Putnam Notes
Polynomials and palindromes

Polynomials show up one way or another in just about every area of math. You will hardly ever see any math competition without at least one problem explicitly concerning polynomials; occasionally you find one where they show up in an implicit way — later.

It is well-known that not every polynomial over the reals has a full set of roots. (I mean, $x^2 + 1$ has no real roots, for instance.) But they almost do; every constant polynomial over the complex numbers factors into degree one polynomials. So if we count the roots with multiplicity, a polynomial of degree n has n roots. This easily implies that, if $p(x)$ is a nonconstant polynomial over the reals, then it factors into polynomials of degree one and two.

[I hope I don't need to explain any of the terminology of the last paragraph. I am willing to do so, but this stuff is really basic. So — I hope — is the direct connection between factoring and finding roots. Incidentally, on the Putnam and most other competitions, the word "number" is usually a real number. If it's more restricted or more general or just different, this is usually either clear from context or made explicit.]

Our first problem is actually standard, but it showed up on the Putnam, to my surprise.

PROBLEM 1 (A2, 1999). Show that if $p(x)$ is a polynomial such that $p(a) \geq 0$ for all a, then there are polynomials $p_1, \ldots, p_k$ such that $p(x) = \sum_{j=1}^{k} p_j(x)^2$.

[Note that there is no mention of what kind of number a is, or what the coefficients are. Thus they are all real by default. k must be a positive integer, because nothing else makes sense.]

Solution: This is done (like a lot of these things) by induction on the degree n of p. The cases $n = 0$ and $n = 1$ are trivial. We suppose that the result is true for any polynomial q with degree $m < n$.

We have that, if $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, then

$$p(x) = a_n(x - r_1)^{d_1}(x - r_2)^{d_2} \cdots (x - r_\ell)^{d_\ell}(x^2 + b_1 x + c_1)^{e_1} \cdots (x^2 + b_t x + c_t)^{e_t},$$

where r_1,...,r_ℓ are the distinct real roots (if any) and each $x^2 + b_s x + c_s$ (if any) is irreducible over the reals — that is, it is positive for every real x.

Let's assume for simplicity of notation that $a_n = 1$. (Without loss of generality, right? — I mean it has to positive (why?), so...) We first consider the case when $d_1 \neq 0$ — that is, there's at least one real root. I claim that d_1 must be even. Otherwise, by choosing a numbers a and b "close enough" to r_1 but on opposite sides of it, we have that $p(a)$ and $p(b)$ have opposite signs. That is, one's positive and one's negative.

How close is "close enough"? Well, if ϵ is the distance from r_1 to the closest other real root and we choose $a < r_1 < b$ with both $r_1 - a$ and $b - r_1$ less than ϵ, then if d_1 is odd, $(a - r_1)^{d_1}$ is negative, and $(b - r_1)^{d_1}$ is positive. Now for any $j \neq 1$ ($j < \ell$), it's clear that $(a-r_j)^{d_j}$ and $(b-r_j)^{d_j}$ have the same sign (a and b are both on the same side of r_j). So do $a^2+b_sa+c_s$ and $b^2+b_sb+c_s$ for the quadratic irreducible factors (if any) — both of these are positive. So $p(a)$ and $p(b)$ would have opposite signs if they are that close to r_1, contradicting the basic assumption.

Now letting $(x-r_1)^{d_1} = q(x)^2$ and (by the IH) the product $t(x)$ of all the other factors be $\sum_{j=1}^{k} t_j(x)^2$, we can let $p_j(x) = q(x)t_j(x)$. [You should check —ideally in your head, or the head of some other bright person — that $p(x) = q(x)^2t(x)$ implies that $t(a) \geq 0$ for all a, too. You should also note that this part of the problem shows that, if $p(a) \geq 0$ for all a and $p(x)$ has all its roots real, then $p(x)$ is a perfect square.]

So we may assume that $p(x)$ has at least one irreducible (over the reals) factor of the form x^2+bx+c. [In fact, we could at this point assume that p factors completely into such quadratics, but this is overkill.] If the complex roots of this quadratic are $\alpha \pm \beta i$, then the quadratic itself is $(x-\alpha)^2+\beta^2$. So if $p(x) = (x^2+bx+c)t(x)$, we easily check that $t(a) \geq 0$ for all a. By induction, $t(x) = \sum_{j=0}^{v} t_j^2(x)$ for some polynomials t_j, and then $p(x)$ will be a sum of $2v$ perfect squares.

I trust this is clear, if rather long-winded. [All those parenthetical asides…] But I wanted not just to solve it, but to pull it to pieces, to extract as much pedagogical juice as was there. I believe this result was known to Da Big Guy.

I used the following very basic fact about an arbitrary nonconstant polynomial $p(x) = a_nx^n + \cdots + a_0$ (with $a_n \neq 0$) rather explicitly in the above proof:

If the roots of $p(x)$ are r_1,…,r_n (repeated with multiplicity if necessary), then

$$p(x) = a_nx^n + \cdots + a_0 = a_n(x-r_1)\cdots(x-r_n).$$

This is a routine observation, but it's often overlooked. Since any polynomial over any field has a full set of roots in some probably bigger field (Algebra I stuff, and you need to know this), this always provides two ways of looking at any nonconstant polynomial.

Even more overlooked is the consequence concerning the coefficients. Just by multiplying out the right-hand side of that last equation, we see that $-\frac{a_{n-1}}{a_n} = r_1+r_2+\cdots+r_n$. Also $+\frac{a_{n-2}}{a_n} = r_1r_2+r_1r_3+\cdots+r_{n-1}r_n$. And so on; $(-1)^j\frac{a_{n-j}}{a_n}$ is the sum of a bunch of products — those products consist of the r_k's taken j at a time. In particular — and a very useful obervation — $r_1r_2\cdots r_n = (-1)^n\frac{a_0}{a_n}$.

Let's see this in action. The next problem was B4 on Putnam 2003.

PROBLEM 2. Suppose that

$$f(z) = az^4+bz^3+cz^2+dz+e = a(z-r_1)(z-r_2)(z-r_3)(z-r_4),$$

where a,b,c,d and e are integers with $a \neq 0$. Show that if r_1+r_2 is rational, and $r_1+r_2 \neq r_3+r_4$, then r_1r_2 is rational.

A few points worth making: first, the use of z as the variable implicitly allows the r_j's to be complex. This does not really affect the problem. Second, the coefficeints being integers is a bit bogus — they might as well be rationals. Third, what the proof shows is that this works over any pair of fields $F \leq K$. If a,b,c,d and e come from F and the roots $r_1, \ldots, r_4$ are in K, and we assume that $r_1 + r_2$ is an element of F which is different from $r_3 + r_4$, then $r_1 r_2$ must also be in F.

Solution: By the observation above, we know that $r_1 + r_2 + r_3 + r_4 = -\frac{b}{a}$, $r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4 = \frac{c}{a}$, $r_1r_2r_3 + r_1r_2r_4 + r_1r_3r_4 + r_2r_3r_4 = -\frac{d}{a}$ and $r_1r_2r_3r_4 = \frac{e}{a}$. Of course, all the right-hand sides of these equations are rational.

From this and the fact that $r_1 + r_2$ is rational, we get that the following are rational, too: $r_3 + r_4 = -\frac{b}{a} - (r_1 + r_2)$; $r_1r_2 + r_3r_4 = \frac{c}{a} - (r_1 + r_2)(r_3 + r_4)$; and $r_1r_2(r_3+r_4) + r_3r_4(r_1+r_2) = -\frac{d}{a}$. So $r_1r_2(r_1+r_2) + r_3r_4(r_1+r_2)$ is also rational. Subtracting the last two expressions, we see that $r_1r_2[(r_1 + r_2) - (r_3 + r_4)]$ is rational. Of course $(r_1 + r_2) - (r_3 + r_4)$ is rational, and since it's nonzero, we can divide by it to draw the desired conclusion.

An important property of polynomials with integer coefficients is *Gauss' Lemma*, which in this context says the following:

LEMMA (da Big Guy). Suppose that $p(x)$ is a polynomial with integer coefficients and that $p(x) = p_1(x)p_2(x)$ where p_1 and p_2 have rational coefficients. Then there are rational constants c_1 and c_2 such that $q_1 = c_1 p_1$ and $q_2 = c_2 p_2$ have integer coefficients; further $p(x) = q_1(x)q_2(x)$.

[Slogan: "If it factors over the rationals, then it factors over the integers, with basically the same factors."]

A simple corollary is this: if $p(x)$ has integer coefficients, and the integer c is a root of p, then $p(x) = (x - c)q(x)$ where q has integer coefficients. This can also be proved directly rather easily. It's a simple observation, but the main thing that makes the rather bizarre proof in the next one run.

PROBLEM 3 (A6, Putnam 2000) Let $f(x)$ be a polynomial with integer coefficients. Let $a_0 = 0$ and $a_{n+1} = f(a_n)$ for any nonnegative integer n. Show that if $a_m = 0$ for some positive m, then $a_1 = 0$ or $a_2 = 0$.

Solution: We start with some simple observations. First, a_1 is the constant coefficient of f. Next, $a_1 | a_n$ for every n (by induction; if $f(x) = a_1 + b_1 x + \cdots + b_j x^j$, then $a_{n+1} = f(a_n) = a_1 + b_1 a_n + \cdots + b_j a_n^j$, etc.)

Now we proceed by contradiction. Assume that a_1 and a_2 are $\neq 0$, but $a_m = 0$ with $m \geq 3$ — further assume that m has been chosen as small as possible.

The last assumption tells us that sequence of a_n's doesn't cycle until we hit $n = m$. That is, if $k < \ell \leq m$, we must have $a_k \neq a_\ell$ — otherwise, by applying f $m - \ell$ times, we would get $a_{k+(m-\ell)} = a_m = 0$, whereas $k + (m - \ell) < m$.

So $a_m = f(a_{m-1}) = 0$. Thus $f(x) = (x - a_{m-1})g(x)$ where g has integer coefficients. We must have that $a_{m-1} | a_1$ and we already know $a_1 | a_{m-1}$. So

$a_{m-1} = \pm a_1$; and $a_{m-1} = a_1$ is impossible. Hence $a_{m-1} = -a_1$ and

$$f(x) = (x + a_1)g(x).$$

Notice that $g(x)$ has constant coefficient 1.

Now comes the crunch; working backwards, we show for each $2 \leq k \leq m-2$ the following by induction on k.

CLAIM. $a_{m-k} = -ka_1$ and $g(a_{m-k}) = 1$.

(If $m = 3$, the claim is vacuously true and we proceed to the next step. We stop once we hit $k = m-2$.)

To show the claim, we start with the case $k = 2$. We know that $a_{m-2} = ba_1$ for some integer b. So

$$-a_1 = a_{m-1} = f(a_{m-2}) = (a_{m-2} + a_1)g(a_{m-2}) = a_1(b+1)g(a_{m-2}).$$

Cancelling the a_1's, we must have $b + 1 = \pm 1$. $b = 0$ is impossible, so indeed $b = -2$ and thus $g(a_{m-2}) = 1$, not -1.

For the general case, suppose we have as the induction hypothesis that for any $2 \leq j < k$, $a_{m-j} = -ja_1$ and $g(a_{m-j}) = 1$ and $k \leq m-2$. Start by applying this to $j = k-1$;

$$-(k-1)a_1 = a_{m-(k-1)} = f(a_{m-k}) = (a_{m-k} + a_1)g(a_{m-k}).$$

Now for some integer c, $a_{m-k} = ca_1$ and we investigate the possibilities for c, eventually concluding that it has to be $-k$. c cannot be 0 or 1. It also cannot be $-j$ for any $1 \leq j < k$ as $a_{m-k} \neq a_{m-j} = -ja_1$.

Substituting ca_1 for a_{m-k} in the last displayed equation, and cancelling a_1's, we get $-(k-1) = (c+1)g(a_{m-k})$ and so $(c+1)|(k-1)$. Now we suppose $c > 1$ and rule that out. Since we know that $g(a_{m-(k-1)}) = 1$, then $g(x) - 1$ has root $a_{m-(k-1)} = -(k-1)a_1$, so that

$$g(x) = 1 + (x + (k-1)a_1)h(x).$$

If $h(a_{m-k}) = 0$, then $g(a_{m-k}) = 1$ and $c = -k$; otherwise

$$|g(a_{m-k})| = |1 + (c + k - 1)a_1 h(a_{m-k})| \geq (c + k - 1)|a_1| - 1.$$

But also $|g(a_{m-k})| \leq |f(a_{m-k})| = |a_{m-(k-1)}| = (k-1)|a_1|$. These inequalities make $c > 1$ impossible.

The only choice left for c is indeed $-k$ (just using $|c+1| \leq k-1$). This immediately forces $g(a_{m-k}) = 1$, and keeps the induction rolling. That's the proof of the claim.

We apply it to $k = m-2$. We get $a_2 = -(m-2)a_1$ and $g(a_2) = 1$. We have

$$-(m-2)a_1 = a_2 = f(a_1) = 2a_1 g(a_1),$$

so $|g(a_1)| = \frac{m-2}{2}$. But as above, $g(x) = 1 + (x + (m-2)a_1)p(x)$, where p has integer coefficients. So $|g(a_1)| \geq |(a_1 + (m-2)a_1)p(a_1)| - 1$. In case $p(a_1) \neq 0$, this is $\geq m-2$. That's out. If $p(a_1) = 0$, then $g(a_1) = 1$, but then $f(a_1) = 2a_1$, and we know it's $-(m-2)a_1$. So that's out, too. We have our final contradiction, and thus the proof of the statement.

Something that should be better known than it is concerns the multiplicity of roots of a polynomial. The basic fact is:

Suppose that r is a root of the polynomial $p(x)$. Then r is of multiplicity ≥ 2 if and only if r is also a root of $p'(x)$. (This is easily proved using the product rule.)

From this it follows easily that r has multiplicity exactly m if and only if r is a root of $p(x)$, $p'(x)$,..., $p^{(m-1)}(x)$ but not of $p^{(m)}$. ($p^{(k)}(x)$ is the kth derivative of p.) It is also easy to see that the multiplicity of r as a root of p' must be exactly $m-1$.

[These facts are usually stated for polynomials over the reals and complex numbers, but are true over field of characteristic 0 if one uses the "formal derivative" — for $p(x) = \sum_{k=0}^{n} a_k x^k$, define $p'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$. Weirdness can happen in finite characteristic — what, specifically?]

PROBLEM 4 (B2, Putnam 1999).Let $P(x)$ be a polynomial of degree n such that $P(x) = Q(x)P''(x)$, where $Q(x)$ is a quadratic polynomial and $P''(x)$ is the second derivative of $P(x)$. Show that if $P(x)$ has at least two distinct roots then it must have n distinct roots. [The roots may be either real or complex.]

Solution: Note that P cannot be a nonzero constant, nor can it have degree 1. We also ignore the (either trivial, or meaningless) case when P is the constant 0. By comparing the coefficients of x^n, we see that the x^2-coefficient of Q can only be $\frac{1}{n(n-1)}$. We do the problem in the contrapositive. Suppose that r is a root of P which has multiplicity at least 2. We show that r has multiplicity n, and that does it — there can be no other roots. To do this, we show that r is a root of $P^{(k)}$ for every $k < n$.

Now by the observations in the last couple of paragraphs, the multiplicity of r as a root of P'' is two less than its multiplicity in P. This implies that $(x-r)^2|Q$ and so Q can only be $\frac{1}{n(n-1)}(x-r)^2$. The given equation becomes $n(n-1)P = (x-r)^2 P''$.

We show by induction on k that

$$[n(n-1) - k(k-1)]P^{(k)} = (x-r)^2 P^{(k+2)} + 2k(x-r)P^{(k+1)}.$$

Interpreting $P^{(0)}$ as P itself, this is just the last equation in case $k = 0$. For $k = 1$ it follows immediately from the last equation by differentiating. Indeed, if are given the displayed equation, the differentiating both sides yields

$$[n(n-1)-k(k-1)]P^{(k+1)} = (x-r)^2 P^{(k+3)} + 2(x-r)P^{(k+2)} + 2k(x-r)P^{(k+2)} + 2kP^{(k+1)}.$$

Shifting $2kP^{(k+1)}$ across the equality and collecting $P^{(k+2)}$-terms gives

$$[n(n-1) - (k+1)k]P^{(k+1)} = (x-r)^2 P^{(k+3)} + 2(k+1)(x-r)P^{(k+2)},$$

finishing the inductive step.

Now if $k < n$, $n(n-1) - k(k-1) > 0$ and $x - r$ is patently a root of the right-hand side of the displayed equation we proved, so indeed $x - r$ is a root of $P^{(k)}$. This does it.

[I presume this is not the first time you have seen a proof of something by induction where we have to prove something stronger than what we really want to keep the ball rolling. Often, the difficulty is finding the correct induction hypothesis.]

One of the cuter simple ideas associated with polynomials is the notion of palindrome. For simplicity, we assume $p(x) = \sum_{k=0}^{n} a_k x^k$ with both $a_n, a_0 \neq 0$; we won't define palindromes of other polynomials. The *palindrome* $Pal(p)$ of p is the polynomial $\sum_{k=0}^{n} a_{m-k} x^k$, also of degree n. (E.g., if $p(x) = -3x^3+2x+1$, then $Pal(p)(x) = x^3+2x^2-3$.) $Pal(p)$ is easily seen to be the same as $x^n p(x^{-1})$. If, we have $Pal(p) = p$, p itself is called **a** *palindrome.* [I should mention that while the terminology "palindrome" is standard, the notation $Pal(p)$ is not — as far as I know, there is no standard notation for the palindrome of a polynomial.]

A few simple observations, all readily checked from the definition or the easy characterization. First $Pal(Pal(p)) = p$ for any p of the required form (this would not work if we extended the definition to all polynomials in the most obvious way). Next, $Pal(p(x)q(x)) = Pal(p(x))Pal(q(x))$. (Under certain situations, $Pal(p+q) = Pal(p) + Pal(q)$, too, but not always.)

Most important, r is a root of $p(x)$ (of multiplicity m) if and only if r^{-1} is a root of $Pal(p)(x)$ (of the same multiplicity m). In particular, if p is its own palindrome, then when r is a root, so is r^{-1}.

I trust you see this is rather adorable. But is it useful? Well, check out following two items, neither of which mentions palindromes explicitly.

PROBLEM 5 (B5, Putnam 1990). Does there exist an infinite sequence $a_0, a_1, \ldots, a_n, \ldots$ of nonzero real numbers such that, for every $n \geq 1$, $p_n(x) = a_0 + a_1 x + \cdots + a_n x^n$ has n distinct real roots?

Solution: The answer's "yes", but it's not as obvious as it might look. In fact, something more is true:

CLAIM: Suppose that $p(x) = \sum_{k=0}^{n} a_k x^k$ is a polynomial with n distinct nonzero real roots. Then there is an $\epsilon > 0$ such that whenever $0 < |a_{n+1}| < \epsilon$, $p(x) + a_{n+1}x^{n+1}$ has $n+1$ distinct real roots.

It is clearly enought to verify this claim, because it allows us to pick our a_n's inductively so that each p_n has n distinct real roots. Any a_0 and a_1 will get us started. So why is the claim true?

Given $p_n = p$ as above, let $q_n(x) = Pal(p_n)$. Then q_n has n distinct nonzero real roots — if $r_1, \ldots, r_n$ are the roots of p_n, then $r_1^{-1}, \ldots, r_n^{-1}$ are the roots of q_n. Then $xq_n(x)$ has $n+1$ distinct real roots, one of which is zero.

Now if $a_{n+1} \neq 0$ is any real number which is small enough in absolute value, then $xq_n(x) + a_{n+1}$ still has $n+1$ distinct real roots, all nonzero. $xq_n(x)$ will have n relative extremums, one between each consecutive pair of roots. This is by Rolle's Theorem. Each relative minimum value will be negative and each relative maximum value positive; if we move the graph of $y = xq_n(x)$ up or down by a small enough constant (less in absolute value than the smallest absolute value of these minimum and maximum values), this will remain true. (I trust this is clear; perhaps an actual graph would help.)

Now take $p_{n+1} = a_0 + a_1x + \cdots + a_nx^n + a_{n+1}x^{n+1}$, the palindrome of $xq_n + a_{n+1}$; it has $n+1$ distinct real roots.

I dare you to do this without using the palindrome — repeating the idea without using the name doesn't count.

The next one really has a sort of "semi-palindrome" in it. But you should see that the idea is the same. How do think I found $g(x)$ in the first place?

PROBLEM 6 (A6, Putnam '85). Given a polynomial $p(x) = \sum_{k=0}^{m} a_kx^k$, let $\Gamma(p(x)) = \sum_{k=0}^{m} a_k^2$. Given $f(x) = 3x^2 + 7x + 2$, find with proof a polynomial $g(x)$ such that

1. $g(0) = 1$, and

2. $\Gamma(f(x)^n) = \Gamma(g(x)^n)$ for every positive integer n.

Of course, if $q = Pal(p)$, then $\Gamma(p) = \Gamma(q)$, but that doesn't work in this case, as the palindrome of f has constant coefficient 3, not 1. But...

Solution: Start by factoring f (always a good move with polynomials). $f(x) = (3x+1)(x+2)$, so maybe the "quasi-palindrome"
$g(x) = (3x+1)(2x+1) = 6x^2 + 5x + 1$ works. In fact it does, and here's why. First note that $f(x)^n = (3x+1)^n(x+2)^n$ and $g(x)^n = (3x+1)^n(2x+1)^n$, for all n; also $(x+2)^n$ and $(2x+1)^n$ are palindromes of each other.

Now Γ is not multiplicative; (e.g., $\Gamma(3x+1) = 10$, $\Gamma(x+2) = 5$ and
$\Gamma((3x+1)(x+2)) = 62$). But it has the following property, which does the trick.

CLAIM: If $p_1(x) = q(x)r_1(x)$ and $p_2(x) = q(x)r_2(x)$, where $r_2 = Pal(r_1)$, then $\Gamma(p_1) = \Gamma(p_2)$.

Proof of the claim (and then end of the problem): The crucial observation is that, for any $p(x)$, $\Gamma(p)$ is the constant coefficient (that is, the coefficient of x^0) in the product $p(x)p(x^{-1})$. This is easily seen just by multiplying out $(a_0 + a_1x + \cdots + a_mx^m)(a_0 + a_1x^{-1} + \cdots + a_mx^{-m})$.

So $\Gamma(p_1)$ is the constant coefficient of $q(x)q(x^{-1})r_1(x)r_1(x^{-1})$ and $\Gamma(p_2)$ is the constant coefficient of $q(x)q(x^{-1})r_2(x)r_2(x^{-1})$. But as r_1 and r_2 are palindromes, $r_1(x)r_1(x^{-1}) = r_2(x)r_2(x^{-1}) = x^{-n}r_1(x)r_2(x)$. That does it.

Here's an oldie-but-goodie.

PROBLEM 7 (A3, Putnam '78) Let $p(x) = 2+4x+3x^2+5x^3+3x^4+4x^5+2x^6$, and for $0 < k < 5$, define

$$I_k = \int_0^\infty \frac{x^k}{p(x)} dx.$$

For which value of k is I_k minimum?

Solution: You will note that the crucial properties of p are (i) it has no nonnegative roots; and (ii) it's a palindrome. If you change the degree (which could be anything at least 2) the numbers will change but the idea won't.

Note that I_k could also be defined for $-1 < k \leq 0$ using the same formula. For negative k, the integral is also improper at 0, but it converges as long as $k > -1$. We do so — that is, we extend the definition to $-1 < k < 5$.

Having noticed that p is a palindrome, we make the obvious substitution. Let $u = x^{-1}$; then $p(x) = p(u^{-1}) = u^{-6}p(u)$. $dx = -\frac{du}{u^2}$ and of course $x^k = u^{-k}$. The integral becomes

$$\int_{\infty}^{0} \frac{u^{-k}}{u^{-6}p(u)}(-\frac{du}{u^2}),$$

which is

$$\int_{0}^{\infty} \frac{u^{4-k}}{p(u)} du,$$

which is I_{4-k}. (This works for any $-1 < k < 5$.)

The minimum occurs when $k = 4 - k$, that is, when $k = 2$. Indeed, we show that $I_k > I_2$ when $k > 2$ (and hence when $k < 2$). Say $k = 2 + 2\alpha$ where $0 < \alpha < \frac{3}{2}$. Then $I_k - I_2 = \frac{1}{2}(I_{2+2\alpha} + I_{2-2\alpha} - 2I_2) =$

$$\frac{1}{2}\int_{0}^{\infty} \frac{x^{2+2\alpha} - 2x^2 + x^{2-2\alpha}}{p(x)} dx.$$

The denominator is always positive on $[0, \infty)$, and so is the numerator, except at $x = 0$, $x = 1$. It's $x^2(x^{2\alpha} - 2 + x^{-2\alpha}) = x^2(x^\alpha - x^{-\alpha})^2$. So the last integral is positive, so $I_k > I_2$. That does it.

The notion of palindrome extends in an obvious way to numbers expressed in decimal notation (e.g., 12345 and 54321 are palindromes of each other, and 102030201 just plain a palindrome) or indeed in any base. Since decimal notation is polynomial in nature, this is to be expected. The next little gem does not mention polynomials at all, but should be thought of in terms of them.

PROBLEM 8 (B5, Putnam 2002). A base b palindrome is an integer which is the same when read backwards in base b. For example, 200 is not a palindrome in base 10, but it is a palindrome in base 9 (242) and in base 7 (404). Show that there is an integer which for at least 2002 values of b is a palindrome in base b with three digits.

Although I'm not sure that I approve of using "digits" for places like that, this is in a way a classic Putnam problem. That is, you can look at it and pick away at it forever without getting anywhere, but it becomes obvious (and short) once you get the idea.

Solution: A base b palindrome with three "digits" is aca in base b. We must have $1 \leq a < b$ and $0 \leq c < b$. The number represented is then $ab^2 + cb + a = a(b^2 + 1) + cb$. In case $c = 2a$, this simplifies to $a(b + 1)^2$.

Let $N = [(2002)!]^2$ and for $j = 1, 2, \ldots, 2002$ let $a_j = j^2$, $c_j = 2j^2$ and $b_j = \frac{(2002)!}{j} - 1$. Clearly $a_j < c_j < b_j$ for each j. The number represented by the base b_j expression $a_j c_j a_j$ is then $a_j b_j^2 + c_j b_j + a_j = a_j(b_j + 1)^2 = N$ for all j.

Without the first paragraph, which is not necessary, this answer is shorter than the statement of the problem. But enough about palindromes for now.

Here's another problem in which no mention is made of polynomials, but they help with the notation. It's easy if you look at it right.

PROBLEM 9 (Putnam A2, 1986) Find the units digit (the number in the ones place) of

$$[\frac{10^{20000}}{10^{100} + 3}].$$

Solution: While it is not necessary, it is useful to think of 10^{100} as x, so that $10^{20000} = x^{200}$. In fact, you might want to think of -3 as y. Let's do so.

$$x^{200} - y^{200} = (x - y)(x^{199} + x^{198}y + \cdots + xy^{198} + y^{199}),$$

so

$$x^{200} = (x^{199} + x^{198}y \cdots + xy^{198} + y^{199})(x - y) + y^{200}.$$

Now $y^{200} = (-3)^{200} = 9^{100} < 10^{100} + 3$, so the integer part of $\frac{x^{200}}{x-y}$ is $x^{199} + \cdots + xy^{198} + y^{199}$, which is clearly equivalent to $(-3)^{199} \pmod{10}$. Operating mod 10, $(-3)^{199} = (-3)(9^{99})$ is equivalent to $(-3)((-1)^{99}) = +3$. The final (units) digit is 3.

For another example where polynomials come in handy, look at this beauty.

PROBLEM 10 (B5, Putnam 2000). Let S_0 be a finite nonempty set of positive integers. We define sets S_1, S_2,...,S_n,... of positive integers as follows:

Integer a is in S_{n+1} if and only if exactly one of a and $a - 1$ is in S_n.

Show that there exist infinitely many integers N such that $S_N = S_0 \cup \{N + a : a \in S_0\}$.

So the set S_0 "replicates" itself later, but reproduces the original, too. It's not obvious how to usefully bring polynomials into this, but just watch. In fact, they are polynomials over the 2-element field $\mathcal{Z}_2$.

Solution: Given any finite nonempty set of positive integers S, let $p_S(x)$ be the polynomial (with coefficients in $\mathcal{Z}_2$) $\sum_{s \in S} x^s$. For any such S, consider $(1 + x)p_S$. If $a - 1 \in S$ and $a \notin S$, then the coefficient of x^a in $(1 + x)p_S$ is 1 as x^{a-1} is multiplied by x; if $a \in S$ but $a - 1 \notin S$, the coefficient is again 1. If neither is in S, the coefficient is 0, as it is if both $a - 1$ and a are in S — then we get $1 \cdot x^a + x \cdot x^{a-1} = 0x^a$ since we are over $\mathcal{Z}_2$.

Thus, if $S = S_n$, $(1 + x)p_S = p_{S_{n+1}}$. Generally, $(1 + x)^n p_{S_0} = p_{S_n}$ for each n. Now if $N = 2^m$ for some m, then $(1 + x)^N = 1 + x^N$ as we are operating over $\mathscr{Z}_2$. If we also suppose that $N > a$ for any $a \in S_0$, then

$$(1+x)^N p_{S_0} = (1+x^N)p_{S_0} = \sum_{a\in S_0} x^a + \sum_{a\in S_0} x^{N+a}$$

with no cancellations. This shows that if N is a large enough power of 2, S_N has exactly the form requested in the statement of the problem.

I could go on, but for now just a word about polynomials in more than one variable. The basic thing to know is that if $p(x_1,\ldots,x_n)$ and $q(x_1,\ldots,x_n)$ are such polynomials (over any infinite field F, usually the reals) and $p(\bar{a}) = q(\bar{a})$ for every $\bar{a} \in F^n$, then the coefficients must be identical. This is obvious when $n = 1$, but true for any n. To spell out what I mean, given any tuple $e = (e_1,\ldots,e_n)$ of nonnegative integers, there is a coefficient c_e of $x_1^{e_1}\cdots x_n^{e_n}$ occurring in p and such a coefficient d_e in q. If $p(\bar{a}) = q(\bar{a})$ for every $\bar{a}$, then $c_e = d_e$ for every e. (This is not hard to prove by induction; it is standard, so you can use it. Also, it definitely needs that the field is infinite — if F is finite, it's false even if $n = 1$.)

Let's do a pretty simple one.

PROBLEM 11 (B1, Putnam 2003). Do there exist polynomials $a(x)$, $b(x)$, $c(y)$ and $d(y)$ such that

$$a(x)c(y) + b(x)d(y) = 1 + xy + x^2y^2$$

holds identically?

Solution: No, as you would expect. The first solution I got to this was very ad hoc, involving taking derivatives and examining the coefficients in detail. I probably couldn't reproduce it to save my life. I present two proofs, one very simple-minded which I found later, the other a very clever one that Mathieu Guay-Paquet showed me.

Proof 1. Suppose towards a contradiction that we have such $a(x)$, etc. I first claim that $a(x)$ cannot have two (or more) distinct complex roots. For suppose that $a(r_1) = a(r_2) = 0$ with $r_1 \neq r_2$. Then $b(r_1)d(y) = 1 + r_1y + r_1^2y^2$ and $b(r_2)d(y) = 1 + r_2y + r_2^2y^2$ (for all y); but this implies that $1 + r_1y + r_1^2y^2$ and $1 + r_2y + r_2y^2$ are scalar multiples of each other (over the complexes). That's false.

Similarly, of course, $b(x)$, $c(y)$ and $d(y)$ can have a most one complex root apiece. Next, I claim that if indeed $a(x)$ has a complex root, it must be 0. For if $r \neq 0$ and $a(r) = 0$, then $b(r)d(y) = 1 + ry + r^2y^2$ for all y. Obviously $b(r) \neq 0$. But then $d(y)$ has the two distinct roots $\frac{1}{2r}(-1 \pm i\sqrt{3})$, contrary to the above.

Similarly the only possible root of the others is 0. So the only possibility is that $a(x) = a(1)x^k$, $b(x) = b(1)x^\ell$, $c(y) = c(1)y^m$ and $d(y) = d(1)y^n$ for some integers k, ℓ, m, n. And that's out, too.

Proof 2. Suppose that $a(x)$, $b(x)$, $c(y)$ and $d(y)$ form a counterexample, where $a(x) = a_0 + a_1x + a_2x^2 + \ldots$, $b(x) = b_0 + b_1x + b_2x^2 + \ldots$, $c(y) =$

$c_0 + c_1 y + c_2 y^2 + \ldots$ and $d(y) = d_0 + d_1 y + d_2 y^2 + \ldots$, where in each case the $\ldots$ stands for terms of higher degree. Then

$$1+xy+x^2y^2 = (a_0+a_1x+a_2x^2+\ldots)(c_0+c_1y+c_2y^2+\ldots)+(b_0+b_1x+b_2x^2+\ldots)(d_0+d_1y+d_2y^2+\ldots).$$

Comparing the coefficients of x^0y^0, xy and x^2y^2 on each side gives $a_0b_0+c_0d_0 = a_1b_1 + c_1d_1 = a_2b_2 + c_2d_2 = 1$. Comparing the coefficients of x, y, x^2, y^2, x^2y and xy^2 we see that $a_1c_0 + b_1d_0 = a_0c_1 + b_0d_1 = a_2c_0 + b_2d_0 = a_0c_2 + b_0d_2 = a_2c_1 + b_2d_1 = a_1c_2 + b_1d_2 = 0$. Thus, $\begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \begin{pmatrix} c_0 & c_1 & c_2 \\ d_0 & d_1 & d_2 \end{pmatrix} = I$, the 3×3 identity matrix. This is impossible over any field.

The second proof (Mathieu's) shows the impossibility of the identity of the polynomials over any field; it is thus slightly preferable to mine, which can be directly adapted to any field of characteristic different from 2 or 3.