 0 = \deg A_1$. So, we can replace the pair (P, Q) with (Q, A_1) or (Q, R_1) and the condition will still hold, contradicting the minimality of $\deg P + \deg Q$. Thus, $A_1R_1 = 0$. But, $A_1 \neq 0$. Thus, $R_1 = 0$. Thus, we have that $PA_1 = QS_1$. Now, if $\deg Q > 0$, we have that any irreducible factor of Q, containing x_1 is co-prime with A_1 and thus must divide P contradicting the assumption that P and Q are co-prime. Thus, $\deg Q = 0$. Now, Q has finitely many roots in x_2. For one of these roots, there are infinitely many values of x_1, that work. Thus, it must be a root of P as well and we are done.