Polynomnomnom

In algebra, NT, and combo!

Raymond Feng

December 11, 2020

Contents

§1 10 Common Approaches

1. For polynomials with integer coefficients, $a - b \mid P(a) - P(b)$.
2. Polynomials with different degrees grow at different rates.
3. Consider roots of polynomial.
4. Similar to 3: try factoring.
5. Odd degree polynomials must have at least 1 real root.
6. Take a derivative!
7. Shifting integer polynomials can be useful.
8. Let input to be "arbitrarily large" (building off of 2).
9. Draw a graph to visualize the problem.
10. For NT: Hensel's lifting lemma (building off 6).

§2 Exercises

Exercise 2.1 (TST 2014/4)**.** Let n be a positive even integer, and let $c_1, c_2, \ldots, c_{n-1}$ be real numbers satisfying

$$\sum_{i=1}^{n-1} |c_i - 1| < 1.$$

Prove that

$$2x^n - c_{n-1}x^{n-1} + c_{n-2}x^{n-2} - \cdots - c_1x^1 + 2$$

has no real roots.

Exercise 2.2 (IMO 1988/4)**.** Show that the solution set of the inequality

$$\sum_{k=1}^{70} \frac{k}{x-k} \geq \frac{5}{4}$$

is a union of disjoint intervals, the sum of whose length is 1988.

Exercise 2.3 (ISL 2010 N3)**.** Find the smallest number n such that there exist polynomials $f_1, f_2, \ldots, f_n$ with rational coefficients satisfying

$$x^2 + 7 = f_1(x)^2 + f_2(x)^2 + \ldots + f_n(x)^2.$$

Exercise 2.4 (Iran TST 2015/1/1)**.** Find all polynomials $P, Q \in \mathbb{Q}[x]$ such that

$$P(x)^3 + Q(x)^3 = x^{12} + 1.$$

Exercise 2.5 (RMM SL 2018 N1)**.** Determine all polynomials f with integer coefficients such that $f(p)$ is a divisor of $2^p - 2$ for every odd prime p.

Exercise 2.6 (RMM SL 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 $A^m = B^n$.

Exercise 2.7 (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?

Exercise 2.8 (ISL 2012 A4)**.** Let f and g be two nonzero polynomials with integer coefficients and $\deg f > \deg g$. Suppose that for infinitely many primes p the polynomial $pf + g$ has a rational root. Prove that f has a rational root.

Exercise 2.9 (ISL 2006 C3)**.** Let S be a finite set of points in the plane such that no three of them are on a line. For each convex polygon P whose vertices are in S, let $a(P)$ be the number of vertices of P, and let $b(P)$ be the number of points of S which are outside P. A line segment, a point, and the empty set are considered as convex polygons of 2, 1, and 0 vertices respectively. Prove that for every real number x

$$\sum_P x^{a(P)}(1-x)^{b(P)} = 1,$$

where the sum is taken over all convex polygons with vertices in S.

Exercise 2.10 (ISL 2013 A6)**.** Let $m \neq 0$ be an integer. Find all polynomials $P(x)$ with real coefficients such that

$$(x^3 - mx^2 + 1)P(x+1) + (x^3 + mx^2 + 1)P(x-1) = 2(x^3 - mx + 1)P(x)$$

for all real number x.

Exercise 2.11 (IMO 2002/3)**.** 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.

Exercise 2.12 (Iran TST 2014/2/3)**.** Prove that for all integers $k > 1$ the equation $(x+1)(x+2)\cdots(x+k) = y^2$ has finitely many solutions.

§3 Solutions

§3.1 TST 2014/4

Let n be a positive even integer, and let $c_1, c_2, \ldots, c_{n-1}$ be real numbers satisfying

$$\sum_{i=1}^{n-1} |c_i - 1| < 1.$$

Prove that

$$2x^n - c_{n-1}x^{n-1} + c_{n-2}x^{n-2} - \cdots - c_1x^1 + 2$$

has no real roots.

Let $a_i = c_i - 1$, so that

$$\sum_{i=1}^{n-1} |a_i| < 1.$$

Note that the polynomial becomes

$$2x^n - x^{n-1} + x^{n-2} - \cdots - x + 2 + \sum_{i=1}^{n-1} (-1)^i a_i x^i.$$

We will show that this quantity is positive for all real numberx x.

The desired inequality (for $x \neq -1$) is

$$x^n + 1 + \frac{x^{n+1} + 1}{x + 1} > \left| \sum_{i=1}^{n-1} (-1)^i a_i x^i \right|.$$

For $|x| < 1$, the RHS is less than 1, while the LHS is not, so we are done. For $|x| > 1$, the RHS is less than $\left|x^{n-1}\right|$, while the LHS is greater than x^n and $x^n > \left|x^{n-1}\right|$, so we are done again. Finally, the case of $x = -1$ can be directly plugged in to be shown that it fails. Thus, the polynomial has no real roots.

§3.2 IMO 1988/4

Show that the solution set of the inequality

$$\sum_{k=1}^{70} \frac{k}{x - k} \geq \frac{5}{4}$$

is a union of disjoint intervals, the sum of whose length is 1988.

In general, the total length of the solution set to

$$f(x) := \sum_{k=1}^{m} \frac{k}{x - k} \geq r$$

is given by $\frac{1}{r} \frac{m(m+1)}{2}$.

First, note that other than at its discontinuities, $f(x)$ is strictly decreasing since each addend is strictly decreasing other than at discontinuities. By IVT, this means that the solution set to the original inequality should be of the form

$$(1, 1+\varepsilon_1) \cup (2, 2+\varepsilon_2) \cup \cdots \cup (m, m+\varepsilon_m)$$

where $\varepsilon_i \in (0,1)$ and $i+\varepsilon_i$ are roots of $f(x) = r$.

It suffices to evaluate $\sum_{i=1}^{m} \varepsilon_i$. Considering $g(x) = \prod_{i=1}^{m}(x-i)^i$. It's clear that $f(x) = \frac{g'(x)}{g(x)}$.

Now, the roots of $g' - rg$ are exactly $i+\varepsilon_i$ for $1 \le i \le m$ and i with multiplicity $i-1$ for $1 \le i \le m$. Thus, the sum of the roots of $g' - rg$ is simply $\sum_{i=1}^{m} i^2 + \sum_{i=1}^{m} \varepsilon_i$. On the other hand, with $M = \binom{m+1}{2}$ and expanding, we have

$$g'(x) - rg(x) = -rx^M + x^{M-1}\left[M + r\left(1^2 + \cdots + m^2\right)\right] + \ldots,$$

implying that the sum of the roots of $g' - rg$ is $\sum_{i=1}^{m} i^2 + \frac{M}{r}$.

Equating, we get $\sum_{i=1}^{m} \varepsilon_i = \frac{M}{r} = \frac{1}{r}\frac{m(m+1)}{2}$, which is what we sought to prove.

§3.3 ISL 2010 N3

Find the smallest number n such that there exist polynomials $f_1, f_2, \ldots, f_n$ with rational coefficients satisfying

$$x^2 + 7 = f_1(x)^2 + f_2(x)^2 + \ldots + f_n(x)^2.$$

The minimal n is $n = 5$, achieveable at $(f_1, f_2, f_3, f_4, f_5) = (x, 2, 1, 1, 1)$.

> **Claim —** 7 cannot be represented as the sum of 3 rational squares.

Proof. The claim is equivalent to showing that there are no solutions to $x^2+y^2+z^2 = 7w^2$ other than $(0,0,0,0)$. WLOG assume $\gcd(x,y,z,w) = 1$.

If w is even, then considering the equation mod 4 we get $x^2 \equiv y^2 \equiv z^2 \equiv 0 \mod 4$, which is a contradiction since this means 2 divides all of x, y, z, w.

If w is odd, we get a contradiction by considering the equation mod 8 (since no 3 squares can sum to 7 mod 8).

This shows that there are no integer solutions, as desired. □

Now suppose there existed a construction for $n = 4$. Noting that not all of f_1, f_2, f_3, f_4 are monic linear functions, WLOG assume that f_1 is not a monic linear function. Then there exists rational x with $f_1(x) = x$ which implies that $7 = f_2(x)^2 + f_3(x)^2 + f_4(x)^2$. However, 7 cannot be represented as the sum of 3 rational squares, contradiction.

§3.4 Iran TST 2015/1/1

Find all polynomials $P, Q \in \mathbb{Q}[x]$ such that

$$P(x)^3 + Q(x)^3 = x^{12} + 1.$$

First, note that the LHS factorizes as $(P+Q)(P^2-PQ+Q^2)$ while the RHS factorizes as $(x^4+1)(x^8-x^4+1)$. It's easy to verify that x^4+1 and x^8-x^4+1 are irreducible in $Q[x]$, hence

$$\left\{P+Q, P^2+Q^2-PQ\right\} = \left\{k\left(x^4+1\right), k^{-1}\left(x^8-x^4+1\right)\right\}$$

for some constant k.

Now, note that $\deg(P^2-PQ+Q^2) = 2\max\{\deg P, \deg Q\} > \deg(P+Q)$, since if $\deg P = \deg Q$, the leading coefficient of $\deg(P^2-PQ+Q^2)$ is positive, and thus nonzero.

Thus, we must have $P+Q = k(x^4+1)$ and $P^2-PQ+Q^2 = k^{-1}(x^8-x^4+1)$. Now, we claim that $\deg P \neq \deg Q$. Suppose that their degrees were equal. Let p, q be the leading coefficients of P and Q. Now noting that $p^2-pq+q^2 > 0$, by the second equation earlier we deduce $\deg P = \deg Q = 4$. Therefore, as $P^3+Q^3 = x^{12}+1$, we have $p^3+q^3 = 1$ for rational p, q which is impossible by Fermat's Last theorem.

As $\deg P \neq \deg Q$, we may WLOG set $\deg P = 4$ and $\deg Q < 4$. The leading coefficient in $P+Q$ is then $p = k$, and the leading coefficient of P^2-PQ+Q^2 is $p^2 = k^{-1}$, thus $p^3 = 1 \implies p = k = 1$. Therefore, $P+Q = x^4+1$ and $P^2-PQ+Q^2 = x^8-x^4+1$, so $3PQ = (P+Q)^2 - (P^2-PQ+Q^2) = 3x^4$. From $\deg P = 4, \deg Q < 4$, and $p = 1$, we find that the only solution is $P(x) = x^4$ and $Q(x) = 1$ and its permutation, which clearly works.

§3.5 RMM SL 2018 N1

Determine all polynomials f with integer coefficients such that $f(p)$ is a divisor of $2^p - 2$ for every odd prime p.

The answer is $f(x) = 1, 2, 3, 6, x, 2x$ and their negations. Now we prove these are the only solutions.

> **Claim —** If p, q are primes with $p \mid f(q)$ then $p \in \{2, 3, q\}$.

Proof. Note that if $p \mid f(q)$ and $p \neq q$, then $q \not\equiv 0 \pmod{p}$ so we can enumerate all primes $q_1, q_2, \ldots$ such that $q_i \equiv q \pmod{p}$. For each i, we have

$$p \mid f(q), p \mid q - q_i \mid f(q) - f(q_i) \implies p \mid f(q_i) \mid 2(2^{q_i-1} - 1).$$

Recalling the well-known fact that $\gcd\left(2^a-1, 2^b-1\right) = 2^{\gcd(a,b)} - 1$, we get

$$p \mid \gcd\left(2\left(2^{q_1-1}-1\right), 2\left(2^{q_2-1}-1\right), \ldots\right) = 2\left(2^{\gcd(q_1-1, q_2-1, \ldots)} - 1\right).$$

Note that for each odd prime $r \neq p$ or for $r \in \{4, p^2\}$, by Dirichlet there exist q_j and q_k such that $q_j \not\equiv q_k \pmod{r}$ and $q_j \equiv q_k \equiv q \pmod{p}$, therefore $r \nmid \gcd(q_1 - 1, q_2 - 1, \dots)$ for all odd primes r and for $r \in \{4, p^2\}$. The above work implies $\gcd(q_1 - 1, q_2 - 1, \dots) \mid 2p$. This means

$$p \mid 2\left(2^{2p} - 1\right) \implies 2\left(2^2 - 1\right) \equiv 2\left(2^{2p} - 1\right) \equiv 0 \pmod{p} \implies p \in \{2, 3\},$$

as desired. □

Claim — $f(x) = c \cdot x^k$ for some constants c, k.

Proof. Let $f(x) = c \cdot x^k + g(x)$ with $\deg f > \deg g$, and let g have leading coefficient d. Furthermore assume WLOG $c > 0$ by negation if necessary. Taking massive primes $p \equiv 2 \pmod{3}$ means that $4 \nmid 2^p - 2$ and $9 \nmid 2^p - 2$. But since p is massive we also have

$$(c - 1) \cdot p^k < f(p) < (c + 1) \cdot p^k.$$

If $f(p) \neq c \cdot p^k$, then $\nu_p(f(p)) \leq k - 1$ so

$$\left| \frac{f(p)}{p^{\nu_p f(p)}} \right| \gg 6,$$

which yields a contradiction by the first claim (since 4 and 9 don't divide $f(p)$). Thus, $f(p) = c \cdot p^k$ for all large p, and since f is a polynomial then $f(x) = c \cdot p^k$ identically. □

Now by the second claim and $f(3) \mid 6$, we can extract the answers claimed in the beginning.

§3.6 RMM SL 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 $A^m = B^n$.

Let $A^m - B^n = P$. We are given that $\deg P \leq m - 1, n - 1$ want to show $P \equiv 0$. Taking the derivative of both sides then multiplying by A yields

$$mA^m A' - nB^{n-1}AB' = AP',$$

and substituting $A^m = P + B^n$ then gives

$$m\left(P + B^n\right)A' - nB^{n-1}AB' = AP'.$$

Rearranging, we have

$$B^{n-1}\left(mBA' - nAB'\right) = AP' - mA'P.$$

Claim — $AP' - mA'P = 0$.

Proof. Suppose not. Then by comparing degrees on both sides, we get (assuming $\deg B > 1$)

$$\begin{aligned}&(n-1)\deg B \le \deg A + \deg P - 1 \le \deg A + (n-1) - 1\\ \implies &\deg B - 1 < (n-1)(\deg B - 1) \le \deg A - 1.\end{aligned}$$

If $\deg A = 1$, we get an immediate contradiction. Otherwise $\deg A > 1$, and we can similarly get $\deg A - 1 < (m-1)(\deg A - 1) \le \deg B - 1$, contradiction. □

Now, suppose $P \neq 0$. Then by comparing leading coefficients of AP' and $mA'P$ we get

$$\deg P = m \deg A \ge m,$$

a contradiction. Thus, $P = 0 \implies A^m = B^n$, as desired.

§3.7 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?

TODO. The main idea is that drawing a graph will immediately tell you which terms to cancel and the sketch of the proof.

§3.8 ISL 2012 A4

Let f and g be two nonzero polynomials with integer coefficients and $\deg f > \deg g$. Suppose that for infinitely many primes p the polynomial $pf + g$ has a rational root. Prove that f has a rational root.

FSoC suppose that f has no rational roots.

Consider the rational function $h(x) = -\frac{g(x)}{f(x)}$. Since $\deg g < \deg f$, this means that $h(x)$ is only unbounded at asymptotes, or roots of f. As there are rational roots to $h(x) = p$ for infinitely many p, there is a subset of these primes $p_1 < p_2 < \dots$ such that the rational roots of $h(x) = p_i$ converge to a root r of f; we restrict our attention to these primes. As we assumed FSoC that f has no rational roots, then r is irrational.

Define $\frac{m_i}{n_i}$ with $\gcd(m_i, n_i) = 1$ to be the rational root of $h(x) = p_i$ (if there are multiple choose the one closest to r). Furthermore, let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ and $g(x) = b_{d-1}x^{d-1} + \cdots + b_0$ where $a_d \neq 0$.

> **Claim —** If $p_i \nmid n_i$ infinitely often, then r is rational.

Proof. For each i with $p_i \nmid n_i$, we must have $n_i \mid a_i$ by RRT, so some n_i appears infinitely often. Furthermore, since these $\frac{m_i}{n_i}$ converge to r, this gives that r is a rational number with denominator n_i, so f has a rational root, as desired. □

Claim — If $p_i \mid n_i$ infinitely often, then r is rational.

Proof. For all sufficiently large i let $n_i = p_i k_i$. Note that $p_i \nmid k_i$ since by RRT $n_i = p_i k_i \mid p_i a_d$ and $p_i \gg a_d$. Since $\frac{m_i}{p_i k_i}$ is a root of $p_i f + g$ this gives

$$a_d \left(\frac{m_i}{k_i}\right)^d + (p_i a_{d-1} + b_{d-1}) \left(\frac{m_i}{k_i}\right)^{d-1} + \cdots + (p_i^d a_0 + p_i^{d-1} b_0) = 0.$$

Taking this modulo p_i then yields

$$a_d \left(\frac{m_i}{k_i}\right) + b_{d-1} \equiv 0 \pmod{p_i}.$$

Thus, for some integer c_i we have

$$m_i = \frac{c_i p_i - b_{d-1}}{\frac{a_d}{k_i}} \implies \frac{m_i}{p_i k_i} = \frac{c_i - \frac{b_{d-1}}{p_i}}{a_d}.$$

Again noting that $\frac{m_i}{p_i k_i}$ must converge to r, this gives that c_i is a constant integer c for large enough i, implying that $\frac{m_i}{p_i k_i}$ converges to $\frac{c}{a_d}$, a rational number. Thus, $r = \frac{c}{a_d}$ is a rational root of f. □

Thus, in all cases r is rational, contradiction. Therefore, f has a rational root.

§3.9 ISL 2006 C3

Let S be a finite set of points in the plane such that no three of them are on a line. For each convex polygon P whose vertices are in S, let $a(P)$ be the number of vertices of P, and let $b(P)$ be the number of points of S which are outside P. A line segment, a point, and the empty set are considered as convex polygons of 2, 1, and 0 vertices respectively. Prove that for every real number x

$$\sum_P x^{a(P)}(1-x)^{b(P)} = 1,$$

where the sum is taken over all convex polygons with vertices in S.

Local Solution: First, we show the result for sets S such that all $|S| = n$ is a convex n-gon. This is simply the binomial theorem, since every subset of S is a convex polygon and we have

$$\sum_P x^{a(P)}(1-x)^{b(P)} = \sum_{i=0}^{n} \binom{n}{i} x^i (1-x)^{n-i} = 1.$$

Next, we show that if S satisfies the property in the problem, then we can move any point arbitrarily. Consider the set of lines that go through exactly 2 points of S. Then let us move one of the points X until it first crosses one of these lines, and let that line pass through A and B with $A, B \in S$. Then consider any convex polygon P that contained A, B, X before the movement. That polygon no longer exists, so we have to subtract

$$x^{a(P)}(1-x)^{b(P)}.$$

However, consider the convex polygon P' which consists of all points except P. Since AB is the first line that X crosses, then the change in the value of $x^{a(P')}(1-x)^{b(P')}$ is

$$x^{a(P)-1}(1-x)^{b(P)} - x^{a(P)-1}(1-x)^{b(P)+1}.$$

Thus, the net change related to P is

$$-x^{a(P)}(1-x)^{b(P)} + x^{a(P)-1}(1-x)^{b(P)} - x^{a(P)-1}(1-x)^{b(P)+1} = 0.$$

Similar arguments show that for any convex polygon P that contains A, B, X after the movement also have net change 0. Thus, moving a point across one line has no effect on the sum

$$\sum_P x^{a(P)}(1-x)^{b(P)} = 1.$$

Therefore, starting from the convex n-gon, which we showed to have sum 1, we can move points until we get any set S, and we are done.

Probability Solution: Color the points of S either white or black with probability p of being white. Then the sum

$$\sum_P p^{a(P)}(1-p)^{b(P)} = 1,$$

simply represents the probability that there exists an entirely white convex polygon such that every point outside it is black. But this probability is 1, since the convex hull of all white points always works. Thus, the equality holds for all $0 < x < 1$. But the sum is a polynomial of finite degree, thus the equality can be extended to all real numbers x, as desired.

§3.10 ISL 2013 A6

Let $m \neq 0$ be an integer. Find all polynomials $P(x)$ with real coefficients such that

$$(x^3 - mx^2 + 1)P(x+1) + (x^3 + mx^2 + 1)P(x-1) = 2(x^3 - mx + 1)P(x)$$

for all real number x.

It's easy to check that $P(x) = cx$ are all valid solutions. We'll show there are no other solutions.

Define the polynomial

$$Q(x) := (x-1)P(x) - xP(x-1).$$

It's easy to verify that the given rewrites as

$$Q(x+1) \cdot \left(x^3 - mx^2 + 1\right) = Q(x) \cdot \left(x^3 + mx^2 + 1\right). \qquad (\clubsuit)$$

Claim — There is a root r of $x^3 - mx^2 + 1$ such that no element of $r + \mathbb{Z}$ is a root of $x^3 + mx^2 + 1$.

Proof. For $m = 2$, take the root $r = 1$. This works since $x^3 + 2x^2 + 1$ has no integer roots.

Otherwise, RRT tells us that $x^3 - mx + 1$ has 3 irrational roots r, s, t; this means that r, s, t are Galois conjugates. Therefore, $r + a, s + a, t + a$ are Galois conjugates for all integers a.

We claim that taking r works. FSoC suppose a is an integer such that $r + a$ is a root of $x^3 + mx^2 + 1$, then so are $s + a$ and $t + a$. By Vieta, this gives $r + s + t = m$ and $r + s + t + 3a = -m$ which means $3a = -2m$. Furthermore, from constant term comparisons we have

$$-1 = (r + a)(s + a)(t + a) = -\left((-a)^3 - m(-a)^2 + 1\right) \implies a^3 + a^2 m = 0,$$

therefore $a = 0$ or $a = -m$. In conjunction with $3a = -2m$, this means $a = m = 0$ which is a contradiction. □

Claim — $Q(x) \equiv 0$.

Proof. FSoC suppose $Q(x) \not\equiv 0$, so it has finitely many roots. Then take $x = r$ in (♣) as a root of $x^3 - mx^2 + 1$ from the first claim. This yields r is a root of $Q(x)$. Now, plug in $x = r - 1$. Since no element of $r + \mathbb{Z}$ is a root of $x^3 + mx^2 + 1$, this means that $r - 1$ is a root of $Q(x)$. Continuing downwards, we get $r - i$ for all positive integers i are roots of $Q(x)$, which is a contradiction. □

Thus, we have $Q(x) \equiv 0 \implies (x - 1)P(x) \equiv xP(x - 1)$. This gives

$$\frac{P(x)}{x} = \frac{P(x - 1)}{x - 1}$$

for all $x \neq 0, 1$, implying that $P(x) \equiv cx$ for some constant c, as desired.

§3.11 IMO 2002/3

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.

First, using the division algorithm for monic polynomials in $\mathbb{Z}[x]$, we have that

$$x^m + x - 1 = Q(x)(x^n + x^2 - 1) + R(x)$$

for some polynomials $Q(x), R(x) \in \mathbb{Z}[x]$ such that $\deg(R) < n$. Suppose that R is not the 0 polynomial. Then, for all sufficiently large a, $R(a) < a^n + a^2 - 1$, thus

$$a^n + a^2 - 1 \nmid a^m + a - 1$$

so the divisibility will only hold for finitely many a, contradiction. Therefore, R is the 0 polynomial.

By IVT, since $1^n+1^2-1>0$ and $0^n+0-1<0$, we may let r be a root of $x^n+x^2-1=0$ such that $0<r<1$. Since R is the 0 polynomial, that implies that r is also a root of $x^m+x-1=0$. As $1=r^n+r^2>r^n+r^{n+1} \implies \frac{1}{1+r}>r^n$, this means that

$$r^m=1-r=\frac{1-r^2}{1+r}=\frac{r^n}{1+r}>r^n\cdot r^n=r^{2n}.$$

Thus, $m<2n$.

Furthermore, another consequence of R being the zero polynomial is that the divisibility must hold for all a. Note that

$$a^n+a^2-1 \mid a^m+a-1 \implies a^n+a^2-1 \mid a^{m+1}+a^m+a^2-1 \implies a^n+a^2-1 \mid a^{m-n+1}+a^{m-n}-1.$$

Consider the case when $m=2n-1$. Then

$$a^n+a^2-1 \mid a^n+a^{n-1}-1 \implies a^n+a^2-1 \mid a^{n-1}-a^2$$

which fails for sufficiently large a unless $n-1=2 \implies (m,n)=(5,3)$. Thus, the only solution in this case is $m=5, n=3$. This is easily verified since $(a^3+a^2-1)(a^2-a+1)=a^5+a-1$.

If $m<2n-1$, then for all sufficiently large a, the divisilibity

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

fails, so no solutions in this case.

To conclude, the only solution is $m=5, n=3$.

§3.12 Iran TST 2014/2/3

Prove that for all integers $k>1$ the equation $(x+1)(x+2)\cdots(x+k)=y^2$ has finitely many solutions.

First, the assertion is true for even k because the LHS is clearly not the square of a polynomial, but it is a monic polynomial of even degree; for sufficiently large x, bounding will show that $(x+1)\cdots(x+k)$ cannot equal a square, so we are done.

Now, suppose k is odd. Suppose FSoC that there are infinitely many x which satisfy the given condition. Then we can fix an x which is arbitrarily large satsifying the condition.

Define $s(n)$ to be the squarefree part of n. Note that for primes $p \geq k$, $p \nmid s(x+i)$ for $1 \leq i \leq k$ since $p \mid x+i$ for at most one value of $1 \leq i \leq k$ and as the LHS is a square, then $2 \mid \nu_p(x+i)$ for that value of i, so p does not divide $s(x+i)$ for any i.

Enumerate the primes $2=p_1<p_2<\cdots<p_l<k$. Then consider the vector in $\mathbb{F}_2^l$ for each $1 \leq i \leq k$ given by

$$\langle \nu_{p_1}(x+i) \pmod 2, \nu_{p_2}(x+i) \pmod 2, \ldots, \nu_{p_l}(x+i) \pmod 2 \rangle.$$

Since $k>l+1$, then not all of these vectors can be linearly independent in $\mathbb{F}_2^l$, thus some subset of the vectors of size at most $l+1$ sums to the 0 vector in $\mathbb{F}_2^l$. The complement

of that set of vectors also sums to the 0 vector, since $(x+1)\cdots(x+k)$ is a perfect square.

Thus, some *nonempty* subset $A \subseteq \{1, 2, \ldots, k\}$ with $|A|$ even satisfies

$$\prod_{i \in A}(x+a) = z^2$$

for some integer z. But note that we took x sufficiently large, and this product is a monic, even degree, nonsquare polynomial in x, which is only a perfect square a finite number of times, contradiction.