MOP experiment (condensed version of analysis and algebra/polynomials/NT)

Victor Wang

July 31, 2014

(See Dropbox: `https://www.dropbox.com/sh/1pd5bjm3038gku2/AACyg9LWs6xFGafWYRAG4lc0a` (or if/once that link breaks, my website, `http://web.mit.edu/vywang/www/`) for the latest version. Email me at vywang (at) mit.edu for errors/comments/suggestions or to discuss anything, e.g. where to look for more of these kinds of problems or topics.)

Recommendation: Work on the topic/problems you think would help you the most.[1] Of course, if you don't feel like doing geometry that's fine; there's an algebra class tomorrow anyways.

Also, while it's important to be able to find certain ideas on your own, I encourage you to occasionally work in small groups, both in and out of class; I think you can gain a surprising amount of intuition just by talking to others. This might be easier to coordinate out of class, especially for the harder problems.

1 Algebra/polynomials, mostly with number theory

1. (Finite fields, concrete/elementary perspective[2]) Let f be a *monic* irreducible degree $d \geq 1$ polynomial *modulo* p (i.e. in $\mathbb{F}_p[x]$), for some prime p.

   (a) Show that $f(x) \mid g(x)^{p^d} - g(x)$ in $\mathbb{F}_p[x]$ for any $g \in \mathbb{F}_p[x]$.

   (b) Show that $x^{p^r} - x \mid g(x)^{p^r} - g(x)$ for any $g \in \mathbb{F}_p[x]$ and positive integer r.

   (c) For positive integers r, show that $f(x) \mid x^{p^r} - x$ modulo p if and only if $d \mid r$.

   (d) $f(x) \mid g(x)^p - g(x)$ in $\mathbb{F}_p[x]$ for some $g \in \mathbb{F}_p[x]$ if and only if $g(x) \pmod{f(x)}$ is a constant.

   (e) Show that $f(t) - \prod_{k=0}^{d-1}(t - x^{p^k}) \in (\mathbb{F}_p[x])[t]$ (i.e. a polynomial in t with coefficients in $\mathbb{F}_p[x]$) is the zero polynomial (in t) modulo $f(x)$, in the sense that its coefficients in t are all divisible by $f(x)$ modulo p (in $\mathbb{F}_p[x]$).

   (f) What do these mean, abstractly? (Don't worry if you haven't seen this before; you can probably find this interpretation in any standard abstract algebra book.)

   (g) (ELMO Shortlist 2013, W.) We define the *Fibonacci sequence* $\{F_n\}_{n\geq 0}$ by $F_0 = 0$, $F_1 = 1$, and for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$; we define the *Stirling number of the second kind* $S(n,k)$ as the number of ways to partition a set of $n \geq 1$ distinguishable elements into $k \geq 1$ indistinguishable nonempty subsets.

   For every positive integer n, let $t_n = \sum_{k=1}^{n} S(n,k)F_k$. Let $p \geq 7$ be a prime. Prove that $t_{n+p^{2p}-1} \equiv t_n \pmod{p}$ for all $n \geq 1$.

   (h) (Putnam 2011) Let p be an odd prime. Show that $\sum_{k=0}^{p-1} k!x^k \in \mathbb{F}_p[x]$ has at most $(p-1)/2$ roots (modulo p).

[1] I remember last year I felt like I wasn't getting anything out of around half of the classes. It's a pity if you're not learning at least one really new/interesting thing every day.

[2] This is only one of many approaches to finite fields. Another common route is to consider the splitting field of $x^{p^r} - x$ (basically [up to isomorphism] the smallest field where it fully factors, and we can use our intuition from complex polynomials and FTA), which behaves nicely by the Frobenius endomorphism: $(x+y)^{p^r} = x^{p^r} + y^{p^r}$. (In the approach above Frobenius doesn't have as central a role.)

(i) (Polya, PFTB) Suppose that $(a_n)_{n\geq 1}$ is a linear recurrence sequence of integers such that n divides a_n for all positive integers n. Prove that (a_n/n) is also a linear recurrence sequence.

2. (Putnam 1956 B7?) The nonconstant polynomials $P(z)$ and $Q(z)$ with complex coefficients have the same set of numbers for their zeros but possibly different multiplicities. The same is true of the polynomials $P(z)+1$ and $Q(z)+1$. Prove that $P(z)=Q(z)$.

3. (I wish I knew more about valuations)

   (a) (Classical?) Let n be a positive integer and a a complex number. If na^k is an algebraic integer for all integers $k\geq 0$, show that a is an algebraic integer itself.

   (b) (MIT Problem-Solving Seminar) Let $f(x)=a_0+a_1x+\cdots\in\mathbb{Z}[[x]]$ be a formal power series with $a_0\neq 0$. Suppose that $f'(x)f(x)^{-1}\in\mathbb{Z}[[x]]$. Prove or disprove that $a_0\mid a_n$ for all $n\geq 0$.

   (c) What's the relation between (a) and (b)?

4. (More practical "valuations", but take this with a grain of salt since I don't fully know what I'm talking about)

   (a) Let $\zeta=e^{2\pi i/p}$ for some prime p. From $(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1})=p$, what can you say about $\frac{(1-\zeta)^{p-1}}{p}$ as an algebraic number? (Something similar works for prime powers, but not for other numbers.)

   (b) (2012-2013 Winter OMO, W.) ω is a primitive 2013th root of unity. Find the number of ordered pairs of integers (a,b) with $1\leq a,b\leq 2013$ such that $\frac{(1+\omega+\cdots+\omega^a)(1+\omega+\cdots+\omega^b)}{3}$ is an algebraic integer.

   (c) (St. Petersburg 2003, PFTB). Let p be a prime and let $n\geq p$ and $a_1,a_2,\ldots,a_n$ be integers. Define $f_0=1$ and f_k the number of subsets $B\subseteq\{1,2,\ldots,n\}$ having k elements and such that p divides $\sum_{i\in B}a_i$. Show that $f_0-f_1+f_2-\cdots+(-1)^nf_n$ is a multiple of p.

   (d) (China 2011) Show that for all positive integers r, $v_2\left(\sum_{k=-n}^{n}\binom{2n}{n+k}k^{2r}\right)\geq v_2((2n)!)$.

   (e) (W., adapted from Gabriel Dospinescu, PFTB, 2010 MR U160) Let p be a prime and let n,s be positive integers. Prove that $v_p\left(\sum_{p\mid k,0\leq k\leq n}(-1)^kk^s\binom{n}{k}\right)\geq v_p(n!)$.

   (f) (Gabriel Dospinescu, PFTB) Let $p>2$ be a prime number and let m and n be multiples of p, with n odd. For any function $f:\{1,2,\ldots,m\}\to\{1,2,\ldots,n\}$ satisfying $\sum_{k=1}^{m}f(k)\equiv 0\pmod p$, consider the product $\prod_{k=1}^{m}f(k)$. Prove that the sum of these products is divisible by $\left(\frac{n}{p}\right)^m$. (Yes, we can strengthen it easily.)

5. (I wish I knew more commutative algebra/algebraic geometry)

   (a) Prove that $\mathbb{C}[x,y]$ has unique factorization into irreducible (two-variable complex) polynomials (up to constant). (It suffices to show every *irreducible* polynomial is *prime*, i.e. if some nonconstant p is irreducible and $p\mid ab$, then $p\mid a$ or $p\mid b$.)

   (b) (Ineffective Bézout's theorem) Prove that two relatively prime polynomials $f,g\in\mathbb{C}[x,y]$ share finitely many common zeros in the complex plane.

   (c) i. (Artin's *Algebra*) Let $x(t),y(t)$ be complex polynomials, not both constant. Show that there exists a polynomial $m\in\mathbb{C}[x,y]$ such that for $f\in\mathbb{C}[x,y]$, we have $m\mid f$ if and only if $f(x(t),y(t))=0$ for all $t\in\mathbb{C}$.

   ii. The following can be done in more than one order:
   (i) Prove that m is irreducible in $\mathbb{C}[x,y]$.
   (ii) Prove that m is unique up to a constant factor.
   (iii) For a point $(a,b)\in\mathbb{C}^2$, prove that $m(a,b)=0$ if and only if there exists $t\in\mathbb{C}$ such that $(x(t),y(t))=(a,b)$.

6. (a) (Putnam 2013 B6) Let p be an odd prime number such that $p \equiv 2 \pmod 3$. Define a permutation π of the residue classes modulo p by $\pi(x) \equiv x^3 \pmod p$. Show that π is an even permutation if and only if $p \equiv 3 \pmod 4$.

   (b) (2013-2013 Winter OMO, W.) Find the remainder when $\prod_{i=0}^{100}(1 - i^2 + i^4)$ is divided by 101.

   (c) (Noga Alon, Jean Bourgain; TST 2014) For a prime p, a subset S of residues modulo p is called a *sum-free multiplicative subgroup* of $\mathbb{F}_p$ if

   (i) there is a nonzero residue α modulo p such that $S = \{1, \alpha^1, \alpha^2, \dots\}$ (all considered mod p), and

   (ii) there are no $a, b, c \in S$ (not necessarily distinct) such that $a + b \equiv c \pmod p$.

   Prove that for every integer N, there is a prime p and a sum-free multiplicative subgroup S of $\mathbb{F}_p$ such that $|S| \geq N$.

   (d) The TST problem, but with (ii) replaced by (ii') $0 \notin a_1S + a_2S + \cdots + a_kS$, for fixed integers a_i *with nonzero sum*. (In (ii) these integers are $+1, +1, -1$.)

   (e) (PFTB, AMM 10748) Let p, q be prime numbers and let r be a positive integer such that $q \mid p-1$, $q \nmid r$, and $p > r^{q-1}$. Let $a_1, \dots, a_r$ be integers such that $a_1^{(p-1)/q} + \cdots + a_r^{(p-1)/q}$ is a multiple of p. Prove that at least one of the a_i's is a multiple of p.

7. (a) (ELMO 2012, Bobby Shen) A diabolical combination lock has n dials (each with c possible states), where $n, c > 1$. The dials are initially set to states $d_1, d_2, \dots, d_n$, where $0 \leq d_i \leq c-1$ for each $1 \leq i \leq n$. Unfortunately, the actual states of the dials (the d_i's) are concealed, and the initial settings of the dials are also unknown. On a given turn, one may advance each dial by an integer amount c_i ($0 \leq c_i \leq c-1$), so that every dial is now in a state $d_i' \equiv d_i + c_i \pmod c$ with $0 \leq d_i' \leq c-1$. After each turn, the lock opens if and only if all of the dials are set to the zero state; otherwise, the lock selects a random integer k and cyclically shifts the d_i's by k (so that for every i, d_i is replaced by d_{i-k}, where indices are taken modulo n).

   Show that the lock can always be opened, regardless of the choices of the initial configuration and the choices of k (which may vary from turn to turn), if and only if n and c are powers of the same prime.

   (b) ($\mathbb{Q}[x]$ representations of n-sequences $\pmod m$, W.) Let $n, m > 1$ be positive integers. We say a sequence $(a_1, a_2, \dots, a_n) \in (\mathbb{Z}/m\mathbb{Z})^n$ is *satisfied* by the integer-valued polynomial $f \in \mathbb{Q}[x]$ if $f(x) \equiv a_i \pmod m$ whenever $x \equiv i \pmod n$.

   (i) Show that n and m are powers of the same prime if and only if every sequence $(a_1, a_2, \dots, a_n) \in (\mathbb{Z}/m\mathbb{Z})^n$ is satisfied by some polynomial $f(x)$.

   (ii) If $n = p^i$ and $m = p^j$ for a prime p and two positive integers i, j, find (in terms of p, i, j) the smallest positive integer M such that every sequence $(a_1, a_2, \dots, a_n) \in (\mathbb{Z}/m\mathbb{Z})^n$ is satisfied by a polynomial $f(x)$ of degree at most M.

2 Analytic-flavored stuff

1. Let's pretend this is analytic number theory.

   (a) (2013-2014 Spring OMO, W.) Warm-up. Classify pairs (m, n) of integers such that $x^3 + y^3 = m + 3nxy$ has infinitely many integer solutions (x, y).

   (b) (Sierpinski, PFTB) Prove that for all N there exists a k such that more than N prime numbers can be written in the form $f(T) + k$ for some integer T, where $f \in \mathbb{Z}[x]$ is a nonconstant monic polynomial.

   (c) (China 2012) Given an integer $n \geq 4$. $S = \{1, 2, \dots, n\}$. A, B are two subsets of S such that $ab + 1$ is a perfect square for all $a \in A$, $b \in B$. Prove that $\min\{|A|, |B|\} \leq \log_2 n$.

   (d) (Russia 2002) Show that the numerator of the reduced fraction form of $H_n = 1/1 + 1/2 + \cdots + 1/n$ is infinitely often not a prime power.

2. (MOP 2007?) $\{a_n\}_{n=1}^{\infty}$ is a sequence satisfying $0 < a_n \leq a_{n+1} + a_{n^2}$ for all natural numbers n. Is $\sum_{n=1}^{\infty} a_n$ necessarily divergent?

3. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{C}[x]$ has roots $z_1, \ldots, z_n \in \mathbb{C}$ (not necessarily distinct).

   (a) (Mahler measure bound) Prove that $\prod_{k=1}^{n} \max(1, |z_k|) \leq \sqrt{1 + |a_{n-1}|^2 + \cdots + |a_0|^2}$.

   (b) (China TST 2003) Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{C}[x]$ has roots $z_1, \ldots, z_n \in \mathbb{C}$. If $\sum_{k=0}^{n-1} |a_k|^2 \leq 1$, show that $\sum_{k=1}^{n} |z_k|^2 \leq n$.

   (c) (MOP 2011) Prove that $\frac{1}{n}\sum_{k=1}^{n} |z_k|^2 < 1 + \max_{1 \leq k \leq n} |a_{n-k}|^2$.

4. (Iterated stuffs)

   (a) (Math Prize 2012) Define $L(x) = x - \frac{x^2}{2}$ for every real number x. Prove that $\lim_{n\to\infty} nL^n(17/n)$ exists, and compute its value explicitly.

   (b) (Putnam 2012) Suppose that $a_0 = 1$ and that $a_{n+1} = a_n + e^{-a_n}$ for $n = 0, 1, 2, \ldots$. Does $a_n - \ln n$ have a finite limit as $n \to \infty$?

   (c) (Putnam 2006) Let $k > 1$ be an integer. Suppose $a_0 > 0$ and define $a_{n+1} = a_n + a_n^{-1/k}$ for $n \geq 0$. Evaluate $\lim_{n\to\infty} a_n^{k+1}/n^k$.

5. (Real roots and interlacing, HroK's blog[3]) The intermediate value theorem and Rolle's theorem are ubiquitous principles in the analysis of real roots of continuous and differentiable functions, respectively.

   As you are likely familiar with the most standard uses of these theorems, we briefly discuss the phenomenon of *interlacing* functions f, g with alternating real roots. (For a much more unified coverage, see Steve Fisk's paper Polynomials, roots, and interlacing.) In particular, we look at polynomial recurrences, which provide some of the most natural examples of interlacing.

   (a) Let's first give an example: The n^{th} Hermite polynomial $H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}$ has all real roots (by induction one easily verifies that H_n is a polynomial of degree n).

   Indeed, we induct to show that for every $n \geq 1$, $h_n(x) = \frac{d^n}{dx^n} e^{-x^2}$ has exactly n roots, where the base case is obvious. But if for some $n > 1$ we assume that $h_{n-1}(x)$ has $n-1$ real roots $a_1 < \cdots < a_{n-1}$, then noting that $\pm\infty$ are also roots and $h_n = \frac{d}{dx} h_{n-1}$, we're done by Rolle's theorem. Obseve that h_n, h_{n-1} interlace, i.e. the roots of h_{n-1} lie in between those of h_n.

   Of course, there are several variations on the same idea. For example, if we have a recurrence like $p_n(x) = xp_{n-1}(x) + p_{n-2}(x)$ and we know that p_{n-1}, p_{n-2} interlace, then under some mild conditions we can show via the IVT that p_n, p_{n-1} and p_n, p_{n-2} also interlace (of course, we need p_n, p_{n-1}, p_{n-2} to have degrees within one of each other). This is in essence the idea behind, for instance, Sturm's theorem.

   Now for some problems, (very) roughly arranged in difficulty order!

   (b) (Steve Fisk) Suppose $\{a_i\}, \{b_i\}, \{c_i\}$ are sequences of reals where all a_i, c_i are positive and the b_i are unrestricted. Define a sequence of polynomials recursively by $p_{-1} = 0$, $p_0 = 1$, and $p_i = (a_i x + b_i)p_{i-1} - c_i p_{i-2}$ for $i > 1$. Show that $p_n(x)$ has all real roots for every positive integer n.

   (c) Prove Sturm's theorem.

   (d) (ELMO Shortlist 2012, David Yang) Prove that any polynomial of the form $1 + a_n x^n + a_{n+1}x^{n+1} + \cdots + a_k x^k$ $(k \geq n)$ has at least $n-2$ non-real roots (counting multiplicity), where the a_i $(n \leq i \leq k)$ are real and $a_k \neq 0$.

   (e) Prove Newton's inequalities.

[3] If you're interested in contributing to this excellent blog, ask me for the password.

(f) (Descartes' rule of signs) For a polynomial $p \in \mathbb{R}[x]$, let $z(p)$ denote the number of positive zeros and $v(p)$ the number of sign changes.

(i) Show that $2 \mid z(p) - v(p)$.

(ii) Prove that $z(p) \leq v(p)$ by writing $p = (x - r)q$ for some positive real root r of $p(x)$ and inducting on $\deg p$.

(iii) Prove that $z(p) \leq v(p)$ by considering the derivative $p'(x)$ (assuming WLOG that $p(0) \neq 0$) and inducting on $\deg p$.

(g) (Classical) Show that out of all monic polynomials of a fixed degree n, $T_n(x)/2^{n-1}$ attains the smallest maximum absolute value on the interval $[-1, 1]$, where $T_n(x)$ denotes the n^{th} Chebyshev polynomial of the first kind.

(h) (MOP 1999) Given n points on the unit circle such that the product of the distances from any point on the circle to the given points does not exceed 2, prove that the points must be vertices of a regular n-gon.

(i) (MOP 2001) Let $P(x)$ be a real-valued polynomial with $P(n) = P(0)$. Show that there exist at least n distinct (unordered) pairs of distinct real numbers $\{x, y\}$ such that $x - y \in \mathbb{Z}$ and $P(x) = P(y)$. Does this necessarily hold if we allow P to be any continuous function?

(j) (USAMO 2002) Prove that any monic polynomial of degree n with real coefficients is the average of two monic polynomials of degree n with n real roots.

(k) (MOP 2007) Let a be a real number. Prove that every nonreal root of $f(x) = x^{2n} + ax^{2n-1} + \cdots + ax + 1$ lies on the unit circle and f has at most 2 real roots.

(l) (ELMO Shortlist 2011, Evan O'Dorney) If $a + b + c = a^n + b^n + c^n = 0$ for some positive integer n and complex a, b, c, show that two of a, b, c have the same magnitude.

(m) ("Enzo", MathOverflow) For $n \geq 1$, let

$$P_n(x) = x^{n+1} \left[\frac{\partial^{2n+1}}{\partial z^{2n+1}} \frac{\sinh(z)}{\cosh(z) - 1 + x} \right]_{z=0}.$$

Prove that $P_n(x)$ is a polynomial of degree n with every root real and strictly greater than 2.